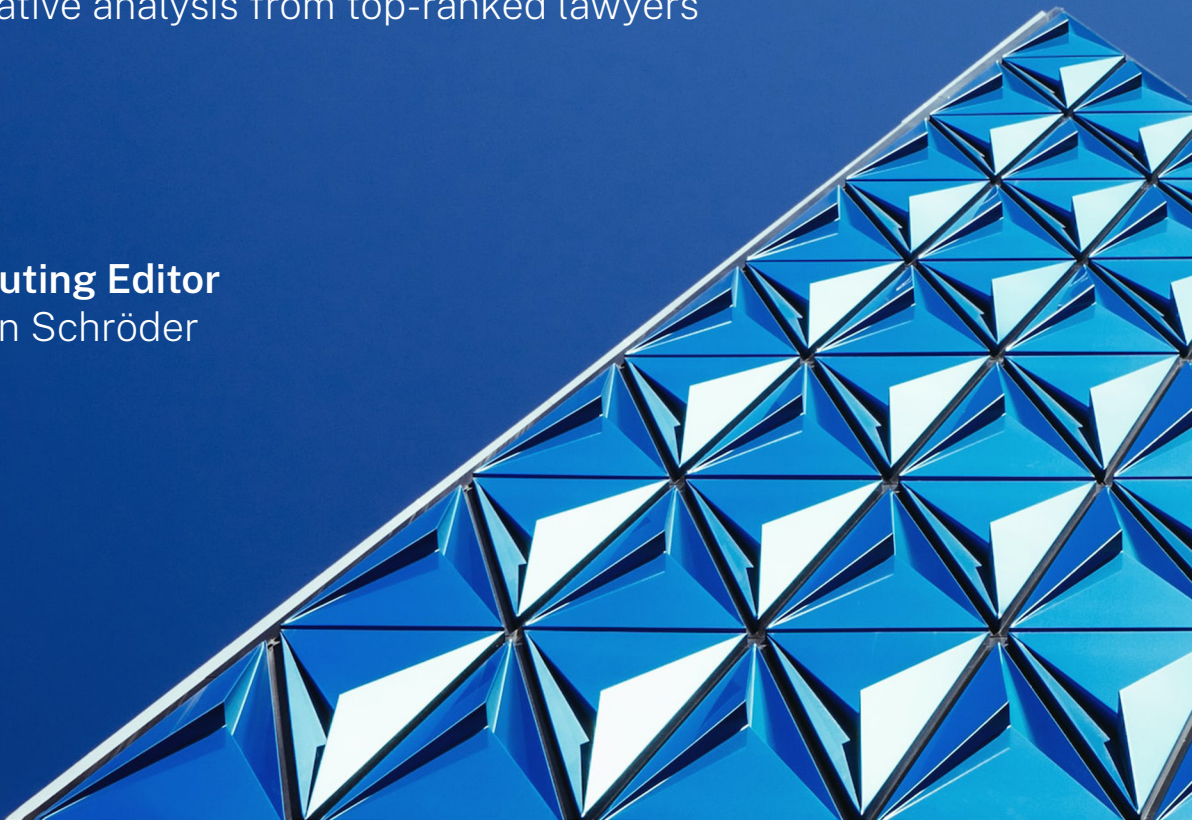

CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2025

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Contributing Editor
Christian Schröder
Orrick



Chambers

Global Practice Guides

Cybersecurity

Contributing Editor

Christian Schröder

Orrick

2025

Chambers Global Practice Guides

For more than 20 years, Chambers Global Guides have ranked lawyers and law firms across the world. Chambers now offer clients a new series of Global Practice Guides, which contain practical guidance on doing legal business in key jurisdictions. We use our knowledge of the world's best lawyers to select leading law firms in each jurisdiction to write the 'Law & Practice' sections. In addition, the 'Trends & Developments' sections analyse trends and developments in local legal markets.

Disclaimer: The information in this guide is provided for general reference only, not as specific legal advice. Views expressed by the authors are not necessarily the views of the law firms in which they practise. For specific legal advice, a lawyer should be consulted.

Content Management Director Claire Oxborrow

Content Manager Jonathan Mendelowitz

Senior Content Reviewer Sally McGonigal, Ethne Withers, Deborah Sinclair and Stephen Dinkeldein

Content Reviewers Vivienne Button, Lawrence Garrett, Sean Marshall, Marianne Page, Heather Palomino and Adrian Ciechacki

Content Coordination Manager Nancy Laidler

Senior Content Coordinators Carla Cagnina and Delicia Tasinda

Content Coordinator Hannah Leinmüller

Head of Production Jasper John

Production Coordinator Genevieve Sibayan

Published by

Chambers and Partners

165 Fleet Street

London

EC4A 2AE

Tel +44 20 7606 8844

Fax +44 20 7831 5662

Web www.chambers.com

Copyright © 2025

Chambers and Partners

CONTENTS

INTRODUCTION

Contributed by Christian Schröder and Odey Hardan, Orrick p.4

AUSTRALIA

Law and Practice p.8

Contributed by Nyman Gibson Miralis

Trends and Developments p.29

Contributed by Nyman Gibson Miralis

BELGIUM

Law and Practice p.39

Contributed by Alston & Bird LLP

Trends and Developments p.53

Contributed by Loyens & Loeff

BRAZIL

Trends and Developments p.61

Contributed by Machado Meyer

CHILE

Law and Practice p.71

Contributed by Magliona Abogados

HUNGARY

Law and Practice p.91

Contributed by PROVARIS Varga & Partners

Trends and Developments p.114

Contributed by PROVARIS Varga & Partners

INDIA

Trends and Developments p.121

Contributed by JSA

ITALY

Law and Practice p.127

Contributed by ICT Legal Consulting

Trends and Developments p.158

Contributed by ICT Legal Consulting

JAPAN

Law and Practice p.163

Contributed by Mori Hamada & Matsumoto

Trends and Developments p.174

Contributed by Nagashima Ohno & Tsunematsu

MEXICO

Law and Practice p.183

Contributed by Nader Hayaux & Goebel

PORTUGAL

Law and Practice p.197

Contributed by Abreu Advogados

Trends and Developments p.215

Contributed by Abreu Advogados

SINGAPORE

Law and Practice p.222

Contributed by Drew & Napier LLC

Trends and Developments p.244

Contributed by CMS

SWEDEN

Law and Practice p.252

Contributed by Mannheimer Swartling

Trends and Developments p.266

Contributed by Mannheimer Swartling

SWITZERLAND

Law and Practice p.272

Contributed by Walder Wyss Ltd

Trends and Developments p.286

Contributed by Walder Wyss Ltd

TÜRKIYE

Law and Practice p.293

Contributed by YAZICIOGLU Legal

UK

Law and Practice p.318

Contributed by Sidley Austin LLP

Trends and Developments p.336

Contributed by Sidley Austin LLP

USA

Law and Practice p.343

Contributed by Freshfields

Trends and Developments p.358

Contributed by Freshfields

INTRODUCTION

Contributed by: Christian Schröder and Odey Hardan, **Orrick**

Orrick is a global law firm dedicated to serving the technology and innovation, energy and infrastructure, finance, and life sciences and healthtech sectors. With more than 1,100 lawyers across 25+ markets worldwide, **Orrick** provides forward-looking, pragmatic advice on transactions, litigation, and compliance matters. As one of the world's leading tech law firms, cybersecurity and privacy are central to **Orrick's** practice. The firm has 15 cybersecurity and privacy-focused partners and over 50 specialised lawyers, making it one of the strongest

data protection practices in the market, recognised by Chambers Global, US, and Europe. **Orrick** helps clients navigate the complex cybersecurity and privacy legal landscape, managing global compliance matters, cyber incidents, litigation, and regulatory investigations. They maximise data value, address global privacy requirements, and reduce security risks. Whether clients are managing compliance challenges, licensing data, or acquiring new companies, **Orrick** offers forward-thinking solutions to address data challenges.

Contributing Editor



Christian Schröder is a partner in **Orrick's** Düsseldorf office and leads the firm's Cyber, Privacy & Data Innovation Group in Europe. He collaborates with team members across the USA,

EU, and Asia to support global clients. Christian specialises in data-focused laws, including cybersecurity, privacy compliance, incident response, data licensing, AI, and regulatory investigations. He advises on internal and external data transfers, product launches, and privacy requirements for connected cars. Christian maintains strong relationships with German and EU data protection authorities, effectively defending clients in investigations. Recognised by Chambers as a top practitioner, he is a noted thought leader in privacy law.

Co-Author



Odey Hardan is an associate in **Orrick's** Cyber, Privacy & Data Innovation Group. He provides comprehensive advice on data law and EU digital law, offering strategic guidance to clients and

representing them before regulatory authorities and in court proceedings. Prior to joining **Orrick**, Odey served as a research assistant focusing on European law, authoring several academic papers. During his doctoral studies, he specialised in European, international, and data protection law.

INTRODUCTION

Contributed by: Christian Schröder and Odey Hardan, **Orrick**

Orrick, Herrington & Sutcliffe LLP

Heinrich-Heine-Allee 12
40213 Düsseldorf
Germany

Tel: +49 211 3678 7316
Email: cschroeder@orrick.com
Web: www.orrick.com



Introduction to the Cybersecurity Guide

In recent years, cybersecurity has become a paramount concern for legal professionals, policymakers, and businesses. The increasing frequency and sophistication of cyberattacks have prompted jurisdictions worldwide to enact comprehensive legal frameworks to protect digital infrastructures and ensure the safety of personal and non-personal data.

The recent wave of cybersecurity regulations reflects a global recognition of the critical importance of safeguarding digital assets. These regulations have significant implications for businesses. They underscore the necessity for comprehensive risk management strategies, accountability at the highest levels of management, and the implementation of rigorous security measures across all sectors.

One of the primary implications of these regulations is the heightened accountability placed on organisational leadership. With the mandate for senior executives to oversee cybersecurity measures, laws aim to ensure that cybersecurity is prioritised at the strategic level. This shift in responsibility requires a cultural change within organisations, where cybersecurity is integrated into the core business strategy rather than treated as a peripheral IT issue.

Furthermore, the emphasis on incident reporting and transparency has profound implications for how organisations handle data breaches and cyber incidents. Timely reporting to regulatory authorities and affected parties is not only a legal obligation but also a critical component of maintaining trust and credibility. Organisations must develop clear protocols for incident response and communication to comply with these requirements.

The focus on supply chain security and the resilience of critical infrastructures highlights the interconnected nature of modern digital ecosystems. Cybersecurity cannot be viewed in isolation; it requires an inclusive approach that involves stakeholders across the supply chain. This interconnectedness of services necessitates that organisations conduct thorough assessments of their third-party relationships and implement stringent security controls to mitigate risks.

The European Union (EU) has implemented a series of directives and regulations aimed at enhancing the security of its digital market.

One of the cornerstone laws in the EU's cybersecurity framework is the Network and Information Security Directive (NIS2). The NIS2 Direc-

INTRODUCTION

Contributed by: Christian Schröder and Odey Hardan, Orrick

tive applies to companies in sectors deemed critical and listed in Annex I and II of the Directive, including digital infrastructure and certain manufacturing industries. Specifically, it affects entities such as internet node operators, DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, and providers of publicly accessible electronic communication services. Additionally, digital service providers like online search engines, online marketplaces, and social networks, as well as manufacturers of electrical equipment, data processing devices, medical devices, and those in the machinery and automotive industries, are also covered. This directive sets out obligations for essential and important entities, such as digital service providers and operators of critical infrastructure, to implement risk management measures, conduct regular cybersecurity audits, and report significant incidents to national authorities. By holding management bodies accountable for compliance, NIS2 ensures that cybersecurity is prioritised at the highest levels of organisational leadership.

In addition to NIS2, the EU has introduced the Digital Operational Resilience Act (DORA), which targets the financial sector. The regulation addresses the critical role of information and communication technologies (ICT) in the financial sector, the vulnerabilities to cyber threats, and the dependencies on external service providers. DORA requires financial entities and critical ICT providers to establish comprehensive ICT risk management frameworks and mandates regular testing of digital operational resilience. This framework should address ICT risks and ensure high digital operational resilience. It must include strategies, policies, procedures, protocols, and applications necessary to protect all information and ICT assets. The principle of

proportionality and a risk-based approach are emphasised in DORA, requiring the framework to be tailored to the company's processes and technical means. To maintain a high level of protection, financial entities must continuously test their digital operational stability. They must develop a programme to assess their defensive readiness, identify vulnerabilities, and implement corrective measures. Tests should be conducted by independent internal or external parties, with sufficient resources provided to avoid conflicts of interest.

The Cyber Resilience Act (CRA) further complements the EU's cybersecurity framework by addressing the security of products with digital elements. The CRA imposes life cycle security obligations on manufacturers, importers, and distributors, requiring them to conduct cyber-risk assessments, manage vulnerabilities, and report security incidents to the European Union Agency for Cybersecurity (ENISA) within specified timeframes. By focusing on the security of digital products, the CRA aims to mitigate vulnerabilities and enhance user trust in the digital marketplace. The draft CRA complements other legislation like NIS2. It applies to all products connected to other devices or networks, with some exclusions such as open-source software and certain regulated services (eg, medical devices, aviation, and cars).

One of the key challenges in cybersecurity regulation is the harmonisation of standards across jurisdictions. While the EU has made strides in creating a unified cybersecurity framework, achieving global consensus remains a complex task. Differences in legal systems, regulatory approaches, and levels of technological development can hinder efforts to establish common standards. However, international co-operation and dialogue are essential to overcoming these

INTRODUCTION

Contributed by: Christian Schröder and Odey Hardan, Orrick

barriers and creating a cohesive global cybersecurity strategy.

Another challenge lies in the integration of emerging technologies, such as artificial intelligence (AI) and the Internet of Things (IoT), into existing cybersecurity frameworks. These technologies offer tremendous potential for innovation but also introduce new vulnerabilities that must be addressed. The EU's AI Act, for example, sets standards for the design and operation of AI systems to ensure they are resilient to errors and secure against unauthorised alterations. As technology continues to evolve, legal frameworks must be adaptable to accommodate new developments and address emerging threats.

Public-private partnerships also play a crucial role in enhancing cybersecurity. By collaborating with private sector entities, governments can leverage the expertise, resources, and innovation of industry leaders to strengthen cybersecurity defences. These partnerships facilitate the sharing of best practices, threat intelligence, and technical expertise, leading to more resilient digital infrastructures.

In the EU, initiatives such as the European Cybersecurity Organisation (ECISO) and the European Cybersecurity Competence Centre (ECCC) exemplify the importance of public-private collaboration. These organisations bring together stakeholders from government, industry, and academia to promote research, innovation, and capacity building in cybersecurity. By fostering a collaborative approach, the EU aims to create a secure digital environment that supports economic growth and protects citizens' rights.

For legal professionals, navigating the complexities of cybersecurity law requires a deep understanding of both the regulatory landscape and the technical aspects of cybersecurity. The path forward involves balancing innovation with regulation, ensuring that legal frameworks are both comprehensive and adaptable to emerging threats. By focusing on the implications of recent regulations and adopting forward-thinking strategies, governments and organisations can enhance their cybersecurity defences and protect their digital assets.

AUSTRALIA



Law and Practice

Contributed by:

Dennis Miralis and Jack Dennis

Nyman Gibson Miralis

Contents

1. General Overview of Laws and Regulators p.10

1.1 Cybersecurity Regulation Strategy p.10

1.2 Cybersecurity Laws p.10

1.3 Cybersecurity Regulators p.12

2. Critical Infrastructure Cybersecurity p.16

2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.16

2.2 Critical Infrastructure Cybersecurity Requirements p.17

2.3 Incident Response and Notification Obligations p.17

2.4 State Responsibilities and Obligations p.19

3. Financial Sector Operational Resilience Regulation p.20

3.1 Scope of Financial Sector Operational Resilience Regulation p.20

3.2 ICT Service Provider Contractual Requirements p.20

3.3 Key Operational Resilience Obligations p.21

3.4 Operational Resilience Enforcement p.22

3.5 International Data Transfers p.22

3.6 Threat-Led Penetration Testing p.24

4. Cyber-Resilience p.24

4.1 Cyber-Resilience Legislation p.24

4.2 Key Obligations Under Legislation p.25

5. Security Certification for ICT Products, Services and Processes p.25

5.1 Key Cybersecurity Certification Legislation p.25

6. Cybersecurity in Other Regulations p.26

6.1 Cybersecurity and Data Protection p.26

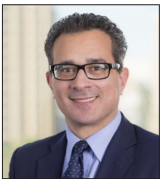
6.2 Cybersecurity and AI p.27

6.3 Cybersecurity in the Healthcare Sector p.27

Nyman Gibson Miralis is a market leader in all aspects of general, complex and international criminal law and is widely recognised for its involvement in some of Australia's most significant cases. The firm's team in Sydney has expertise in dealing with complex national and international cybercrime investigations and advising individuals and businesses who are the

subject of cybercrime investigations. Its expertise includes dealing with law enforcement requests for information from foreign jurisdictions, challenging potential extradition proceedings as well as advising and appearing in cases where assets have been restrained and confiscated worldwide.

Authors



Dennis Miralis is a partner at Nyman Gibson Miralis and a leading Australian defence lawyer who specialises in international criminal law, with a focus on complex multi-

jurisdictional investigations and criminal prosecutions. His areas of expertise include cybercrime investigations, anti-bribery and corruption, global tax investigations, proceeds of crime, anti-money laundering, worldwide freezing orders, national security law, INTERPOL Red Notices, extradition and mutual legal assistance law. In 2021 Dennis was awarded a certificate of completion for the "Cybersecurity: The Intersection of Policy and Technology" programme, January 2021, John F. Kennedy School of Government at Harvard University, Executive Education.



Jack Dennis is a senior criminal defence lawyer who practises in international and domestic criminal, corporate and tax law at Nyman Gibson Miralis. His international criminal work

includes transnational criminal and regulatory investigations, liaising with foreign legal and regulatory bodies, as well as advising clients on matters concerning international public law. Domestically, Jack has advised on a range of criminal issues and investigations, including white-collar crime, fraud, sanctions, INTERPOL, extraditions and national security. He also has significant international, corporate and tax experience, having advised on cross-border transactions and disputes involving foreign and domestic corporations and individuals, across the software, financial services and crypto industries.

Nyman Gibson Miralis

Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 292 648 884
Email: dm@ngm.com.au
Web: www.ngm.com.au



1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

On 22 November 2023 the Australian government released the 2023-2030 Australian Cyber Security Strategy (the “Strategy”), with the aim of strengthening Australia’s cyber defences and supporting people and businesses to be resilient to and recover quickly from cyber-attacks.

Alongside the Strategy was the 2023-2030 Australian Cyber Security Strategy: Action Plan (the “Action Plan”) setting out three “Horizons”, which culminate in Horizon 3 with Australia as a leader of the global frontier in developing cyber technologies and adapting to risk and opportunities. Currently, Australia is in the final year of Horizon 1 (“Strengthen our foundations”) whereby it is aiming to address critical gaps, build protections and support “initial cyber maturity uplift”, with the government setting itself up for Horizon 2 (“Expand our search”) come 2026, which aims to scale cyber maturity across the whole economy, make investments and grow a diverse cyber workforce.

The government has grounded its vision in six “shields” or “layers of defence” comprising the

businesses and citizens, safe technology, world-class threat sharing and blocking, protected critical infrastructure, sovereign capabilities, and resilient region and global leadership. It has set out in its Action Plan different actions and objectives for each shield, some of which can be seen through recent reform and others not.

Notwithstanding 2025 is the final year of Horizon 1, it is also the first year that the Action Plan is set to be reviewed; and with the Federal election to take place by May 2025, there may be some changes to the strategy, purposes and actions to come.

1.2 Cybersecurity Laws

Australia has a broad system of federal, state and territory-based laws which govern data protection, cybersecurity and cybercrime.

Data Protection

Entities dealing with personal information in Australia should also be aware of their obligations with respect to:

- the Privacy Act 1988 (Cth) (the “Privacy Act”), which regulates the handling of personal information by “APPs entities” pursuant to the Australian Privacy Principles (APPs);

- the Digital ID Act 2024 (Cth) (the “Digital ID Act”), which is intended to embed safeguards for digital ID services and data in addition to the Privacy Act;
- privacy legislation enacted at the state and territory level;
- the My Health Records Act 2012 (Cth) (the “My Health Records Act”), which imposes specific obligations for health information collected and stored in Australia’s national online health database (in addition to the Privacy Act);
- state and territory health records legislation enacted in NSW, Victoria (Vic) and the Australian Capital Territory (ACT); and
- federal, state and territory surveillance legislation, which regulates video surveillance, computer and data monitoring, GPS tracking and the use of listening devices on individuals.

Further definitions and details on the Privacy Act are set out in **6.1 Cybersecurity and Data Protection**.

Cybersecurity

Cybersecurity laws in Australia are primarily governed under sector-specific federal laws, and include the following.

- **Critical infrastructure:** this sector is regulated under the Security of Critical Infrastructure Act 2018 (Cth) (the “SOCI Act”), which imposes registration, reporting and notification obligations on owners and operators of critical infrastructure and empowers the Australian government to gather information and issue directions where there is a risk to security. More details are in **2. Critical Infrastructure Cybersecurity**.
- **Telecommunications:** this sector is regulated by dual legislation, being:

- (a) the Telecommunications Act 1997 (Cth) (the “Telecommunications Act”), which imposes security and notification obligations on Australian telecommunications providers and empowers the Australian government to gather information and issue directions; and

- (b) the Telecommunications (Interception and Access) Act 1979 (Cth) (the “TIA Act”), which prohibits the interception of communication and access to stored communication data, except for certain law enforcement and national security purposes.

- **Corporate:** corporations generally are regulated under the Corporations Act 2001 (Cth) (the “Corporations Act”), which is highly relevant to the cybersecurity space. For example, the director’s duty to exercise “care and diligence” (Section 180) is equally relevant here.
- **Financial services:** certain financial, insurance and superannuation entities are regulated through standards, including the Prudential Standard CPS 234 on Information Security (CPS 234), issued by the Australian Prudential Regulation Authority (APRA). Additionally, entities in the financial services have specific obligations under the Corporations Act, such as adequate risk management systems to hold a financial licence (Section 912A).

There are additional laws that are highly relevant to the cybersecurity space that are less sector-specific, such as consumer law, specifically the Competition and Consumer Act 2010 (Cth) (the “Consumer Act”) which addresses consumer affairs, including consumer data protection and cyberscams.

Cybercrime

Overlaying the above are various cybercrime offences in Australia at the federal, state and ter-

ritory levels. These offences broadly encompass two categories:

- offences that are directed at computers or other devices and involve hacking-type activities; and
- cyber-enabled offences where such devices are used as a key component of the offence, including in online fraud, online child abuse offences and cyberstalking.

Federally, cybercrime is criminalised under Parts 10.6 and 10.7 of the Schedule to the Criminal Code Act 1995 (Cth) (the “Criminal Code”), which set out a variety of offences with maximum penalties ranging from fine-only through to life imprisonment.

Organisations should note that in addition to the Criminal Code:

- the TIA Act also makes it a federal offence for an individual to (without authorisation) intercept or access private telecommunications without the knowledge of those involved; and
- state and territory laws criminalise computer offences similar to those criminalised under the Criminal Code (eg, Part 6 of the Crimes Act 1900 (NSW) provide for multiple computer offences regarding unauthorised access, modification or impairment of restricted data and electronic communications).

Australian states and territories also have their own criminal laws which govern cybercrime offences.

Other Laws

Areas that are also related to cybersecurity include:

- the Broadcasting Services Act 1992 (Cth) (the “Broadcasting Act”) regulates broadcasting services through internet and other means in Australia and enables the creation of industry codes of practice regulating the content of such services;
- the Online Safety Act 2021 (Cth) (OSA) establishes complaint systems for cyberbullying of children, non-consensual sharing of intimate images, cyber-abuse of adults, and the online/social media availability of content that would be subject to broadcasting classifications (restricted or age 18 years and over);
- The Spam Act 2003 (Cth) (the “Spam Act”) prohibits the use of electronic communications for the purpose of sending unsolicited marketing materials to individuals; and
- The Do Not Call Register Act 2006 (Cth) (the “DNCR Act”) prohibits unsolicited telemarketing calls being made to phone numbers registered on a Do Not Call Register.

1.3 Cybersecurity Regulators

Australia has a range of federal, state and territory regulators and agencies which deal with cybersecurity.

The overarching government agencies are:

- the Department of Home Affairs (DoHA); and
- the Australian Signals Directorate (ASD).

The key regulators and enforcement bodies include:

- the Office of the Information Commissioner (OAIC);
- the Critical Infrastructure Centre (CIC);
- the Australian Communications and Media Authority (ACMA);
- the Australian Securities and Investments Commission (ASIC);

- the Australian Prudential Regulation Authority (APRA); and
- the Australian Competition and Consumer Commission (ACCC).

Specifically in relation to criminal enforcement, the following regulators are key:

- the Australian Federal Police (AFP);
- the Commonwealth Director of Public Prosecutions (CDPP);
- the Australian Security Intelligence Organisation (ASIO);
- the Australian Transaction Reports and Analysis Centre (AUSTRAC); and
- the Australian Criminal Intelligence Commission (ACIC).

Each of the above are addressed below.

Overarching Government Agencies

DoHA

The DoHA is the lead government department for cyberpolicy. The DoHA develops cybersecurity and cybercrime law and policy, implements Australia's national cybersecurity strategy and responds to international and domestic cybersecurity threats and opportunities, including in the areas of critical infrastructure and emerging technologies. The DoHA also has responsibility for cybersecurity and cybercrime operational agencies including the AFP, ACIC, AUSTRAC, and ASIO.

ASD, ACSC and CERT

The ASD is Australia's operational lead on cybersecurity and plays both a signals intelligence and information security role. The ASD undertakes cyberthreat monitoring and conducts defensive, disruption and offensive cyber-operations offshore to support military operations and to counter terrorism, cyber-espionage and serious

cyber-enabled crime. The ASD also advises and co-ordinates operational responses to cyber-intrusions on government, critical infrastructure, information networks and other systems of national significance.

Within the ASD sits the Australian Cyber Security Centre (ACSC). The ACSC drives cyber-resilience across the whole Australian economy including with respect to critical infrastructure, government, large organisations and small to medium businesses, academia, NGOs and the broader Australian community. The ACSC provides general information, advice and assistance to Australian organisations and the public on cyberthreats and it collaborates with business, government and the community to increase cyber-resilience across Australia.

The ACSC also runs the Computer Emergency Response Team (CERT), which provides advice and support to industry on cybersecurity issues affecting Australia's critical infrastructure and other systems of national significance.

Other key government bodies

At this juncture, the following should also be noted.

- The Attorney-General's Department (AGD) advises government on cybersecurity policies and law, including in relation to human rights, privacy, protective security, international law, administration of criminal justice, and oversight of intelligence, security and law enforcement agencies.
- The Department of Defence (DoD) contributes to Australia's whole-of-government cybersecurity policy and operations and houses ASD; it also houses the Information Warfare Division, which develops information warfare

capabilities for the Australian Defence Force (ADF).

- The Department of Foreign Affairs and Trade (DFAT) advances Australia's international cyber-affairs agenda, which includes digital trade, cybersecurity, cybercrime, international security, internet governance and co-operation, human rights and democracy online, and technology for development.

Data Protection and Privacy

The OAIC is the federal privacy and information regulator with a range of functions and powers to investigate and resolve privacy complaints, enforce privacy compliance, make determinations and provide remedies for breaches under the notifiable data breach (NDB) scheme. The OAIC operates by reference to the Privacy Act, the My Health Records Act, the Telecommunications Act, the TIA Act, and recently the Digital ID Act.

The remedies range from enforceable undertakings to civil penalties of 2,000 penalty units (approximately AUD626,000); but may also involve imprisonment. Since December 2022, serious and repeated interferences with privacy may attract a penalty of up to:

- for entities, not body corporates – AUD2.5 million; or
- for body corporates – the greater of AUD50 million, three times the value of the benefit attributable to the conduct or 30% of the adjusted turnover for the relevant period.

There are also state and territory privacy commissioners which administer state and territory-based privacy and health information laws. These include:

- the NSW Information and Privacy Commission who administers, inter alia, the Privacy and Personal Information Protection Act 1998 (NSW) and Health Records and Information Privacy Act 2002 (NSW); and
- the Office of the Victorian Information Commissioner who administers the Privacy and Data Protection Act 2014 (Vic) and the Victorian Health Complaints Commissioner handles breaches of the Health Records Act 2001 (Vic).

Critical Infrastructure Cybersecurity

The CIC is part of the DoHA and is the federal regulator of the SOCI Act and certain provisions of the Telecommunications Act with powers to investigate, audit and enforce on compliance matters.

The CIC also has the ability to make recommendations to DoHA and the Home Affairs Minister on whether their information-gathering powers and directions powers should be exercised. The CIC also has enforcement powers which allows it to issue penalties for non-compliance that range from performance injunctions, enforceable undertakings, civil penalties of up to 250 penalty units (AUD78,250) or seek two years' imprisonment.

Telecommunications, Broadcasting and Marketing Cybersecurity

The ACMA is Australia's regulator for broadcasting, telecommunication and certain online content and provides licensing to industry providers. ACMA has specific regulatory powers under the Telecommunications Act, the TIA Act, the Spam Act, and the DNCR Act to investigate and resolve complaints and enforce compliance. In dealing with non-compliance, ACMA is empowered to issue warnings, infringement notices, enforceable undertakings and remedial directions. ACMA

is further able to cancel or impose conditions on licences and accreditations. ACMA also has the ability to commence civil proceedings or refer matters for criminal prosecution.

Additionally, the Office of the eSafety Commissioner (the “eSafety Commissioner”) has powers to promote and regulate online safety with respect to telecommunications, broadcasting and other online industries. However, the eSafety Commissioner cannot investigate matters of cybercrime. Penalties range from takedown notices and blocking directions.

Corporations, Consumers and Financial Services Cybersecurity

The ASIC is Australia’s corporate, market and financial services regulator, is empowered under the Corporations Act to investigate and bring actions against corporations, directors and officers for non-compliance with the Corporations Act, which, in some circumstances, may involve cybersecurity issues. It regulates publicly listed corporations under the Corporations Act and may investigate issues which touch on cybersecurity.

The APRA regulates certain finance, banking, insurance and superannuation entities and issued information security standards CPS 234. APRA has powers to supervise, monitor and intervene in matters of cybersecurity for regulated entities and has a range of enforcement powers to deal with breaches of its standards. Such powers involve APRA issuing infringement notices, providing directions or enforceable undertakings, imposing licensing conditions, disqualifying senior officials and commencing court-based action.

The ACCC is Australia’s competition regulator and consumer protector, may, where appro-

priate, undertake enforcement action against breaches of the Consumer Act, including breaches involving cybersecurity, cybercrime and cyberscam issues. The ACCC additionally:

- administers the Consumer Data Right (CDR) regime;
- co-regulates (with OAIC) the Digital ID Act; and
- hosts the Scamwatch website which provides public information, alerts and access to complaints mechanisms on a wide range of consumer scams, including scams perpetrated online.

Also relevant for the financial sector is that OAIC regulates the aspects of the Privacy Act which deal with credit reporting obligations and the credit reporting code, which imposes certain conditions on entities that hold credit-related personal information.

Cybercrime

Cybercrime at the federal level is investigated and enforced by the AFP and prosecuted by the CDPP. The AFP have a dedicated cybercrime operations team comprising investigators, technical specialists and intelligence analysts who operate across multiple jurisdictions to conduct cyber-assessments and to triage, investigate and disrupt cybercrime.

More specifically:

- ACIC is Australia’s national criminal intelligence agency – it has broad investigative and coercive powers and shares information between all levels of law enforcement;
- AUSTRAC is the domestic watchdog for Australia’s anti-money laundering and counter-terrorism measures – it supports law

- enforcement operations involving cybercrime financing; and
- ASIO investigates cyber-activity involving espionage, sabotage and terrorism related activities – ASIO also contributes to the investigation of computer network operations directed against Australia’s systems.

State and territory-based police and prosecution agencies investigate, enforce and prosecute state and territory cybercrimes.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

Australia’s critical infrastructure and assets are regulated through Commonwealth, state and territory legislation, with a particular emphasis on the SOCI Act. That said, there is broader legislation, such as the Privacy Act and Cyber Security Act, and more sector-specific legislation, such as the Telecommunications Act, that cannot be ignored.

SOCI Act (and TSSR)

The SOCI Act currently regulates certain assets across eleven sectors: communications, data storage and processing, financial services, energy, food and grocery, health and medical, higher education and research, space technology, transport, water and sewerage, and the defence industry. And from November 2025, telecommunications security obligations (which are currently under the Telecommunication Sector Security Reforms (TSSR)) will be moved into the SOCI, a change implemented by the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024 (Cth) (the “2024 SOCI Amendment Act”).

Notwithstanding recent reforms which clarified the SOCI Act, the exact parameters of the legislation are broad and complex, and extend to various participants in a supply chain including “responsible entities”, “reporting entities”, “direct interest holders”, “managed service providers” and “operators”. Some of these definitions are asset-specific, but for our purposes, it is important to note that a “responsible entity” is generally the entity that owns, is licensed or otherwise responsible for operating the asset.

Further, despite the imminent shift of the TSSR and its obligations to the SOCI Act, these obligations still remain in force and apply to the relevant infrastructure as is. The TSSR are applicable to carriers, carriage service providers and carriage service intermediaries.

Cyber Security Act

Additionally, there are cybersecurity obligations imposed on critical infrastructure under the Cyber Security Act where they constitute “a reporting business entity”.

A “reporting business entity” is an entity that:

- is carrying on a business in Australia with an annual turnover for the previous financial year that exceeds the “turnover threshold for that year” (to be determined) but is not a Commonwealth body, State body, or responsible entity for a critical infrastructure asset; or
- a responsible entity for a critical infrastructure asset “to which Part 2B of the Security of Critical Infrastructure Act 2018 applies”, which is defined in the rules or declaration – at the time of writing, these were prescribed in Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022 (the “SOCI Application Rules”) and includes most infrastructure assets.

2.2 Critical Infrastructure Cybersecurity Requirements

The SOCI Act imposes requirements on owners and operators of assets across various fields. The exact requirements vary depending on the particular asset/industry; however, may include a requirement to:

- register with the Register of Critical Infrastructure Assets;
- provide ownership and operational information;
- notify the government of certain cyber-incidents;
- implement and comply with a critical infrastructure risk management programme (CIRMP); and
- if they have “business critical data” processed or stored by a third party on a commercial basis, they must take reasonable steps to notify that third party.

Further still, the SOCI Act and associated rules impose enhanced cybersecurity obligations on assets designated as “systems of national significance” (SoNS). These must be assets that are already considered a “critical infrastructure asset”, but also that they are of “national significance”. These designations are private and confidential so as to avoid publicising their significance to malicious actors. Reports indicate that over 200 systems have been designated to date.

A responsible entity for a SoNS may be required to:

- fulfil statutory response planning obligations;
- undertake a cybersecurity exercise (see **3.6 Threat-Led Penetration Testing**);
- undertake a vulnerability assessment (see **3.6 Threat-Led Penetration Testing**); and

- where the system is a computer or needs a computer to operate the system, undertake periodic reports, provide event-based reports or install software that transmits system information to the ASD.

It is also worth noting that the SOCI Act also includes:

- an information gathering power for the Secretary of the DoHA to monitor compliance; and
- a directions power for the Home Affairs Minister to direct regulated entities to do or not do a specified thing that is reasonably necessary to protect critical infrastructure from national security risks.

2.3 Incident Response and Notification Obligations

Mandatory Incident Reporting Obligations *SOCI Act*

As mentioned above, the SOCI Act and associated rules impose reporting obligations on various entities.

Responsible entities must report cybersecurity incidents that have a significant or relevant impact on their asset. In other words, a “responsible entity” must make a report when it becomes aware of the following.

- A “cyber security incident” that “has had, or is having, a significant impact (whether direct or indirect) on the availability of the asset” – such a “significant impact” is defined as being where “the incident has materially disrupted the availability of [the] essential goods or service” in connection with which the asset is used to provide. The report must be made “as soon as practicable, and in any event within 12 hours, after the entity becomes aware”. If the initial report is oral, then a writ-

ten report must be made within 84 hours after the oral report is given.

- A “cyber security incident” that “has had, or is having, or is likely to have, a relevant impact on the asset” – such a “relevant impact” is defined (for critical infrastructure assets) as a (direct or indirect) impact on the availability, integrity, reliability of the asset, or on the confidentiality of information about the asset, information stored on the asset or computer data constituting the asset. The report must be made “as soon as practicable, and in any event within 72 hours, after the entity becomes aware. If the initial report is oral, then a written report must be filed within 48 hours of the oral report.

A “cyber security incident” is the:

- unauthorised access to or modification of computer data or computer program;
- unauthorised impairment of electronic communications to or from a computer (but does not include “a mere interception of any such communication”); or
- unauthorised impairment of the availability, reliability, security or operation of computer data, a computer program or a computer.

Either of these reports must be given to the ASD (unless another relevant Commonwealth body is specified in the rules). Failure to make a report at all or in writing, or in the approved form, can each be punished by an AUD16,500 fine.

Cyber Security Act

Irrespective of whether the cybersecurity incident meets the above significance or relevance thresholds, most critical infrastructure assets (being “a reporting business entity”) have additional reporting obligations under the Cyber Security Act.

In summary, there is an obligation to report to the ASD (or other designated Commonwealth agency) where:

- there is a cybersecurity incident that has had, is having, or could reasonably be expected to have a (direct or indirect) impact on a reporting business entity;
- an entity (the extorting entity) demands a benefit; and
- the reporting entity (or a third party on their behalf) makes the ransomware payment.

Such a report must be given within 72 hours of the reporting business entity becoming aware of the payment and must contain certain information.

A “cyber security incident” for these purposes broader than under the SOCI Act as it not only includes any such incident that falls within the scope of the SOCI Act, but is presumed to include any incident:

- involving unauthorised impairment of electronic communication to or from a computer (per the SOCI Act) including mere interception of any such communication; and
- where the incident is (actually or is reasonably expected to be) effected by means of “telegraphic, telephonic or other like service”, if the incident (actually, probably, or it is reasonable to expect it) impeded or impaired “the ability of a computer to connect to such a service” or the incident (probably or is reasonably expected to have) prejudiced Australia’s social/economic stability, defence or national security.

Voluntary Incident Reporting Obligations

The ACSC has a cyber-incident reporting portal through which critical asset owners are encour-

aged to voluntarily report cybersecurity incidents.

Any impacted entity carrying on a business in Australia or otherwise a responsible entity for critical infrastructure is now being statutorily encouraged to make voluntary reports to the NCS Coordinator under the Cyber Security Act, even where it is unclear if an incident is a cybersecurity incident.

Other Mandatory Reporting Obligations

Other reporting obligations under the SOCI Act for critical infrastructure assets include:

- taking reasonable steps to notify a third-party entity if that third party is processing or storing “business critical data” on a commercial basis;
- an ongoing obligation on a “reporting entity” to report a “notifiable event” in relation to an asset usually within 30 days after the event occurs, which relates to changes in the operational information and interest/control information in relation to “director interest holders”, or the status of an entity as a reporting entity; and
- reporting if a hazard had significant relevant impacts on a critical infrastructure asset.

See additionally relevant obligations in **6.1 Cybersecurity and Data Protection**.

Criminal Offences

Related to infrastructure, Part 10.6 of the Criminal Code places obligations on providers of content or hosting services to notify the AFP as to the existence of material displaying “abhorrent violent conduct” (if occurring in Australia) and, in any event, to expeditiously remove or cease to host such material.

2.4 State Responsibilities and Obligations

The Australian government considers “the responsibility for ensuring the continuity of operations and the provision of essential services to the Australian economy and community” as being shared “between owners and operators of critical infrastructure, state and territory governments and the Australian Government”.

Generally speaking, government bodies may also be captured within the scope of legislative regimes such as the Privacy Act, and therefore have the same (or similar) obligations as their private-sphere counterparts. However, the SOCI Act does not apply to the Commonwealth or a body corporate established under Commonwealth law unless so declared or prescribed.

The Australian government is responsible for the “final defence” of Australian infrastructure and cybersecurity. To this end, the SOCI Act grants the Minister last resort “government assistance measures” and powers where a cybersecurity incident relates to a declared national emergency, or else where there is a material risk that a cybersecurity incident has, is or will likely seriously prejudice the Australia’s social or economic stability, defence or national security. These include the heavily circumscribed Ministerial power to request an authorised agency to intervene in relation to computer-related activities where an entity is unwilling or unable to respond to an incident.

Additionally, the Cyber Incident Review Board (CIRB) has been established as an independent statutory advisory body responsible for conducting no-fault, post-incident reviews of significant cybersecurity incidents in Australia. The CIRB post review report will contain recommendations to government and industry about actions

to prevent, detect, respond to or minimise the impact of future cybersecurity incidents of a similar nature.

In pursuit of national cohesion, the state authorities adopt the following approaches.

- The ACSC facilitates information and collaboration across private, public and NGO sectors to develop collective cyber-resilience and to respond to cyber-incidents. In this regard, the ACSC has commenced: a partnership programme, involving private, public, and NGO sectors, to enable information sharing and network hardening; and an alert service, which provides information on recent cyber threats as well as prevention and mitigation advice.
- The Joint Cyber Security Centres (JCSC) are state-based agencies which collaborate with organisations across the private, public and NGO sectors on cybersecurity and cyber-crime threats and response options.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

Even for the financial sector, there is a patchwork of legislation covering the financial sector's operational resilience, leading to variation in scopes. This legislation includes the SOCI Act, the Corporations Act, the Banking Act 1959 (Cth) and the Insurance Act 1973 (Cth).

Corporations Act

As a starting point, the Corporations Act imposes a duty to exercise "care and diligence" on all directors and officers of corporations (Section 180) which inherently involves considerations

relating to cybersecurity resilience. But more specifically, the Corporations Act requires corporations holding financial licences to have adequate risk management systems (Section 912A).

CPS 234

On top of this, APRA's CPS 234 regulates information security standards for APRA-regulated financial, insurance and superannuation entities.

Other Legislation (SOCI Act and Cyber Security Act)

Additionally, other legislation and regulation applicable to sectors beyond the financial is equally relevant here. These include the SOCI Act, since the financial services and markets sector does fall within its scope, so as to include certain banking assets, superannuation assets, insurance assets and financial market infrastructure assets (see **2. Scope of Critical Infrastructure Cybersecurity**). Each of these are, in turn, defined and cover a range of assets owned or operated by entities with certain Australian market licensees, CS facility licensees, benchmark administrators, and more, but most with the underlying condition that the asset is "critical to the security and reliability of the financial services and markets sector".

Those that fall outside the scope of the SOCI Act may fall within the scope of the Cyber Security Act, which imposes reporting obligations on "reporting business entities". See **2. Scope of Critical Infrastructure Cybersecurity**.

3.2 ICT Service Provider Contractual Requirements

Information and communications technology (ICT) service providers are not expressly defined in Australia. However, legislation does address "data processing or storage" assets and providers. Such an asset may be considered itself

a critical infrastructure asset, separate to other critical infrastructure, and therefore fall within the scope of the SOCI Act.

Specifically, an entity that owns or operates a “data storage or processing asset” will be considered a responsible entity under the SOCI Act and their asset “critical” if:

- the entity wholly or primarily provides data storage or processing services that relate to “business critical data”, being “personal information” (per the Privacy Act – see **6.1 Cybersecurity and Data Protection**) relating to at least 20,000 individuals, or otherwise information relating to any research and development, needed to operate, systems needed to operate, or risk management and business continuity in relation to a critical infrastructure asset;
- these services are provided to certain end-users, primarily either:
 - (a) the Commonwealth, a State, a Territory, or a body corporate established under such a Commonwealth, State or Territory law; or
 - (b) the responsible entity for a critical infrastructure asset;
- the entity knows that the asset is used by the above end-user; and
- the asset does not constitute another critical infrastructure asset.

Further, the 2024 SOCI Amendment Act clarified the SOCI Act so that it included secondary assets who hold business critical data relating to the primary asset. Notably, the intent behind these amendments is not to capture all non-operational systems holding business critical data; rather only those where vulnerabilities could significantly impact critical infrastructure assets. Examples of relevant operational data

included network blueprints, encryption keys, algorithms, operational system code, and tactics, techniques and procedures.

The regulations may specifically exclude other such assets. See **2. Critical Infrastructure Cybersecurity** for their obligations and responsibilities.

3.3 Key Operational Resilience Obligations

There is no specific legislation for “digital operational resilience” for the financial sector as seen in the European jurisdictions; however, the objectives of enabling the financial sector to be or remain resilient in the face of serious operational disruption and prevent/mitigate cyberthreats are reflected in the patchwork of legislation.

SOCI

Specifically looking at the obligations under the SOCI Act for the financial sector, although financial business using or constituting critical infrastructure assets have the same incident reporting obligations already covered (see **2.3 Incident Response and Notification Obligations**), such services do not have the obligations to register as critical assets and to have a CIRMP under the SOCI Act (except where they are “payment services”).

As an aside, a financial service can be classified as a SoNS under the SOCI Act, attracting the enhanced cybersecurity obligations.

Corporations Act

Notwithstanding the position under the SOCI Act, financial services are likely already required to be registered with APRA and/or obtain a form of financial service licensing; and in doing the latter, must, inter alia, provide their services

“efficiently and fairly” and have an adequate risk management program. Australian courts have already confirmed that such a risk management plan must ensure adequate cybersecurity and cyber-resilience measures are adequately implemented across its business.

CPS 234

APRA’s CPS 234 requires APRA-regulated financial, insurance and superannuation entities to comply with legally binding minimum standards of information security, including by:

- specifying information security roles and responsibilities for the entities’ board, senior management, governing bodies and individuals;
- implementing and maintaining appropriate information security capabilities;
- maintaining tools to detect and respond to information security incidents in a timely way; and
- notifying APRA of any material information security incidents.

These standards provide that an entity’s board is ultimately responsible for information security and that the board must ensure that its entity maintains information security in a manner that is commensurate with the size and vulnerability of that entity’s information assets.

APRA-regulated entities are required to externally audit their organisation’s compliance with CPS 234 and report to APRA in a timely manner.

If organisations are non-compliant, they may be required to issue breach notices and create rectification plans. If organisations are unable to comply with the standards following this process, APRA may undertake a more for-

mal enforcement process which may include enforceable undertakings or court proceedings.

Cyber Security Act

In addition to the reporting obligations under the CPS 234, certain responsible entities concerning “critical financial market infrastructure asset” (2.1 Scope of Critical Infrastructure Cybersecurity Regulation) also have ransomware reporting obligations under the Cyber Security Act (see 2.3 Incident Response and Notification Obligations).

3.4 Operational Resilience Enforcement

As at the time of writing, there was no enforcement action against “data processing or storage” providers or other ICT services. In fact, there has been no enforcement action reported in relation to the SOCI Act.

According to CISC’s Compliance and Enforcement Strategy published in April 2022, the CISC prioritises industry partnership and pursues a co-operative, educative and overall voluntary approach. Although it has a range of regulatory options available, it is yet to use any penalising enforcement action.

Depending on the breach, action against ICTs may also come from other regulators such as the OAIC.

3.5 International Data Transfers Government Transfers

Although there are limits on the use of the cybersecurity information provided by reporting business entities under the Cyber Security Act and Intelligence Services Act 2001 (Cth), these limitations are unlikely to prevent the ASD, National Cyber Security Coordinator (NCS Coordinator) or CIRB from disclosing the information to foreign authorities or joint partnerships for particu-

lar purposes. For example, where information is voluntarily provided in relation to a significant cybersecurity incident, the NCS Coordinator disclose this information in “coordinating the whole of Government response” or otherwise to inform Commonwealth ministers; who may then disclose this information for a “permitted cybersecurity purpose” such as mitigating material risks that prejudice Australia’s social/economic stability, defence or national security. This may include sharing and international transfers of information to foreign authorities or co-ordinated partnerships.

Market Transfers

Privacy Act

The primary legislation governing data transfers in Australia is the Privacy Act, which was relevantly amended by the Privacy and Other Legislation Amendment Act 2024 (Cth) (the “2024 Privacy Amendments”) on 29 November 2024.

Prior to these amendments, international (cross-border) disclosures of personal information were addressed primarily by APP 8. This principle required APP entities to “take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles”. What is “reasonable” depends on one’s specific circumstances but will usually involve a contract incorporating the APPs and the Australian entities monitoring or at least assessing the overseas entity’s systems. Importantly, APP 8 is not limited to where there is active transfer of data but rather extends to wherever data is accessible to an overseas entity (eg, stored on servers in Australia, but accessible by overseas entities).

The 2024 Privacy Amendments introduces an adequacy regime, meaning there is now a mechanism by which the Government can prescribe

a “white list” of countries and binding schemes that are recognised as being on par with APP 8.

Consumer Data Right

In respect of data transfers more generally, Part IVD of the Consumer Act regulates the handling (including sharing) of CDR. The CDR was rolled out to the banking and energy sectors in 2020 and 2022 respectively. Although it was to continue into the superannuation, insurance and telecommunications sectors (and then into the non-bank lenders and Buy Now Pay Later products), the government paused the roll out in 2023, commissioned a report in August 2024 (which found that compliance costs exceeded initial estimates) and is now considering amendments to “reset” the CDR, involving the simplification of the customer consent process and the encouragement of operational enhancements to reduce the barriers to participation in the CDR.

Prohibitions

Certain information is prohibited from being held or taken outside Australia, such as records held for the purposes of the My Health Record system. Breach of this prohibition could result in a maximum criminal penalty of five years imprisonment and AUD99,000; or a civil penalty of AUD495,000.

Cybercrime

For completeness, it should also be noted that unauthorised access to computer systems (hacking, forceable transfers, etc) is criminalised by both State and Federal legislation. For example, persons suspected of unauthorised access to computer systems are charged pursuant to Section 478.1 of the Criminal Code, which provides for the offence of “Unauthorised access to, or modification of, restricted data”.

These offences have extraterritorial application, meaning that conduct undertaken outside Australia can still be charged and prosecuted under Australian law if:

- the crime involves conduct both inside and outside Australia;
- the crime results in harm within Australia;
- the offender is an Australian citizen, or a corporation incorporated in Australia; or
- the crime is related to another crime that occurred in Australia.

Other legislation

In addition to the above, the following existing and potential legislation is relevant to data transfers, including those that are cross-border.

- In December 2024, the Digital ID Act and the Digital ID (Transitional and Consequential Provisions) Act 2024 (Cth) commenced that, inter alia, restrict an accredited entity on the collection, use and disclosure of biometrics and other personal information. The Digital ID Rules are to also address the storing and transfer of information outside Australia and are expected to take the form of blanket prohibitions, with an exemption application process.
- The Australian Treasury's action has stalled since 2023 when it announced that a formal ban on "screen scraping" or "digital data capture" (ie, collection of displayed data for various uses) in the banking sector was being considered. There are continuing concerns of the protection of screen scraped data, and how existing legislation applies to its handling or transfers.

3.6 Threat-Led Penetration Testing

Threat-led penetration testing (TLPT) is the testing of systems by replicating the methods used

by actual threat actors against. Generally speaking, TLPT is not a requirement in Australia.

Currently, only those critical infrastructure assets designated as a SoNS may be required to undertake:

- a "cyber security exercise", the purpose of which is to test the entity's ability to respond appropriately, preparedness to respond appropriately, and ability to mitigate the relevant impacts, and thereafter prepare an internal report, which can in turn, be audited; and
- a vulnerability assessment, the purpose of which is to test system vulnerabilities to the relevant cybersecurity incident, and thereafter prepare a vulnerability assessment report.

TLPT is also a component of regulatory guidance (eg, ASD's best practices for deploying secure and resilient AI systems).

On the flipside, unsolicited/unauthorised penetration testing activity could be captured by Section 478.1 of the Criminal Code, which provides for the offence of "[un]authorised access to, or modification of, restricted data".

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

There is no specific legislation for cyber-resilience in Australia.

However, cyber-resilience requirements have legislative status across various contexts, including:

- the risk management programmes required by the legislation already discussed under the

SOCI Act for responsible entities of critical infrastructure assets (**2.2 Critical Infrastructure Cybersecurity**) and the Corporations Act for financial licensees (**3.3 Key Operational Resilience Obligations**);

- other obligations on certain responsible entities concerning TLPT-like requirements (**3.6 Threat-Led Penetration Testing**); and
- the data protection standards for various types of information such as “personal information” (**6.1 Cybersecurity and Data Protection**) and the healthcare sector (**6.3 Cybersecurity in the Healthcare Sector**).

Further, the Cyber Security Act provided a framework by which the Minister can prescribe mandatory rules for smart devices, which seeks to replace the 2020 voluntary Code of Practice: Securing the Internet of Things for Consumers. The details of the framework are still yet to enter into law, but it will apply to products that are either “internet-connectable” or “network-connectable”, subject to certain exceptions relating to laptops, medical devices and cars. This framework will be primarily targeted towards manufacturers and suppliers of these devices.

4.2 Key Obligations Under Legislation

Cyber-resilience obligations are imposed on certain responsible entities of critical infrastructure asset by way of the Critical Infrastructure Risk Management Program, which must be adopted, reviewed and updated. The purpose of these programmes is to identify each hazard with a material risk and minimise, eliminate or mitigate that hazard (or its material risk). The relevant responsible entities and specific requirements for these programmes are set out in the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023.

In respect of smart devices, according to the CISC’s explanatory document outlining the Cyber Security (Security Standards for Smart Devices) Rules, their cyber-resilience obligations will include mandatory obligations relating to passwords, procedures to report security issues, support period for security updates, as well as voluntary labelling schemes. However, the regulations are yet to be passed.

Other cyber-resilience obligations for critical infrastructure, the broader financial sector and others are discussed elsewhere in this chapter.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

There is no single legislation in Australia addressing broad-sweeping information technology and cybersecurity (ITC) certification procedures.

However, ITC-relevant certification provisions are relevant to the SOCI Act. Specifically, where a responsible entity holds a certain “certificate of hosting certification (strategic level)” that relates to its critical infrastructure asset, that entity is exempt from needing a critical infrastructure risk management programme. This certificate must be issued under a scheme that is administered by the Commonwealth and known as the hosting certification framework.

At the time of writing, this framework was only available to data centre providers and cloud service providers; and approximately 11 data centre facilities and 14 cloud services were certified.

For additional context, since 30 June 2022, all government contracts for hosting services must

be with certified service providers. However, this policy requirement is not restricted to “strategic level” certification per the SOCI Act. Under this framework, there are three certification “strategic”, “assured” and “uncertified”. Depending on a government department’s risk profile and data set, they may contract with a “Certified Assured Service Provider”.

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection The Privacy Act

Scope

Federally, data containing personal information is protected under the Privacy Act, which regulates the handling of this information by “APPs entities”.

At this juncture, it is important to note two definitions.

- “Personal information” under the Privacy Act is defined broadly as information or an opinion about an identified or reasonably identifiable individual. It is not required to be true or recorded in a material form. Personal information also includes “sensitive information”, which includes information or opinions on an individual’s race, ethnicity, politics, religion, sexual orientation, health, trade associations and criminal records. Sensitive information is often afforded a higher level of protection than other personal information.
- “APP entities” are, subject to some exceptions, federal government agencies, private sector organisations with an annual turnover of over AUD3 million and smaller entities with data-intensive business practices (including private health providers, businesses that sell

or purchase personal information and service providers to the federal government).

Schedule 1 of the Privacy Act contains 13 APPs, which are minimum standards for processing and handling personal information by APP entities. The Privacy Act also requires mandatory reporting for certain APP breaches under the NDB scheme. Breaches of the Privacy Act may result in investigation and enforcement action by the OAIC.

Reporting obligations (the NDB scheme)

The NDB scheme requires APP entities to notify both affected individuals and the OAIC where there are reasonable grounds to believe that an “eligible data breach” has occurred. In short, as per Section 26WE(2) of the Privacy Act, an “eligible data breach” occurs where:

- there is unauthorised access to/disclosure of personal information and a reasonable person would conclude that this “would be likely to result in serious harm to any of the individuals to whom the information relates”; or
- personal information is lost in circumstances where a reasonable person would conclude that unauthorised access to/disclosure of it is likely to occur and, were it to occur, it “would be likely to result in serious harm to any of the individuals to whom the information relates”.

However, Section 26WF of the Privacy Act creates an exception to reporting such an incident, where the entity in question takes remedial action to ensure that the breach does not cause serious harm to the individuals concerned.

Notably, specific data breaches related to certain health records are excluded from this scheme and are to be addressed under Section 75 of the

My Health Records Act (see **6.3 Cybersecurity in the Healthcare Sector**).

The ACSC provides an overarching definition for cybersecurity events in its Guidelines for Cyber Security Incidents. In these Guidelines, a cybersecurity event is “an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security”. While there is no general legislative definition of a cybersecurity event, the SOCI Act, at Section 12M, provides a limited, more complex definition.

Statutory tort

Also, it is important to note here that the 2024 Privacy Amendment introduced a statutory tort for serious invasions of privacy, giving individuals a route to seek redress for privacy harms in the courts.

State and Territory Reporting Obligations

There are also schemes at the state/territory level. For example, both NSW and Queensland had introduced mandatory notification of data breach schemes via, respectively, the Privacy and Personal Information Protection Amendment Act 2022 (NSW) (entered into force 28 November 2023) and Information Privacy and Other Legislation Amendment Act 2023 (Qld) (commencement date to be set by proclamation). These largely mirror the federal scheme.

Other Reporting Obligations

There is other relevant legislation for data protection and reporting obligations, including in relation to certain health records (see **6.3 Cybersecurity in the Healthcare Sector**), financial sector (**3. Financial Sector Operational Resilience**) and critical infrastructure assets (**2. Critical Infrastructure Cybersecurity**).

6.2 Cybersecurity and AI

At the time of writing, there is no AI-specific regulation on AI; however, there is a patchwork of laws regulating critical infrastructure, privacy, consumer protection, data security and more that all touch on aspects of AI development and use.

Further, Australia has voluntary instruments, including:

- ethical frameworks, including the Australia’s AI Ethics Principles, that has been supplemented on 15 June 2023 by NAIC’s Implementing Australia’s AI Ethics principles: A selection of responsible AI practices and resources; and
- a voluntary AI Safety Standard released on 5 September 2024, comprising practical guidance in the form of ten “AI guardrails”.

Similarly, regulators ASD, in conjunction with foreign authorities such as the U.S. National Security Agency’s Artificial Intelligence Security Center, has published guidance on deploying, engaging with and developing AI systems. Further, the ASD has endorsed the Cybersecurity Performance Goals (CPGs) developed by the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST).

6.3 Cybersecurity in the Healthcare Sector

Reporting Obligations

Certain data breaches relating to My Health Record information or the system itself are to be reported under Section 75 of the My Health Records Act (rather than through the NDB scheme under the Privacy Act).

Section 75 of the My Health Records Act requires a report where there has (actually or potentially) been unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record or the (actual or potential) compromise of the security or integrity of the My Health Record. Such a report must be made to the relevant system operator and/or the OAIC. Subsequently, all "affected healthcare recipients" must also be notified of the compromise or unauthorised disclosure.

Other than those data breaches to which the My Health Records Act applies, medical data would generally be personal information and covered by the federal NDB scheme (see **6.1 Cybersecurity and Data Protection**).

Trends and Developments

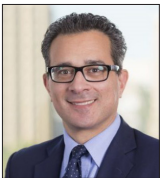
Contributed by:

Dennis Miralis and Jack Dennis
Nyman Gibson Miralis

Nyman Gibson Miralis is a market leader in all aspects of general, complex and international criminal law and is widely recognised for its involvement in some of Australia's most significant cases. The firm's team in Sydney has expertise in dealing with complex national and international cybercrime investigations and advising individuals and businesses who are the

subject of cybercrime investigations. Its expertise includes dealing with law enforcement requests for information from foreign jurisdictions, challenging potential extradition proceedings as well as advising and appearing in cases where assets have been restrained and confiscated worldwide.

Authors



Dennis Miralis is a partner at Nyman Gibson Miralis and a leading Australian defence lawyer who specialises in international criminal law, with a focus on complex multi-

jurisdictional investigations and criminal prosecutions. His areas of expertise include cybercrime investigations, anti-bribery and corruption, global tax investigations, proceeds of crime, anti-money laundering, worldwide freezing orders, national security law, INTERPOL Red Notices, extradition and mutual legal assistance law. In 2021 Dennis was awarded a certificate of completion for the "Cybersecurity: The Intersection of Policy and Technology" programme, January 2021, John F. Kennedy School of Government at Harvard University, Executive Education.



Jack Dennis is a senior criminal defence lawyer who practises in international and domestic criminal, corporate and tax law at Nyman Gibson Miralis. His international criminal work

includes transnational criminal and regulatory investigations, liaising with foreign legal and regulatory bodies, as well as advising clients on matters concerning international public law. Domestically, Jack has advised on a range of criminal issues and investigations, including white-collar crime, fraud, sanctions, INTERPOL, extraditions and national security. He also has significant international, corporate and tax experience, having advised on cross-border transactions and disputes involving foreign and domestic corporations and individuals, across the software, financial services and crypto industries.

Nyman Gibson Miralis

Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 292 648 884
Email: dm@ngm.com.au
Web: www.ngm.com.au



Introduction

Since releasing the 2023-2030 Australian Cyber Security Strategy (the “CS Strategy”) on 22 November 2023, the Australian government has pursued sweeping reforms to address the gaps in cybersecurity. The government aims to become “a world leader in cybersecurity by 2030”; however, the effectiveness of these actions and reforms still remains to be seen. For 2025, the actual impact of the 2024 reforms remains to be seen in the still-patchwork style legislative landscape and the Australian government continues to play catch-up with both technology and other countries as it with an eyes the “frontier”.

The CS Strategy is aimed at strengthening Australia’s cyberdefences and supporting people and businesses to be resilient to and recover quickly from cyber-attacks. Grounded in the 2023-2030 Australian Cyber Security Strategy: Action Plan (the “Action Plan”), the CS Strategy is planned out across three “Horizons” targeting six “shields” or “layers of defence”. Currently, Australia is in the final (albeit second) year of Horizon 1 (“Strengthen our foundations”) whereby it is aiming to address critical gaps, build protections and support “initial cyber maturity uplift”, with the government’s performance target being 75% of department-led activities to

be on track. The government is setting itself up for Horizon 2 (“Expand our search”) come 2026, which aims to scale cyber maturity across the whole economy, make investments and grow a diverse cyber workforce.

In its pursuit of the cyber frontier, the Australian government introduced the Cyber Security Bill 2024 (Cth) as part of the Cyber Security Legislative Package 2024, involving a number of updates to existing legislation. This bill is Australia’s first standalone cybersecurity legislation, but reflects largely what has been seen in the UK, Europe and other jurisdictions. This reform occurred in a long line of changes that have preceded 2024. Overall, 2024 can be categorised as another year of change for the cybersecurity space, illustrating the fast pace of the technologies and malicious actors, the delayed yet quickening pace of the government, and the inherent but necessary gap between implementation and enforcement to accommodate the slow adoption of these laws and regulation throughout many industries.

Despite the success of law enforcement, such as Operation Cronos, cyber vulnerabilities are becoming more and more critical, as demonstrated by ransomware attacks such as against UnitedHealthGroup in February 2024 or even

software upgrades gone wrong as in the case of CrowdStrike-Microsoft Outage in July 2024. Attacks by state-sponsored and independent actors are only set to increase. And the importance of effective cybersecurity laws and protections is becoming ever-more critical.

Threat Landscape

Victim typologies

The Australian Signals Directorate's (ASD) Annual Cyber Threat Report for 2023-24 (the "ASD 2023-24 Report") confirmed that the "top 5" sectors reporting cyberthreats remained the same as FY2022-23: federal government, state/local governments, healthcare, and tied fifth were education, professional/scientific services, utility services and information/telecommunications services. Yet vulnerabilities beyond these sectors cannot be understated.

The ASD 2023-24 Report flagged that the ASD responded to 11,000 cybersecurity incidents and received over 87,400 cybercrime reports (which was, in fact, a drop of 7%). The crime trends differ amongst targets:

- for individuals, self-reported cybercrimes comprised identify fraud (26%), online shopping fraud (15%) and online banking fraud (12%);
- for businesses, it was email compromise (20%), online banking fraud (13%) and business email compromise fraud (13%); and
- for critical infrastructure, it was compromised accounts or credentials (32%), malware infection (excluding ransomware) (17%), and compromised asset, network or infrastructure (12%).

With the government's focus primarily being on critical infrastructure, there remains a growing concern that small businesses are low-hanging

fruit: vulnerable, ill-prepared, and are being increasingly targeted. Yet, most small businesses are exempt from basic statutory obligations such as the Privacy Act 1988 (Cth) (the "Privacy Act"). Immediate resourcing and compliance costs must be weighed against costs and damage of potential attacks.

Increasing efficiency of attacks

Attacks are becoming more efficient and sophisticated. This capacity strengthening is due, in part, to AI; however, such developments may also assist countermeasures. In recognition of this double-edged sword, the ASD has published resources for businesses and government, including Best Practices for Deploying Secure and Resilient AI Systems.

Similarly, the ASD recently confirmed that 2023 saw a rise in zero-day vulnerabilities (ie, exploitation of an unknown vulnerability, which developers have had "zero days" to address). Overall, this emphasises the need for the proactive "stance of 'when' not 'if' a cybersecurity incident will occur", as well as a pre-emptive approach such as with the secure by design principles.

State-sponsored attacks

Regulators noticed:

- state-sponsored actors targeting supply chain compromises;
- PRC state-sponsored actors' "increasingly emerging" living off the land (LOTL) techniques, "pre-positioning" themselves on or adjacent to critical infrastructure networks "for disruptive effects rather than traditional cyber espionage operations"; and
- Russian-sponsored actors adapting their operations to match industry shifts to cloud-based infrastructure.

State-sponsored cyber-operations are set only to increase with growing geo-political tensions, including the competition in the Indo-Pacific. As we continue to see sanctions, states may co-opt actors and state hacking itself to supplement revenue streams.

Other risks/vulnerabilities

Overall, it is important to acknowledge that the vulnerabilities are not only from external malicious actors. Incidences that occurred in 2024 highlight other critical focus points, such as the following.

- **Insider threats:** in October 2024, Qantas confirmed that two contractors working for Air India SATS company had allegedly accessed at least 800 customer booking details and diverted their frequent flyer points. As this India SATS provides services to a lot of airlines across the OneWorldAlliance, the true extent of the issue may never be known.
- **Software issues:** in July 2024, CrowdStrike released an update that caused worldwide outages of certain programs.

Legislative and Regulatory Reform

In 2024, the Australian government passed the Cyber Security Act package, introducing a range of new legislative reforms; some of which are explored below. Overall, these changes pave the way for better-informed government actions as well as increased enforcement actions to raise the general standard of Australian businesses across the board.

SOCI Act

The Security of Critical Infrastructure Act 2018 (Cth) (the “SOCI Act”) regulates the critical infrastructure assets identified across eleven sectors, and was amended in November 2024 by the Security of Critical Infrastructure and Other Leg-

islation Amendment (Enhanced Response and Prevention) Act 2024 (Cth) (the “SOCI Amendment Act”).

The SOCI Amendment Act included:

- crucial clarifications on the status of data storage systems;
- amendments to what is protected information, as well as exemptions to the prohibitions on the use and disclosure of such information; and
- new regulatory powers for “seriously deficient” Critical Infrastructure Risk Management Programs (CIRMP).

The shared-responsibility for and complexities of a single business’ CIRMP and cybersecurity overall is demonstrated by the media’s coverage of the back-and-forth between Delta Air Lines and CrowdStrike after the former commenced proceedings against the latter for damages caused by the CrowdStrike-Microsoft outage in July 2024. Delta claimed, inter alia, that CrowdStrike “cut corners, took shortcuts, and circumvented the very testing and certification processes it advertised”; while CrowdStrike retorted that Delta has had a “slow recovery away from its failure to modernise its antiquated IT infrastructure”. Both businesses and service providers have responsibilities under a capable CIRMP. It remains to be seen if this specific matter progresses further.

The importance of reviewing and properly implementing these changes is only increased by the continued stance taken by the Department of Home Affairs (DoHA) under its performance targets. Target 8 comprises that 100% of instances of identified non-compliance with obligations in the SOCI Act will be subject to a compliance action within 90 days. The precise “compliance

action” will be determined by CISC’s Compliance and Enforcement Framework “and the published regulatory posture”. Watch this space.

Cyber Security Act

The Cyber Security Act was an Australian-first: legislation specifically aimed at cybersecurity. It introduced standards for smart devices, new reporting obligations, and also established two new roles:

- the National Cyber Security Coordinator (NCSC) responsible for co-ordinating whole-of-government action in response to significant cybersecurity incidents, policies and capabilities; and
- the Cyber Incident Review Board (CIRB), an independent advisory body that will undertake reviews of certain cybersecurity incidents on a no-fault basis.

Information-gathering routes under the Cyber Security Act include:

- obligatory ransomware reporting: see below;
- CIRB compulsive powers: the CIRB has the power to compel information and documents from entities believed to be “involved in a cyber security incident” (subject to a request for information having been made); and
- voluntary reporting: see below.

Information-gathering: ransomware reporting

2021-22 research suggests only one in five Australians are reporting ransomware attacks to authorities. This statistic undoubtedly needs updating with the increased prevalence of attacks and access to technology.

The Cyber Security Act mandated reporting when ransomware payments (or other benefits) are demanded for certain entities. This obliga-

tion joins the ranks of a slowly growing set of confined reporting obligations. This currently includes those imposed on critical infrastructure assets in respect of certain cybersecurity incidents (irrespective of ransomware payments) under the SOCI Act; on APRA-regulated entities in respect of material information security incidents. Outside these regimes, the Australian government relies on their own detection of such incidents, and more likely, voluntary reporting.

This ransomware obligation is just one more confined patch in Australia’s patchwork of obligations. This obligation is imposed only on a “reporting business entity”, which is defined by reference to the Australian business’ previous year’s turnover (the number undetermined at writing) or by being specific critical infrastructure assets. Therefore, the true extent to which these new obligations will be felt across Australian businesses (beyond critical infrastructure) remains to be determined (by the yet-to-be-published rules). The threshold will likely be determined with reference to the cybersecurity threat landscape as well as the compliance capabilities, costs and other burdens on Australian businesses. Speculatively, this may match the threshold under the Privacy Act, so as to include small businesses. This set-up grants the Australian government flexibility to adjust obligations according to the perceived needs but will likely result in a gap in the obliged reporting where there is a ransomware. That is without even acknowledging that these obligations only arise where there is a “ransom” demanded in the first place (albeit irrespective of the type of benefit, not only payments; and also irrespective of actual payment of the demand).

This piece is just one of many that makes up the puzzle of Australia’s cybersecurity and attempts to balance several aspects including security,

compliance burden and costs. Nevertheless, it will likely still see a lot of incidents pass under the radar, leaving a widespread and fertile ground for malicious actors to test ransomware largely undetected and non-ransomware cyber-incidents more generally. With no safe harbour protections and heightening reputational concerns over breaches, an over-reliance on voluntary reporting may be insufficient.

Use of reports and other data shared

A key premise of Australia's strategy in obtaining information on incidents is to better understand vulnerabilities/targets, methods and techniques, and ultimately generate tools and strategies to proactively and reactively respond to future incidents. Australia has sought to increase the open and frank communications of ransomware reporting by restricting the use of the information. These purposes primarily relate to responding to, mitigating or resolving cybersecurity incidents. How far these express purposes extend may be the subject of future proceedings.

Taking a closer look at ransomware reporting, the Act implements "limited use" obligations on the bodies who receive the information (primarily or secondarily). In doing so, the Act excludes the use of the information for investigations or enforcement action unless it is a contravention of the reporting obligations themselves or a law attracting "a penalty or sanction for a criminal offence". This prevents the information from being used in most regulatory enforcement actions, but leaves the entities exposed to criminal law provisions. While individuals (including directors) may be able to rely on the privilege against self-incrimination where criminal law issues become live, the business entity itself is unlikely to have such protections given corporate entities do not have such a privilege under Australian law. Public suggestions of including

a safe harbour provision were dismissed by the Australian government. In fact, the government expressly stated the intention was not to "shield a reporting entity from legal liability" or "to restrict law enforcement [...] from gathering this information through another passage using their own existing powers" raising the concern of secondary methods of obtaining the obligatorily shared information by even civil regulators. This may complicate compliance with this obligation, particularly should the Australian government rely on criminal sanctions (alone or as alternatives to civil penalties) to enforce cybersecurity legislation.

There are expanded protections for any information voluntarily provided to the NCSC concerning an actual or potential cybersecurity incident, with Section 42 rendering such information inadmissible in criminal proceedings (except very specific circumstances) and any "proceedings for breach of any other Commonwealth, State or Territory law (including the common law)". Yet, these protections do not prevent authorities from obtaining the information via other methods and relying on it thereafter.

Online Safety Act

Surpassing the ranks of Russia's ban of Discord and the United States' (incredibly short) ban of TikTok, Australia passed a world-first age restriction on social media platforms for those under 16 years by introducing the Online Safety Amendment (Social Media Minimum Age) Act 2024 (Cth). The obligation is to take "reasonable steps" to prevent age-restricted users from having an account, but will impose restrictions on the kind of information that can be collected and how this information is stored, used and protected. Specific platforms are still to be confirmed, but the government initially intends to include Snapchat, TikTok, Facebook, Instagram

and X; while excluding messenger, online gaming, health and educational-focused services. Any platforms where an “account” is not needed (eg, Youtube) will not be caught.

Privacy Act

On 28 September 2023, the Australian government published its response to the Attorney-General’s Department’s Privacy Act Review Report (the “Review”). The Review contained 116 proposals to amend the current Privacy Act 1988 (Cth) (the “Privacy Act”) to better align Australia’s privacy laws with global standards of information privacy protection.

Of the 116 proposals in the Report, the government has “agreed” to 38 proposals and “agreed in-principle” to 68 others.

A year later, and Australia has seen the first tranche of resulting reforms. The Privacy and Other Legislation Amendment Act 2024 (Cth) took effect on 10 December 2024, and:

- introduces a new tort for serious privacy invasions;
- expands Office of the Information Commissioner’s (OAIC) enforcement powers, including information-gathering powers concerning actual or suspected eligible data breaches;
- introduces the long-awaited automated decision-making requirements;
- introduces an adequacy regime (a “white list”) specifying jurisdictions with which Australian companies may more freely share data;
- criminalises doxing; and
- clarifies that APP11 of the APPs (Australian Privacy Principles) (ie, APP entities must take active measures to ensure the security of personal information it holds) includes both technical (eg, IT expertise) as well as more general organisational training.

The Attorney-General’s Department has indicated that it will start consulting on the second tranche of privacy reforms soon, which will likely reflect the remaining proposals that were “agreed”, and potentially those “agreed in-principle”.

Reflections on the Anti-Encryption Legislation

In a world-first initiative, the Telecommunications (Assistance and Access) Act 2018 (Cth) granted the Department of Home Affairs the power to request or compel assistance from telecommunications providers and technology companies in accessing encrypted communications, such as Technical Assistance Requests (TARs).

According to evidence from the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in 2020, the Australian Security Intelligence Organisation (ASIO) has issued “fewer than 20” TARs, the AFP has issued eight, and the New South Wales Police Force has issued 13. At this point, these requests were (reportedly) complied with on the most part (if not all).

Since then, the ASIO Director has stated that “encryption damages intelligence coverage” in all priority counter-terrorism and counter-espionage cases; but instead of flagging an increased use of these powers, has called for “tech companies to do more [...] to give effect to the existing powers and to uphold existing laws”. This tact calls into question the utility of the powers and authorities’ capacities to properly wield them.

Responses, Investigations and Enforcement Sanctions

On 23 January 2024, Australia imposed a cyber sanction under the Autonomous Sanctions Act 2011 (Cth) on Russian national Aleksandr Erma- kov for his role in the compromise of Medibank Private in 2022. This sanction was the first such

use of the significant cyber-incidents sanctions regime established on 21 December 2021.

Since then, four more individuals have been added to the list for their involvement in LockBit and Evil Corp cybercrime groups.

Financial sanctions under the Sanctions Act now make it a criminal offence, punishable by up to ten years' imprisonment and heavy fines, to provide assets to designated individuals or to use or deal with his assets, including through cryptocurrency wallets or ransomware payments. The designated persons are also banned from travelling to or remaining in Australia.

Although ransomware payments are not illegal, the juncture between cyber sanctions and ransomware payments requires further consideration. Currently, the Department of Foreign Affairs and Trade (DFAT) encourages all such payments to be reported (mandatorily or voluntarily), and states that such disclosure "would be taken into account in any decision to pursue any enforcement or compliance action".

The crossover between cybersecurity and sanctions has continued to increase. DFAT has identified in their Advisory Note – Democratic People's Republic of Korea (DPRK) information technology (IT) workers (14 December 2024) a recent tactic by the Democratic People's Republic of Korea (DPRK) to deploy thousands of information technology professionals to seek remote employment (posing as non-DPRK nationals) to illicitly finance the DPRK and circumvent sanctions. At a time when many industries are looking to establish cybersecurity structures and compliant procedures, more and more are hiring or outsourcing these services (some reports suggest 76% of leading global businesses do so),

potentially making them more vulnerable (eg, accessible, desperate) to other legal risks.

ASIC mandate

In November 2023, the chairperson of the Australian Securities and Investments Commission (ASIC), Joe Longo, stated that ASIC's priority for 2024 would be addressing governance and breach of directors' duties following the results of ASIC's 2023 Cyber Pulse Survey. As a snapshot, the survey found significant gaps in Australia's corporate security, with:

- 44% of participants failing to manage cyber-risks posed when dealing with third parties;
- 58% of participants having limited or no capability to adequately protect confidential information;
- 33% of participants not having a cyber-incident response plan; and
- 20% of participants not having adopted cybersecurity standards.

This was speculated to include ASIC prosecuting directors or officers for breaches of directors' duties concerning cybersecurity breaches. However, there was limited outward action on this front in 2024.

Nevertheless, a change may be afoot. At the ASIC Annual Forum on 14 November 2024, the ASIC deputy chairperson, Sarah Court, confirmed ASIC is "considering a range of matters where we consider [financial services and credit] licensees may have not adequately prepared for [cybersecurity] events". There, Court announced that ASIC's 2024 priority of action against financial service licensees who fail to comply with reporting obligations was out, to make way for ASIC's new 2025 priority of action against financial service and credit licensee's failures to have adequate cybersecurity protections. One

would expect this new priority will build on the 2022 Federal Court decision of *ASIC v RI Advice Group Pty Ltd* [2021] FCA 1193.

This change signals a potentially bigger shift. Data breaches and cybersecurity issues have generally been regulated from a privacy perspective by the Office of the Australian Information Commissioner (OAIC). This area may be a hot spot to watch for regulator “pile-ons”.

CISC audits

The Cyber and Infrastructure Security Centre (CISC) considered 2022-2023 a learning and familiarisation period with the introduction of the Security of Critical Infrastructure (Application) Rules 2022. Then, in 2024, the CISC shifted its compliance focus from one primarily of education and awareness raising (2023-24) to a balance of education/awareness and compliance activities (2024-25). The SOCI Compliance Regulatory Posture was updated. In making this shift, the CISC conducted a limited series of trial audits with certain responsible entities “to test our processes for determining industry compliance with SOCI Act obligations”. The CISC has also announced that a formal audit programme to evaluate compliance with SOCI obligations will commence in 2024-2025.

2024 marked the first year that responsible entities (under the SOCI Act) were required to file annual reports per the SOCI (Critical infrastructure risk management program) Rules (LIN 23/006) 2023 (CIRMP).

OAIC determination and guidance on facial recognition

On 19 November 2024, the OAIC published a determination finding that retail chain Bunnings breached the Privacy Act 1988 (Cth) through its practices of automatically monitoring CCTV

footage, processing imagery of individuals’ faces, and storing the same on databases against allegedly known violent customers. This determination is a major development in facial recognition technology and biometric data under Australian law, and was also accompanied by new guidance, “Facial recognition technology: a guide to assessing the privacy risks”.

Industry programs

Industry-wise, an increasing number of sector and government partners are choosing to participate in ASD programs, including the ASD-Microsoft initiative to connect ASD’s Cyber Threat Intelligence Sharing platform with Microsoft’s Sentinel platform.

Joint advisories and investigations

Internationally, Australia is pursuing a co-ordinated approach with its allies in the field of cybercrime where there have been co-ordinated international investigative and law enforcement efforts, resulting in the simultaneous sanctioning of entities. This was seen in 2024 with Operation Cronos, a co-ordinated law enforcement action against the LockBit ransomware group and comprising Australia, the UK, the USA, France and many more.

In addition to simultaneous sanctioning, the international partnerships also result in joint advisories, often seen in respect of Australian-viewed state-sponsored malicious actors. For example, the ASD continues to work with partners to highlight evolving state-sponsored cyber-actors, such the PRC-sponsored Volt Typhoon, APT40, and Integrity Technology Group, Russia’s Unit 29155, and Iranian cyber-actors generally.

Another notable joint-operation appears to have involved the ASD and its international partners in identifying a “botnet” comprising 260,000

compromised devices controlled and managed by PRC's state-sponsored Integrity Technology Group since as early as mid-2021 world-wide. Although uncovering these actions is incredibly useful in strengthening cybersecurity, the authorities appear to have been able to do little more than release a joint advisory encouraging exposed device vendors, owners and operators to update and secure their devices. This example illustrates a government's reliance on industry and individuals in dealing with identified threats, at least when it comes to state-sponsored threats – if not beyond.

On the Horizon

Looking towards the future, there are reforms and threats emerging, both old and new.

Legislative changes are on the table such as tranche 2 of the Privacy Act amendments, as are regulations with the public consultation pro-

cesses concerning the Cyber Security Act rules to take place by February 2025; but the formal and informal transitional periods of 2023-2024 are coming to an end. There have been noticeable shifts in regulatory approaches, as regulators' powers expand (eg, OAIC), their focuses shift to cyberspace (eg, ASIC), and their public approaches start firming into one of enforcement (eg, CISC). Even government agencies are set to adopt new approaches, with DoHA intending to create a new Technology Strategy and Cyber Security Strategy.

The year of 2025 is scheduled to be the end of Horizon 1, yet there appears to be much more foundational work to occur and gaps in Australia's cybersecurity to be addressed. With the Action Plan to be reviewed and the Federal election to take place by May 2025, the stage is set for significant changes in the strategy, purposes and actions across the board.

BELGIUM

Law and Practice

Contributed by:

Wim Nauwelaerts
Alston & Bird LLP



Contents

1. General Overview of Laws and Regulators p.41

- 1.1 Cybersecurity Regulation Strategy p.41
- 1.2 Cybersecurity Laws p.41
- 1.3 Cybersecurity Regulators p.42

2. Critical Infrastructure Cybersecurity p.44

- 2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.44
- 2.2 Critical Infrastructure Cybersecurity Requirements p.44
- 2.3 Incident Response and Notification Obligations p.45
- 2.4 State Responsibilities and Obligations p.46

3. Financial Sector Operational Resilience Regulation p.46

- 3.1 Scope of Financial Sector Operational Resilience Regulation p.46
- 3.2 ICT Service Provider Contractual Requirements p.46
- 3.3 Key Operational Resilience Obligations p.47
- 3.4 Operational Resilience Enforcement p.48
- 3.5 International Data Transfers p.48
- 3.6 Threat-Led Penetration Testing p.48

4. Cyber-Resilience p.49

- 4.1 Cyber-Resilience Legislation p.49
- 4.2 Key Obligations Under Legislation p.49

5. Security Certification for ICT Products, Services and Processes p.50

- 5.1 Key Cybersecurity Certification Legislation p.50

6. Cybersecurity in Other Regulations p.51

- 6.1 Cybersecurity and Data Protection p.51
- 6.2 Cybersecurity and AI p.51
- 6.3 Cybersecurity in the Healthcare Sector p.51

Contributed by: Wim Nauwelaerts, **Alston & Bird LLP**

Alston & Bird LLP is an international law firm with extensive experience in a wide spectrum of cybersecurity issues. The firm leverages this experience to help companies manage their

cybersecurity-related responsibilities. This includes advising clients on incident response and breach notification requirements under EU and UK law.

Author



Wim Nauwelaerts is the partner-in-charge of Alston & Bird's Brussels office, leading the firm's European privacy, cyber and data strategy team. A true veteran in his field, Wim has

been advising multinational companies on privacy, data protection and cybersecurity matters for more than 25 years.

Alston & Bird LLP

Rue Guimard 9
B-1040 Brussels
Belgium

Tel: +32 2486 8822
Email: Wim.Nauwelaerts@alston.com
Web: www.alston.com

ALSTON & BIRD

1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

Belgium's Cybersecurity Strategy 2.0 (2021–25; the "Strategy"), which was designed by the Belgian federal government in co-operation with the Belgian Cybersecurity Centre (CCB), aims to make Belgium one of the least vulnerable countries in Europe in terms of cybersecurity. It includes a strategic plan to support the development of appropriate capacity to detect, investigate, prosecute and sanction cybercrime.

One of the key objectives of the Strategy is to build out expertise across all levels of law enforcement so that the necessary investigation capacities can be effectively and quickly deployed in a digital environment. The intention is to ensure that the prosecutor's office and the courts of all judicial districts have prosecutors and judges with sufficient experience in combating cybercrime.

The Strategy also sets out several strategic objectives that the CCB intends to pursue in co-operation with all relevant stakeholders in the cybersecurity sector in the upcoming years.

These objectives include:

- strengthening and increasing trust in digital environments;
- arming users and administrators of computers and networks;
- protecting organisations of vital interest against cyberthreats;
- responding effectively to cyberthreats;
- improving public, private and academic collaborations; and
- participating in international commitments involving cybersecurity.

1.2 Cybersecurity Laws

The main laws and regulations in Belgium relating to cybersecurity include:

- Article 22 of the Belgian Constitution;
- Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation; GDPR);
- the Act of 3 December 2017 establishing the Data Protection Authority (the "DPA Act"), amended by the Act of 25 December 2023;
- the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data, supplementing the GDPR (the "Data Protection Act");
- the Belgian Criminal Code, as amended by the Act of 28 November 2000 on Cybercrime and the Act of 15 May 2006 on Cybercrime, in particular Article 210bis on computer-related forgery, Articles 259bis and 314bis on the interception of electronic communications, Article 504quater on computer-related fraud, Article 550bis on illegal access (hacking) and Article 550ter on computer sabotage;
- the Belgian Criminal Procedure Code;
- the Royal Decree of 10 October 2014 for the establishment of the CCB, supplemented by Royal Decree of 12 October 2023 determining the conditions for awarding subsidies for activities related to informing and raising awareness in the field of cybersecurity;
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) 526/2013 (the "Cybersecurity Act");

- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the “NIS Directive”), as repealed by Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) 910/2014 and Directive (EU) 2018/1972 (the “NIS2 Directive”);
- the Act of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security, and transposing the NIS2 Directive (the “NIS2 Act”);
- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) 1060/2009, (EU) 648/2012, (EU) 600/2014, (EU) 909/2014 and (EU) 2016/1011 (DORA);
- Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (the “Cyber Resilience Act” or CRA);
- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (the “Critical Infrastructures Directive”), as repealed by Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (the “CER Directive”);
- the Act of 1 July 2011 on the security and protection of critical infrastructures, partially implementing the Critical Infrastructures Directive (the “Critical Infrastructures Act”) – the Critical Infrastructures Act was amended by the Royal Decree of 15 September 2023 to align the security requirements for the energy sector with those imposed by the CER Directive; and
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) 300/2008, (EU) 167/2013, (EU) 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (the “AI Act”).

1.3 Cybersecurity Regulators

The CCB operates under the authority of the federal Prime Minister and is the central authority for cybersecurity in Belgium, in addition to assuming the role of national computer security incident response team (CSIRT). The CCB is charged with monitoring, co-ordinating and supervising the implementation of the government’s cybersecurity policy and strategy.

The federal computer emergency response team (CERT) is the operational service of the CCB. The task of CERT is to detect, observe and analyse online security problems, and to provide continuous information about these problems. It helps the government, emergency services and companies to prevent, co-ordinate and provide assistance in the event of cyber-incidents.

The Cyber Threat Research and Intelligence Sharing (“CyTRIS”) Department within the CCB monitors cyberthreats and publishes regular reports.

In addition to the CCB, several sectoral authorities are charged with monitoring cyber-related matters for their respective sectors:

- the federal Minister for Energy – the energy sector (Federal Public Service Economy);
- the federal Minister for Transport – the transport sector, with the exception of transport over waters accessible to seagoing vessels;
- the federal Minister for Maritime Mobility – transport over water accessible to seagoing vessels;
- the federal Minister for Public Health – the health sector; and
- the federal Minister for Economy – the digital services sector, encompassing cloud computing services, online search engines and online marketplaces (Federal Public Service Economy).

Together with the CCB, the National Crisis Centre (NCCN) ensures the organisation and co-ordination of the Cyber Emergency Plan at national level. The two authorities are jointly responsible for crisis management. The NCCN is also in charge of making national risk assessments, and it is the (inter)national point of contact for critical infrastructures. Moreover, the NCCN prepares national emergency plans and provides local support. It operates 24/7, ensures the protection of people and institutions and monitors events.

The Belgian Institute for Postal Services and Telecommunications (BIPT) monitors the security of the electronic communications networks and services of telecoms operators. The BIPT is also the sectoral authority and inspection service for the digital infrastructure sector under the NIS2 Act, and for the electronic communications and digital infrastructure sectors under the Critical Infrastructures Act.

The National Security Council is charged with the co-ordination and evaluation of general intelligence and security policy matters and the national security strategy, the prioritisation of intelligence and security services, the co-ordination of national security priorities, the co-ordination of a general policy on the protection of sensitive information, the co-ordination of the fight against terrorism and extremism and the monitoring of its decisions.

The Coordination Unit for Threat Analysis (CUTA), operating under the Minister of Justice and the Minister of Interior Affairs, is an independent knowledge centre in charge of assessing terrorist and extremist threats in Belgium.

The Belgian Data Protection Authority (DPA) is an independent body that ensures that the fundamental principles of personal data protection are properly observed. This includes the GDPR's requirements relating to data security and personal data breach notifications. The DPA consists of different departments, each of which plays a specific role in enforcement cases. The Frontline Service performs a triage function to determine which complaints merit further investigation, the Inspection Body carries out investigations, and the Dispute Resolution Chamber issues enforcement decisions. Investigations are typically triggered by a complaint or request for information, but the DPA can also decide to open an investigation at its own initiative.

The Information Security Committee (ISC) was created by the Act of 5 September 2018 to grant certain authorisations in relation to the processing and communication of specific categories of personal data (eg, national registry numbers).

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

The NIS2 Directive and the Belgian NIS2 Act transposing it apply to public or private entities that are established in Belgium and that provide one of the services listed in Annex I or II to the NIS2 Act within the EU.

An entity will be subject to the NIS2 Act if it carries out one of the activities listed in Annex I or II to the NIS2 Act – as an “essential” or “important” entity – within the EU, and if it is at least considered to be a medium-sized enterprise within the meaning of European Commission Recommendation 2003/361/EC of 6 May 2003 (concerning the definition of micro, small and medium-sized enterprises).

“Essential entities” are those that provide a service listed in Annex I and meet the definition of a large enterprise within the meaning of Recommendation 2003/361/EC.

“Important entities” are organisations that provide a service:

- listed in Annex I and meet the definition of a “medium-sized enterprise” within the meaning of Recommendation 2003/361/EC; or
- listed in Annex II and meet the definition of a “medium-sized or large enterprise” within the meaning of Recommendation 2003/361/EC.

For the purposes of calculating the size of the entity, the European Commission has published guidance as well as a calculation tool. In addition, the CCB has issued guidelines specifying that the scope of the NIS2 Act covers the whole

of the entity concerned and not just the activities listed in the Annexes to the NIS2 Act.

Moreover, an entity will be considered in scope of the NIS2 Act even if the essential service it provides is only an ancillary part of all its activities – unless the definition of the service in the Annex takes into account the principal or incidental nature of the activity.

In terms of territorial scope, the NIS2 Act applies in principle to entities established in Belgium that provide their services or carry out their activities within the EU. The concept of establishment consists of the actual pursuit of an activity by means of a permanent installation, irrespective of the legal form adopted, whether this is a registered office, a local branch or a subsidiary with legal personality.

It should also be noted that the operator of one or more critical infrastructure(s) identified under Critical Infrastructures Act will be considered to be an essential entity within the meaning of the NIS2 Act. The NIS2 authorities and the competent authorities under the Critical Infrastructures Act are expected to work together to supervise these entities.

2.2 Critical Infrastructure Cybersecurity Requirements

The main cybersecurity requirements for entities in scope of the NIS2 Act can be summarised as follows:

- register with the relevant (sectoral) authorities – this can be done by completing an online form on the Safeonweb@Work registration platform, provided that the entity is already registered with the Belgian Crossroads Bank for Enterprises;

- adopt appropriate cybersecurity risk-management measures – these are technical, operational or organisational measures that allow the entity to manage the risks relating to the security of their network and information systems, and to prevent or minimise the impact of cyber-incidents;
- provide training to their management bodies to ensure that their knowledge and skills are sufficient to identify risks and assess risk-management measures in terms of cybersecurity and their impact on any services provided to the entity;
- ensure supply chain security, which refers to security-related aspects of the relationships between entities and their direct suppliers or service providers – the NIS2 Act does not explain in detail how NIS2 entities should manage this supply chain security obligation, but the CCB recommends that covered entities contractually impose a label or certification obligation on their suppliers, such as those included in the CCB's CyberFundamentals (CyFun®) framework, in order to demonstrate compliance with this requirement; and
- notify significant (cybersecurity) incidents to the CCB (see 2.3 Incident Response and Notification Obligations).

2.3 Incident Response and Notification Obligations

Entities in scope of the NIS2 Act are required to notify the national CSIRT (ie, the CCB) in the event of a significant (cybersecurity) incident.

A significant incident is defined as any incident that has a significant impact on the provision of services in the sectors or subsectors listed in the Annexes to the NIS2 Act, and which has caused or is likely to cause:

- serious disruption to the operation of any of the services in the sectors or subsectors listed in Annexes I and II or financial loss to the concerned entity; or
- significant material, personal or non-material damage to other natural or legal persons.

Notification takes place through the following steps:

- first, an early warning is submitted, within 24 hours of becoming aware of the significant incident;
- a formal incident notification is subsequently filed within 72 hours of becoming aware of the significant incident; and
- a final report is ultimately submitted, no later than one month after the initial notification – in the meantime, the CCB may request interim reports, and the CCB will also provide recommendations on when notification is required and on the procedure to follow.

In principle, NIS2 entities are expected to notify incidents to the CCB only. The CCB will subsequently forward notifications to the relevant sectoral authorities and to the NCCN (for essential entities).

However, the notification regime is different for entities in the banking and financial sectors that are in scope of DORA. Those types of entities should notify incidents, as appropriate, to the National Bank of Belgium (NBB) or the Financial Services and Markets Authority (FSMA), which will forward the incident notification to the CCB.

In some cases, entities that have suffered a significant incident will also be required to notify the recipients of their services.

2.4 State Responsibilities and Obligations

The CCB is responsible for co-ordinating and monitoring the NIS2 Act. Under the NIS2 Act, the CCB will be in charge of supervising essential and important entities (in co-operation with sectoral authorities), in addition to being the central contact point for NIS2 implementation.

Belgium's CSIRT is also part of the CCB. Entities in scope of the NIS2 Act are required to report significant incidents to this CSIRT. In addition, the NCCN is involved in the implementation of the NIS2 Act, in particular as regards incident notification, cybercrisis management and physical security measures implemented by operators of critical infrastructures and critical entities (subject to the Critical Infrastructures Act).

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

DORA applies to the following types of financial entities, which are under the supervision of the FSMA:

- asset management and investment advisory companies (investment firms);
- authorised managers of alternative investment funds;
- management companies of collective investment undertakings and self-managed collective investment undertakings;
- trading platforms;
- crowdfunding service providers (crowdfunding platforms);
- insurance and reinsurance intermediaries and ancillary insurance intermediaries; and

- institutions for occupational retirement provision (IORPs).

DORA also applies to institutions that are under the supervision of the NBB, such as credit institutions, insurance and reinsurance companies and payment institutions.

3.2 ICT Service Provider Contractual Requirements

DORA defines information and communication technology (third-party) service providers (ICT TPSPs) as undertakings providing ICT services to financial entities in scope of DORA. ICT services in the context of DORA should be understood in a broad manner, encompassing digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis. This may include providers of cloud computing services, software, data analytics services and data centre services. If financial entities delegate critical or important functions to ICT TPSPs, more stringent requirements will apply.

To ensure the conformity of their ICT risk management framework, financial entities are expected to maintain and update a specific information register (register of information or ROI) that lists the relevant contracts relating to the use of ICT services provided by ICT TPSPs. The agreements with ICT TPSPs will have to be properly documented and clearly distinguish those applicable to ICT services in support of critical functions.

Upon request, financial entities will have to make the entire ROI or certain parts of it available to the FSMA, together with all information that is considered necessary to enable effective supervision of the financial entity.

In addition, financial entities will have to inform the FSMA of any new or planned agreements on the use of ICT services that support critical or important functions.

Contractual provisions on the use of ICT services should include at least the following elements:

- a description of the services provided;
- a description of the locations where the services will be provided;
- the availability, confidentiality and security of the data;
- access to and return of the data;
- the relevant service levels;
- a contractual obligation to assist the customer/financial entity;
- a contractual obligation to co-operate with the FSMA;
- a contractual obligation to contribute to customer/financial entity awareness and education; and
- a right of termination and cancellation.

3.3 Key Operational Resilience Obligations

DORA aims to strengthen the digital operational resilience of the financial sector in the EU by imposing additional (cybersecurity) requirements on financial entities such as crypto-asset service providers, credit institutions and e-money providers (referred to as “financial entities” under DORA).

Sector-specific requirements under DORA include obligations to design ICT risk management frameworks, report major ICT-related incidents and perform digital operational resilience testing. DORA also requires financial entities to address and manage external sources of ICT risks that may result from their use of ICT TPSPs. To this end, financial entities are required

to undertake due diligence on prospective ICT TPSPs, enter into specific contractual arrangements with ICT TPSPs and maintain and update a register with information on their relationships with ICT TPSPs.

After collecting and analysing all relevant information, financial entities must report serious ICT-related incidents to the FSMA. This information enables the FSMA to determine the scope of the incident and its possible cross-border effects, and to communicate it to other supervisors and authorities concerned.

The reporting of serious ICT-related incidents involves different steps, including the submission of an initial report, an interim report and a final report. Financial entities must submit an interim report if the status or handling of the incident has changed significantly, or at the request of the FSMA. The final report contains the analysis of the underlying causes of the incident, as well as information about the actual impact of the incident.

When a serious ICT-related incident affects the financial interests of their clients, financial entities must inform them of the incident and the measures taken to mitigate any negative impact thereof.

DORA also includes a (voluntary) notification regime for significant cyberthreats – ie, cyberthreats that could result in a major ICT-related incident or a major operational or security payment-related incident. Financial entities may, on a voluntary basis, notify significant cyberthreats to the FSMA when they consider the threat to be of relevance to the financial system, service users or clients. Where appropriate, the FSMA may report that information to the other authorities and bodies concerned.

In the case of a significant cyberthreat, financial entities may need to, where applicable, inform clients that are potentially affected of any appropriate protection measures that they should consider taking.

Financial entities may outsource their reporting duties, but they remain fully responsible for ensuring compliance with their financial entity obligations under DORA.

3.4 Operational Resilience Enforcement

The NBB and the FSMA are the primary financial services regulators in Belgium. They are also in charge of monitoring cybersecurity risks in the Belgian financial sector. Therefore, DORA compliance will be overseen primarily by the FSMA.

To harmonise the supervision of ICT risks in the financial sector, DORA also brings together EU financial authorities, such as the European Banking Authority and the European Securities and Markets Authority, collectively referred to as the European Supervisory Authorities.

DORA allows EU member state authorities competent to monitor the activities of financial entities and ICTSPs to impose administrative fines (including in collaboration with other authorities, such as DPAs). For example, DORA leaves it to the discretion of these authorities to examine whether a DORA violation was intentional or resulted from a financial entity's or ICTSP's negligence in determining the amounts of fines to be imposed.

Furthermore, the EU legislators wanted to ensure appropriate oversight of critical ICTSPs, especially because these companies also provide, in some cases, their services to financial entities within the same group, which may lead to potential conflicts of interest and concentration

risks. To address this issue, DORA establishes a new oversight framework whereby one of the major EU financial authorities (eg the European Banking Authority or the European Securities and Markets Authority) is designated as a lead overseer (LO) to monitor the activities of critical ICT TPSPs.

Critical ICT TPSPs are ICT TPSPs that the European Supervisory Authorities have designated as "critical" for financial entities, following an assessment that takes into account the criteria specified in DORA. LOs will have the power to conduct investigations (ie, on-site and offsite inspections) and adopt decisions imposing a periodic penalty payment to compel critical ICT TPSPs to co-operate with the LO in the course of an investigation.

3.5 International Data Transfers

Under DORA, financial entities are required to design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit. To achieve these objectives, financial entities are required to use ICT solutions and processes that, inter alia, ensure the security of the means of transfer of data.

In addition, if the data includes personal data (as defined in the GDPR), restrictions imposed by the GDPR may apply to transfers of personal data to recipients in jurisdictions outside of the EU.

3.6 Threat-Led Penetration Testing

DORA requires certain entities to conduct advanced threat-led penetration tests. This

requirement will only apply to financial entities selected on the basis of an assessment of the following elements:

- impact-related factors, in particular the extent to which the financial entity's services and activities have an impact on the financial sector;
- possible financial stability concerns, including the systemic nature of the financial entity at the EU or national level, where applicable; and
- the specific ICT risk profile, the level of ICT maturity of the financial entity or the technological characteristics at stake.

The obligation to conduct advanced threat-led penetration tests does not apply to (i) small and unconnected investment firms, (ii) IORPs that have no more than 100 affiliates, or (iii) financial entities employing fewer than ten people, and whose annual turnover and/or annual balance sheet total does not exceed EUR2 million.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

The CRA imposes minimum cybersecurity standards for connected products placed on the Belgian market, with a view to making the internet of things (IoT) more secure. It contains horizontal cybersecurity requirements for products with digital elements (PDEs), which are defined as products that can be connected to a device or network and include:

- hardware products with connected features, such as smartphones, laptops, home surveillance systems and connected toys; and

- software not embedded in a product and sold on a standalone basis, for example accounting software and mobile gaming apps.

All manufacturers placing PDEs on the Belgian market must comply with the CRA even if they are based outside the EU. For instance, the CRA may apply to a Chinese manufacturer of solar panels that sells its products in Belgium.

The CRA primarily imposes obligations on manufacturers of PDEs to ensure that their products are secure before they are put on the EU/Belgian market, but also afterwards throughout the whole life cycle of the product.

Furthermore, it includes provisions affecting other operators of PDEs such as importers, distributors, open-source software stewards, conformity assessment bodies (CABs) and public authorities.

According to the CCB, the CRA is expected to contribute to the CCB's vision of making Belgium more cybersecure by ensuring that its citizens and organisations are less vulnerable to cyber-attacks.

4.2 Key Obligations Under Legislation

The CRA imposes a minimum level of cybersecurity for all PDEs that are placed on the Belgian market and requires manufacturers of PDEs to:

- design their PDEs with cybersecurity in mind – eg, by ensuring that data stored or transmitted with(in) the product is encrypted, and that the attack surface is as limited as possible;
- ensure that the default settings of their PDEs help reduce vulnerabilities – eg, by avoiding weak default passwords or by making sure that security updates are installed automatically;

- implement user transparency via clear disclosure, on the PDE or its packaging, of the end-of-support date, namely the date until which the manufacturer commits to provide security updates – this should assist PDE users with making purchasing decisions not only based on price and functionality, but also on the PDE's level of cybersecurity; and
- report actively exploited vulnerabilities as well as severe incidents impacting the security of PDEs to public authorities, within 72 hours (with an early warning within 24 hours) of becoming aware of the vulnerability or incident – to facilitate the notification process and enable secure data sharing among European CSIRTs and ENISA, the CRA introduces a new single reporting platform with different national “end-points”, where this single reporting platform is different from the European vulnerability database established by the NIS2 Directive.

All PDEs, regardless of their cybersecurity risk level, must comply with the CRA's basic cybersecurity standards outlined in the foregoing. PDEs that are considered more sensitive from a cybersecurity viewpoint – which the CRA refers to as “important” or “critical” products (eg password managers, firewalls, smart meters) are subject to additional, stricter obligations.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

Cybersecurity certification plays an important role in increasing trust and security in IoT-related products, services and processes, and the Cybersecurity Act has therefore introduced a European cybersecurity certification framework.

ENISA, the EU Agency for cybersecurity, is in charge of in setting up and maintaining the European cybersecurity certification framework by preparing the technical ground for specific certification schemes. It is also responsible for informing the public on the certification schemes and the issued certificates through a dedicated website.

In addition, Belgium has created (by Royal Decree dated 16 October 2022), a framework that enables companies to evaluate and certify the security of ICT products, services and processes, in line with the Cybersecurity Act. The CCB has been designated as the national cybersecurity certification authority that will co-ordinate the necessary expertise in cybersecurity certification, authorise certificates with high security requirements and establish close collaboration with the Belgian accreditation organisation.

To help covered entities demonstrate compliance with the NIS2 Act in particular, the CCB has created the CyFun framework, which is based on several commonly used cybersecurity frameworks or standards including the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), International Organization for Standardization (ISO) 27001/ISO 27002, Center for Internet Security (CIS) Controls and International Electrotechnical Commission (IEC) 62443. Following a NIS2 conformity assessment, a CyFun certification can be granted by a CAB that is approved by the CCB. CABs are bodies responsible for verifying an entity's compliance with the requirements set out in the CyFun reference framework.

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

The GDPR provides that controllers have a legitimate interest in processing personal data to the extent that such processing is strictly necessary and proportionate for the purposes of ensuring network and information security. The GDPR further specifies that permitted practices and tools for network and information security could include those that focus on:

- preventing unauthorised access to electronic communications networks and malicious code distribution; and/or
- stopping “denial of service” attacks and damage to computer and electronic communication systems.

The GDPR also includes a notification regime for personal data breaches. The concept of “personal data breach” is broadly defined in the GDPR as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”. Controllers whose processing of personal data is subject to Belgian law may be required to notify personal data breaches to the Belgian DPA and, in some cases, to the individuals whose personal data is affected.

A personal data breach is a type of data security incident. While all personal data breaches are data security incidents, not all data security incidents are necessarily personal data breaches. The GDPR, and hence the notification duties to the DPA and affected individuals, only apply where there is a personal data breach.

6.2 Cybersecurity and AI

The AI Act requires that high-risk AI systems must achieve suitable accuracy, robustness and cybersecurity levels, and that they perform consistently in those respects throughout their life cycle. The technical solutions aiming to ensure the cybersecurity of high-risk AI systems must be appropriate to the relevant circumstances and the risks. They can include measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set (data poisoning), pre-trained components used in training (model poisoning), inputs designed to cause an AI model to make a mistake (adversarial examples or model evasion), confidentiality attacks and model flaws.

The European Commission has requested the European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC) to draft the new European standards or European standardisation deliverables on AI by 30 April 2025, including European standard(s) and/or European standardisation deliverable(s) on cybersecurity specifications for AI systems.

High-risk AI systems that have been certified, or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to the Cybersecurity Act, will be presumed to comply with the cybersecurity requirements set out in the AI Act (in so far as the cybersecurity certificate or statement of conformity, or parts thereof, cover those requirements).

6.3 Cybersecurity in the Healthcare Sector

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) 178/2002 and Regulation

(EC) 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (the “Medical Devices Regulation”), requires that, for devices that incorporate software or for software packages that are medical devices in themselves, the software must be developed and manufactured in accordance with the state-of-the-art, including in regard to information security standards and verification invalidation. Manufacturers of such medical devices must set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including any protection against unauthorised access.

Incidents involving the security of medical devices that include or constitute software may require notification to the national competent authority, if certain conditions are met. This will be the case, for example, where the medical device is suspected to be a contributory cause of the incident and the incident has (or might have) led to the death or serious deterioration in the state of health of a patient or other person. For incidents that occur on the Belgian territory, the national competent authority is the Federal Agency for Pharmaceuticals and Health Products (FAGG).

Trends and Developments

Contributed by:

Stéphanie De Smedt, Virginie de France, Bram Goetry and Olivier Verhasselt
Loyens & Loeff

Loyens & Loeff is a leading law and tax firm, and the logical choice for businesses in the Netherlands, Belgium, Luxembourg and Switzerland (its four home markets). With over 1,000 advisers in its Benelux and Swiss offices and key financial centres worldwide, Loyens & Loeff offers customised, innovative advice. The firm's cybersecurity team excels in identifying, assessing and mitigating risks through pragmatic expert advice, both in a transactional

and a litigation context. Loyens & Loeff develop and implement policies and contractual frameworks, manage regulatory reporting and investigations and advise on compliance with laws like the GDPR, the NIS2 Directive and the Cyber Resilience Act. The firm's services also include compliance audits, due diligence assessments and tailored training for board members, general counsels and employees on cybersecurity risks, regulations and best practices.

Authors



Stéphanie De Smedt is a partner in the Brussels office of Loyens & Loeff. She is an expert in commercial and IP/ICT law, and is the go-to person for clients active in the digital

economy and tech sector. Developments such as artificial intelligence and the regulation of new technologies in general are among Stéphanie's core focus areas. She has developed recognised expertise with respect to regulatory compliance – more specifically as a CIPP/E-certified expert – in relation to the protection of personal data, cybersecurity and life sciences. Stéphanie is a member of the International Association of Privacy Professionals (IAPP) and of iTechLaw.



Virginie de France mainly focuses on ICT law, more specifically data protection law and cybersecurity. In her position as lawyer and professional support lawyer at

Loyens & Loeff, she oversees and manages all aspects of the team's know-how, but also advises and represents clients in her fields of expertise. Virginie is a member of the Brussels Bar.



Bram Goetry is an associate at the Brussels office of Loyens & Loeff. He focuses on data protection law and cybersecurity, and general commercial and intellectual

property law, and he advises and represents clients in both litigious and non-litigious matters in these fields of expertise. Bram is a member of the Brussels Bar.

Contributed by: Stéphanie De Smedt, Virginie de France, Bram Goetry and Olivier Verhasselt, **Loyens & Loeff**



Olivier Verhasselt is an associate at the Brussels office of Loyens & Loeff. Olivier mainly focuses on data protection law and privacy, but also has broader expertise in all areas of IP/IT law and general commercial law. He advises and represents clients in both litigious and non-litigious matters in these fields of expertise. Olivier is a member of the Brussels Bar.

Loyens & Loeff

Tervurenlaan 2
1040 Brussels
Belgium

Tel: +32 2743 4343
Fax: +32 2743 4310
Email: Info.brussels@loyensloeff.com
Web: www.loyensloeff.com

LOYENS  LOEFF
Law & Tax

Introduction

As digital transformation accelerates and cyberspace becomes increasingly complex, cybersecurity has emerged as a critical concern for organisations. The deep interconnectivity of the cyber-ecosystem means that a breach in a single entity can trigger a chain reaction, compromising entire networks with far-reaching consequences. Even the smallest vulnerabilities in digital systems can lead to significant disruptions, from financial losses to reputational damage.

For many organisations, cybersecurity is no longer merely an operational concern – it is also a legal imperative. In 2024, Belgium was the first EU member state to transpose Directive (EU) 2022/2555 (the “NIS2 Directive”) into national law (the “NIS2 Law”). As a direct consequence thereof, 2025 is set to be an intense year as this landmark legislation is expected to impact over 2,500 entities across a wide range of sectors. In addition to implementing risk management measures, organisations will need to review their contracts with suppliers and subcontractors and ensure that future agreements explicitly include cybersecurity warranties. Management bodies will also be heavily involved, as the law imposes numerous obligations and responsibilities on them. Compliance with the NIS2 Law is overseen and enforced in Belgium by the Centre for Cyber Security (the CCB).

Below is an overview of the main cybersecurity trends the authors see for 2025.

CyberFundamentals as a Cybersecurity Framework Originating in Belgium, but Potentially With Much Broader Recognition

Under the NIS2 legislation, certain entities are required to undergo periodic compliance assessments, which result in certification. In Belgium, only two certifications are recognised by law:

- the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 certification; and
- the Belgium-specific CyberFundamentals (“CyFun”) certification scheme.

The latter is a certification granted by a conformity assessment body approved by the CCB. The framework is based on commonly used cybersecurity frameworks, namely the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), ISO 27001/ISO 27002, Center for Internet Security (CIS) Controls and IEC 62443. To address the varying levels of risk organisations face, the framework offers four assurance levels: small, basic, important and essential. The CyFun framework is generally deemed to be less burdensome (and less expensive) to implement than ISO certification, and the CCB has also published a multitude of online guidance notes and tools to aid implementation thereof by Belgian companies.

Interestingly, Romania has already implemented the NIS2 Directive, and has explicitly recognised the Belgian CyFun certification scheme as a valid compliance framework under its local law.

Following the Romanian example, CyFun, although initially a local Belgian initiative, could receive broader international recognition, with more countries expected to follow Romania’s lead.

Cybersecurity Clauses as a “Must Have” for Both Current and Future Contracts

In cases where IT services are outsourced, the legal responsibility under cybersecurity legislation (eg, NIS2 and DORA) remains with the in-scope organisation itself. Therefore, it is crucial for these organisations to properly map the various contactors, suppliers, service provid-

ers, etc, that have access to their IT systems, provide cloud-based software solutions or may otherwise impact the organisation's cybersecurity risk profile.

In Belgium, the authors are seeing a clear trend towards companies requesting additional cybersecurity-related guarantees and certifications from their suppliers. Since past cyber-attacks have highlighted the intrinsic link with various ecosystems, cybersecurity clauses are becoming a key concern in supply chain risk management.

More specifically, the authors see an increased focus on the following types of clauses in various types of commercial (supply/services) contracts, not only in the IT sector:

- clauses setting minimum standards and obligations of result in relation to cybersecurity (obtaining and maintaining certifications, annexes with detailed lists of technical and organisational measures to implement, etc) for the supplier;
- clauses ensuring swift incident reporting by suppliers, in order for the client – which may be a regulated entity under NIS2 or the Digital Operational Resilience Act (DORA) – to meet its own legal reporting obligations, often detailing reporting deadlines, mandatory information to be provided and co-operation obligations;
- clauses providing extensive cybersecurity audit rights for the client;
- liability and exoneration clauses (a higher or no liability cap for cyber-incidents, indemnification obligations for third-party claims, etc); and
- termination clauses in case of serious cyber-incidents or material non-compliance, etc.

While the arrangements for cybersecurity are in some cases set out in a lot of detail in the legislation itself (see DORA), this is not always the case (see NIS2), which leaves a lot of room for diverging practices and tough negotiations. In 2025, the authors expect more common practices and standards to develop in this respect – as it did for data processing agreements under the General Data Protection Regulation (GDPR), for example.

The focus on supply chain risk management will in any event remain in 2025. Noteworthy in this respect is the finding that, of all large organisations, 54% identified supply chain challenges as the biggest barrier to achieving cyber-resilience. The increasing complexity of supply chains, coupled with a lack of visibility and oversight regarding the security levels of suppliers, has emerged as the leading cybersecurity risk for organisations. Key concerns include software vulnerabilities introduced by third parties and the propagation of cyber-attacks throughout the ecosystem, as noted in the World Economic Forum's Global Cybersecurity Outlook 2025.

Leaders Must Adopt a “Security-First” Mindset

The NIS2 legislation requires management bodies to play an active role in cybersecurity, making their involvement not only beneficial but also legally mandatory. The authors expect this to become a board-level priority in 2025.

More specifically, management bodies of NIS2-in-scope entities must:

- approve risk management measures related to cybersecurity and oversee their implementation;
- complete training to ensure they possess the necessary knowledge and skills to identify risks, assess cybersecurity risk management

practices and understand their impact on the services provided by their organisation (this entails an obligation for management to follow regular cybersecurity awareness trainings); and

- ensure the organisation's compliance with the law.

As the concept of “management body” is not defined in the NIS2 Directive, the explanatory memorandum to the Belgian NIS2 Law defines a “member of a management body” as “Any natural or legal person who:

1. exercises a function within or in relation to an entity which authorises him or her (a) to administer and represent the entity in question or (b) to take decisions in the name and on behalf of the entity which are legally binding on it or to participate, within a body of that entity, in the taking of such decisions, or
2. has control over the entity, meaning the power, in law or in fact, to exercise decisive influence over the appointment of the majority of the entity's directors or managers or over the direction of the entity's management”.

Where the entity is a company governed by Belgian law, this control is determined in accordance with Articles 1:14 to 1:18 of the Belgian Code of Companies and Associations.

Moreover, if an organisation that is in-scope of NIS2 fails to comply with the NIS2 Law, then its management body may be held accountable and face not only director's liability, but also a temporary ban from holding executive responsibilities within the organisation. It remains to be seen how this liability will be assessed in practice, and

in which situations (likely only very extreme ones) the CCB would impose such a temporary ban.

While 2025 will likely still be a year of transition, enforcement of the NIS2 Law by the CCB is expected to gradually increase, especially in case of major cybersecurity incidents in critical or public sectors.

The Role of the CCB and the Data Protection Authority in Cybersecurity Compliance

The CCB has been designated by the NIS2 Law as the national authority responsible for the monitoring, supervision and enforcement of the NIS2 Law on Belgian territory. However, entities may also have to face another authority in the context of cybersecurity: the Belgian Data Protection Authority (DPA), which oversees the enforcement of the GDPR and national legislation concerning personal data protection. Indeed, the DPA is often called upon to examine IT systems and their use within companies, particularly due to the risks of personal data breaches, becoming a valuable asset in the event of cybersecurity incidents. The NIS2 Directive itself acknowledges in its recitals that personal data protection and cybersecurity are closely linked.

As a result, when a company suffers a cyber-attack leading to a personal data breach – a common occurrence – it often finds itself engaging with multiple authorities, sometimes including sectoral regulators, while also adhering to tight deadlines and different formal requirements. Firstly, companies subject to the NIS2 Law must notify significant incidents to the CCB without undue delay, at the latest within 24 hours of becoming aware of the incident. Additionally, these companies must also notify the DPA if the incident constitutes a personal data breach under data protection law, and this must

be done no later than 72 hours after becoming aware of the breach.

The NIS2 Law does not provide amendments or exemptions to the GDPR in this regard. For initial notification, many companies will therefore first notify the CCB and then prepare their notification to the DPA. A late notification can lead to sanctions for non-compliance, as well as a broader investigation by the relevant regulatory authority.

The only exemption to the obligation to notify in the case of a personal data breach is provided by Article 74 of the NIS2 Law. According to this article, the data controller may be exempted from notifying a personal data breach to certain affected individuals, as provided in Article 34 of the GDPR. This exemption is possible subject to the CCB's approval, where such individual notification could jeopardise the control and supervision of the entities, as well as the preparation, organisation, management and follow-up of administrative measures and fines. However, it is important to note that this exemption only applies to the obligation to notify the affected individuals, not the authorities.

Therefore, it is essential that entities systematically notify incidents involving personal data to both relevant authorities, in accordance with the requirements and procedures of both pieces of legislation. This approach also aligns with the “cyber incident response plan” model published by the CCB, which explicitly mentions the CCB and the DPA among the entities that should receive a report.

The next natural question is whether, following a notification and any subsequent investigation by the CCB and the DPA, a company could face two fines, one under the NIS2 Law and another

under the GDPR. The fourth Title of the NIS2 Law states that the CCB or any competent sectoral authority will not impose an administrative fine for an infraction resulting from the same behaviour for which an administrative fine has already been imposed by the DPA. Instead, they may decide to impose alternative sanctions for the same actions (eg, requiring the entities involved to make certain aspects of the violations public). However, neither the NIS2 Law nor the GDPR or its implementing legislation provide a solution where the CCB first imposes an administrative fine, and the DPA then decides to do the same. However, it is reasonable to expect that a similar approach will be applied in such a case, by analogy with the criminal law principle of *non bis in idem*.

Ethical Hacking in Belgium Is Legal, Under Certain Conditions

Since 15 February 2023, in the context of the entry into force of a new whistle-blower law, the Belgian legislator has legalised “ethical hacking”. Under certain conditions, ethical hackers are protected against criminal liability, even where the hacked organisation did not consent to being subject to such “testing” of their cybersecurity standards.

Traditionally, the term “hacker” evokes individuals who exploit security flaws in IT systems for malicious purposes, such as extortion, sabotage or data theft. However, there are also hackers with good intentions, known as “ethical hackers”. “Ethical hacking” refers to the practice of testing an organisation's systems and networks to identify and fix potential vulnerabilities without any fraudulent intent.

Until 18 October 2024, any natural or legal person was allowed to search for and report security vulnerabilities, even outside a co-ordinated

vulnerability disclosure policy, without risking criminal prosecution, provided that they comply with certain conditions:

- there is no intent to cause harm or to obtain illegitimate benefits (eg, they cannot request payment, unless this has been agreed upon in advance, such as in the context of bug bounty programmes);
- the vulnerabilities they discover must be reported to the CCB without delay, as well as to the organisation they “hacked” – to gain some control over this process and safeguard both confidentiality and a streamlined notification process, several companies have already set up ethical hacking policies and dedicated communication channels;
- the hacker cannot do anything that goes beyond what is necessary and proportionate in order to uncover a cybersecurity vulnerability; and
- the hacker is prohibited from publicly disclosing the discovered vulnerabilities without prior authorisation to do so from the CCB.

However, in 2024, the NIS2 Law narrowed the previous general liability exemption for ethical hacking to a specific list of defined offences:

- interception of private communications (Article 314bis of the Criminal Code);
- violation of professional secrecy (Article 458 of the Criminal Code);
- hacking (Article 550bis of the Criminal Code);
- IT sabotage (Article 550ter of the Criminal Code); and
- offences related to telecommunications legislation.

Other offences, such as breaking and entering, are not included.

In other words, ethical hacking is now only permitted for conventional cyber-attacks involving remote access to IT systems. Physical attacks on these systems are no longer legally protected and require prior authorisation from the competent authorities. Otherwise, perpetrators face criminal prosecution, including charges of breaking and entering.

Furthermore, the four conditions established in 2023 remain in effect and are further clarified by the NIS2 Law, which entered into force on 18 October 2024.

- **Proportionality and necessity:** The hackers must limit themselves to the actions strictly necessary to demonstrate the existence of a vulnerability, without exceeding what is needed to prove the security flaw. This also means they are prohibited from disrupting the target organisation’s services, even if an investigation is ongoing.
- **No harm or blackmail:** The hacker must never intend to cause harm or obtain sensitive information from the targeted company. Any form of blackmail, such as threatening to disclose vulnerabilities in exchange for benefits, is strictly prohibited.
- **Reporting vulnerabilities:** The hacker must promptly submit a simplified notification that includes the identification of the affected system and a brief description of the potential vulnerability, no later than 24 hours after its discovery, to both the organisation responsible for the system and the CCB. The hacker must submit a complete notification, without delay and no later than 72 hours after its discovery, to both the organisation responsible for the system (if applicable, in accordance with the reporting procedures established by that organisation) and the CCB. It is also important to note that disclosing information

BELGIUM TRENDS AND DEVELOPMENTS

Contributed by: Stéphanie De Smedt, Virginie de France, Bram Goetry and Olivier Verhasselt, **Loyens & Loeff**

publicly without prior consent from the CCB is strictly forbidden.

- **Legal responsibility:** The legislation on ethical hacking does not protect against potential violations or prosecutions under foreign laws. Hackers can still face legal action based on the legislation of other countries.

With the Belgian NIS2 Law reinforcing the legal framework for ethical hacking and the 2025–29 federal coalition agreement of the new Belgian government granting law enforcement agencies the authority to collaborate with ethical hackers, organisations are advised to be aware of the applicable legal requirements to protect themselves against potential abuse.

BRAZIL

Trends and Developments

Contributed by:

Juliana Abrusio and Mario Cosac

Machado Meyer



Machado Meyer is a leading Brazilian law firm renowned for its comprehensive legal services and commitment to excellence. Established in 1972, the firm has built a strong reputation for its expertise across various practice areas, including technology, the internet, and data protection law. With a team of highly skilled attorneys, Machado Meyer provides tailored solutions to meet the unique needs of its clients, who range from multinational corporations to start-ups. The firm is recognised for its innova-

tive approach and deep understanding of the Brazilian legal landscape, enabling the team to navigate complex legal challenges effectively. Machado Meyer's dedication to client service and its collaborative culture foster long-lasting relationships, making it a trusted partner in the legal field. The firm's commitment to diversity and inclusion further enhances its ability to deliver exceptional legal services in an ever-evolving market.

Authors



Juliana Abrusio of Machado Meyer works in the areas of digital law and data protection, including information security (data protection law, regulations, policies, incidents and training),

response to data leaks, due diligence, electronic contracts, digital fraud, among other topics. She also provides services related to administrative litigation before the Brazilian Data Protection Authority (ANPD), as well as judicial litigation involving digital law and data protection. Juliana has experience in the legal structuring of new digital business models (fintech, agrotech, edutech, heathtech, insurtech) and in markets involving blockchain and cryptocurrencies. In addition, she advises companies on the use of AI (big data and data analytics).



Mario Cosac of Machado Meyer has extensive experience in litigation and advisory matters in the areas of technology, digital law, and IP. In the technology sector, he has experience with

judicial and administrative issues related to privacy, data protection, civil liability of internet platforms, and issues related to e-commerce. In the area of IP, Mario acts mainly in cases involving misuse of confidential information and in disputes involving trade marks, unfair competition, copyrights, advertising, and franchise issues, as well as in complex negotiations of contracts involving technology and intellectual assets.

Machado Meyer

Avenida Brigadeiro Faria Lima 3200
5th Floor
Itaim Bibi
01453-050
Brazil

Tel: +55 113 150 3311
Email: jabrusio@machadomeyer.com.br
Web: www.machadomeyer.com.br/en



The Cybersecurity Landscape in Brazil

The Brazilian cybersecurity landscape can be analysed both at the macro level and in specific sectors. This is due to the existence of regulations and research at the federal level, as well as specific regulations pertaining to certain sectors of the economy, which will be outlined throughout this article. The federal scenario shall be considered first, however, before moving on to other, more specific regulation.

Federal landscape

Approved through Decree No 10,222 on 5 February 2020, the National Cybersecurity Strategy (*Estratégia Nacional de Segurança Cibernética*, or “E-Ciber”) outlined strategic actions for the period from 2020 to 2023, with the aim of guiding Brazilian society on the federal government’s main initiatives around cybersecurity – both nationally and internationally. Among the E-Ciber’s objectives were to make Brazil more prosperous and reliable in the digital environment, increase resilience to cybersecurity threats, and strengthen the country’s international role in cybersecurity.

Following the E-Ciber, on 26 December 2023, President Luiz Inácio Lula da Silva signed Decree

No 11,856, establishing the National Cybersecurity Policy (*Política Nacional de Cibersegurança*, or “PNCiber”). This policy aims to guide cybersecurity activities in the country, establishing guidelines to protect critical infrastructures and promote cyber-resilience. In addition, the decree created the National Cybersecurity Committee (*Comitê Nacional de Cibersegurança*, or CNCiber), formed by representatives from the government, civil society, scientific institutions and the business sector. The CNCiber is responsible for monitoring the implementation and evolution of the E-Ciber, proposing updates to the PNCiber, and evaluating and suggesting measures to improve cybersecurity in Brazil, as well as formulating international technical co-operation strategies.

The policy arises from the need for protection, given that cyber-attacks represent one of the greatest threats to entities in today’s world. In 2021, there was a [major data leak in Brazil](#), whereby 220 million individual taxpayer registration (*Cadastro de Pessoas Físicas*, or CPF) and company registration (*Cadastro Nacional da Pessoa Jurídica*, or CNPJ) numbers were exposed. Although the source of the leak has not been identified, 37 databases covering name,

address, photo, credit score, income, Internal Revenue Service status and National Social Security Institute (*Instituto Nacional do Seguro Social*, or INSS) number were made available on the internet. Part of the data was published for free, such as name and CPF number, while the complete set was sold online.

Most recently, during the CNCiber meeting held on 4 December 2024, a new proposal for the E-Ciber text was presented. Now that suggestions and changes have been made by the members, the new text should be approved and formalised soon. The new E-Ciber will include a new regulatory agenda, as well as directions for new recommendations to the technology market and digital service providers, in addition to suggesting possible legal frameworks to strengthen cybersecurity governance in the country.

At the same time, Brazil has sought to improve mechanisms for sharing information about incidents and vulnerabilities between the public and private sectors. The creation of Computer Security Incident Response Team (CSIRT) centres has been encouraged, with the aim of strengthening the capacity to prevent, detect and respond to cybersecurity incidents. Currently, the country has the Cyber Incident Prevention, Handling and Response Centre of the Brazilian Government (*Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo*, or CTIR Gov), which is responsible for co-ordinating cybersecurity actions at government level.

In addition, it is worth mentioning the Brazilian Strategy for Digital Transformation (*Estratégia Brasileira para a Transformação Digital*, or “E-Digital”) and the National Information Security Policy (*Política Nacional de Segurança da Informação*, or PNSI). The latter offers a diagnosis of the challenges of the digital transforma-

tion of Brazilian society and establishes strategic actions, setting trust in the digital environment as one of its axes.

E-Digital is focused on two areas, which are:

- protection of rights and privacy; and
- defence and security in the digital environment.

It also presents eight strategic actions, which include the draft of a national cybersecurity policy and a national plan to prevent incidents and cybersecurity threats.

Finally, the PNSI was approved through Decree No 9.637/2018 and established within the scope of the entire federal public administration. The PNSI covers:

- cybersecurity;
- cyberdefence;
- physical security and protection of organisational data; and
- actions aimed at ensuring the availability, integrity, confidentiality and authenticity of information.

This policy is implemented through the National Information Security Strategy (*Estratégia Nacional de Segurança da Informação*, or ENSI) and national plans.

Brazilian Data Protection Authority

The Brazilian Data Protection Authority (*Autoridade Nacional de Proteção de Dados*, or ANPD) is the entity responsible for overseeing data processing activities, ensuring the protection of personal data. Therefore, its regulation affects all sectors where there is data processing activity, according to the Brazilian General Data Protection Regulation (*Lei Geral de Proteção de Dados*,

or LGPD). Although the ANPD does not regulate cybersecurity specifically, it has already implemented several regulations to ensure a secure environment for data processing activities, providing insights into the expectations for data processing agents.

Among these, the following stand out:

- case and technical studies on anonymisation and regulatory sandboxes related to the topic;
- informative notices on data breaches and security measures recommended for data subjects;
- guidelines on information security for small business data processing agents, with an information security checklist that directly names cybersecurity controls, such as web application firewalls or multifactor authentication; and
- other regulations related to the topic, such as Resolution No 15/2024, which establishes the procedure for reporting incidents.

As regards Resolution No 15/2024, the ANPD did not expressly establish the security mechanisms that companies must adopt to ensure data protection – it simply indicated that companies must implement the necessary mechanisms to ensure information security. However, the incident reporting form provided by the ANPD outlines certain expected security mechanisms, such as encryption, authentication methods, back-ups, and firewalls.

Furthermore, several cybersecurity-related topics are included in the ANPD's regulatory agenda for 2025-26, such as security measures, technical and administrative standards (including minimum technical security standards), and anonymisation and pseudonymisation. This

demonstrates the significance of the subject for the ANPD, as well as the obligations that data processing agents will need to adhere to in the future.

Energy sector

The energy sector is classified as critical infrastructure, making it a prime target for cyberattacks. The vulnerability of this sector to cybersecurity threats, such as ransomware attacks and data breaches, is a significant concern. Supervisory Control and Data Acquisition (SCADA) systems, which are integral to the operation of energy networks, are particularly susceptible to such attacks.

To mitigate these risks, the sector has been increasingly adopting international cybersecurity frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the International Organization for Standardization (ISO)'s ISO 27001, and the International Electrotechnical Commission (IEC)'s IEC 62443. These frameworks provide comprehensive guidelines for securing critical infrastructure.

Moreover, energy companies are held accountable for any service disruptions caused by cyberincidents, facing [civil liabilities](#) and [administrative liabilities](#) alike. Service-level agreements (SLAs) and stringent security requirements for suppliers further reinforce the sector's resilience against cybersecurity threats.

The energy sector in Brazil is governed by a robust regulatory framework aimed at ensuring digital compliance and cybersecurity. The National Electric Energy Agency (*Agência Nacional de Energia Elétrica*, or ANEEL) plays a pivotal role in this regard, with specific regulations such as Resolution No 964/2021, which

outlines the requirements for digitalisation and cybersecurity measures within the sector. This resolution mandates energy companies to adopt stringent cybersecurity protocols to protect their infrastructure and data.

Additionally, the State-Owned Companies Law ([Law No 13.303/2016](#)) and the Digital Government Law ([Law No 14.129/2021](#)) impose further compliance obligations on energy companies, emphasising transparency, accountability, and the secure handling of data. These regulations collectively ensure that energy concessionaires adhere to high standards of data governance and cybersecurity, thereby safeguarding the sector against potential cybersecurity threats.

Consumer protection

In recent years, Brazil has made significant strides in enhancing consumer protection and cybersecurity. An important development in this area was the signing of the Technical Co-operation Agreement No 1/2021 between the ANPD and the National Consumer Secretariat (*Secretaria Nacional do Consumidor*, or “Senacon”) on 22 March 2021. This agreement aims to expedite investigations involving cybersecurity incidents by fostering collaboration between the two entities.

Through the exchange of information, educational initiatives, research, and joint enforcement actions, Senacon and the ANPD are working together to safeguard personal data and defend consumer rights. Senacon provides the ANPD with access to its database, which includes complaints and notifications, whereas the ANPD focuses on regulatory and enforcement actions under the LGPD. This partnership is expected to not only speed up investigations but also to strengthen the culture of data protection in Bra-

zil, ensuring greater legal security for consumers and organisations alike.

In July 2024, Senacon announced an [investigation into the damage caused by a recent cybersecurity breach](#) that affected various sectors in Brazil. The incident stemmed from a problematic update by cybersecurity provider CrowdStrike, which disrupted services provided by Microsoft. This error disconnected computers and servers from the internet, leading to a system recovery loop that rendered machines inoperable. The fallout was widespread, impacting global companies and causing significant disruptions in Brazil. Airlines, banks, and even the health-care system faced operational challenges, with manual check-ins at airports for travellers and service interruptions for hospitals and energy distributors.

Digital piracy

Another significant effort in the realm of cybersecurity is Brazil’s fight against digital piracy in the field of consumer protection. On 10 February 2025, the National Council for Combating Piracy and Intellectual Property Offences (*Conselho Nacional de Combate à Pirataria e Delitos contra a Propriedade Intelectual*, or CNCP) submitted a list of 393 blocked pirate websites to the World Intellectual Property Organization (WIPO). This list will be included in [WIPO Alert](#), an international monitoring and dissemination mechanism.

The CNCP, which is linked to Senacon, has been actively involved in combating digital piracy and protecting citizens from cybercrimes. Operations such as Redirect and 404 have targeted illegal platforms, blocking hundreds of websites and applications. These pirate sites not only distribute illegal content but also expose more than 90 million consumers to fraud, data theft, and

cyber-attacks, often featuring illegal gambling ads that particularly affect minors.

Role of public prosecutor

On 28 May 2024, the National Council of the Public Prosecutor's Office (*Conselho Nacional do Ministério Público*, or CNMP) unanimously approved a resolution establishing the National Cybersecurity Policy and System of the Public Prosecutor's Office (*Política e o Sistema Nacional de Cibersegurança do Ministério Público*, or "PNCiber-MP"). [Resolution No 294/2024](#) aims to set forth principles, guidelines, and a minimum governance system to guide the planning, actions, and control of cybersecurity within the units and branches of the public prosecutor. The proposal consists of nine chapters addressing various aspects such as principles, goals, instruments, governance, and the management of the PNCiber-MP. The resolution was officially published on 3 July 2024.

The PNCiber-MP is an integral part of the Institutional Security Policy of the Public Prosecutor's Office (*Política de Segurança Institucional do Ministério Público*, or PSI/MP), established by CNMP Resolution No 156/2016, which regulates measures aimed at security in information and communications technology (ICT). The resolution outlines that cybersecurity encompasses a set of actions designed to prevent, detect, treat, and respond to digital threats using appropriate controls, including policies, rules, processes, procedures, organisational structures, technologies, and people. These measures aim to ensure the availability, integrity, confidentiality and authenticity of information, in line with the risk profile of the public prosecutor. The guiding principles of the PNCiber-MP include:

- the protection of fundamental rights and guarantees of users;

- integration and co-operation among cybersecurity actors;
- proactive incident prevention; and
- the reliability of information systems.

The instruments defined by the PNCiber-MP include the National Strategic Planning of the Public Prosecutor's Office (*Planejamento Estratégico Nacional do Ministério Público*, or PEN-MP), the PSI/MP, the National Information Technology Policy (*Política Nacional de Tecnologia da Informação do Ministério Público*, or PNTI-MP), and the National Strategic Information Technology Plan (*Plano Estratégico Nacional de Tecnologia da Informação do Ministério Público*, or PEN-TI-MP).

Additionally, the PNCiber-MP includes the institutional security plans and strategic information technology plans of the units and branches of the Public Prosecutor's Office, as well as protocols, instructions, manuals, and technical statements issued by governance and management bodies. The National Cybersecurity System of the Public Prosecutor's Office, co-ordinated by the CNMP, will adopt a co-operative governance methodology and include the National Cybersecurity Management Committee (*Comitê Gestor Nacional de Cibersegurança do Ministério Público*, or "CGNCiber-MP"), the Cyber Crisis Management Committee, and the National Cybersecurity Co-operation Network (*Rede Nacional de Cooperação em Cibersegurança do Ministério Público*, or "REDECiber-MP").

Ministry of Science, Technology, and Innovation

The Ministry of Science, Technology, and Innovation (*Ministério da Ciência, Tecnologia e Inovação*, or MCTI) in Brazil, in collaboration with the Brazilian Agency for Industrial Research and Innovation (*Empresa Brasileira de Pesquisa e Ino-*

vação Industrial, or “Embrapii”), has announced the establishment of the [Cybersecurity Competence Centre](#), which will receive an investment of BRL60 million from the MCTI’s Priority Programme (*Programa Prioritário em Informática*, or PPI) IoT/Manufacturing 4.0. The centre will focus on four key research areas:

- identity and access management;
- data protection and privacy;
- cybersecurity threat intelligence; and
- legal, ethical and behavioural aspects.

The announcement, made in May 2024, underscores the Brazilian government’s commitment to enhancing cybersecurity infrastructure. This is crucial for the secure operation of essential systems, including government digital services.

The creation of the Cybersecurity Competence Centre is part of a broader initiative by Embrapii and the MCTI to establish multiple competence centres across various strategic and frontier technology areas, with a total investment of BRL495 million. These centres aim to generate knowledge, develop human resources, and foster innovation through collaboration with industrial partners and start-ups. The initiative is expected to bolster Brazil’s cybersecurity capabilities, protect critical national infrastructure, and stimulate the national cybersecurity industry – thereby enhancing the country’s competitiveness and attracting foreign investment. The Cybersecurity Competence Centre is poised to play an important role in addressing the complex cybersecurity challenges facing Brazil, leveraging its extensive experience in innovation and technology development.

[Hackers do Bem hub](#)

In addition to the Cybersecurity Competence Centre, the MCTI has also launched the

[Hackers do Bem](#) hub, which is a virtual space created by the National Education and Research Network (*Rede Nacional de Ensino e Pesquisa*, or RNP). This initiative aims to strengthen Brazil’s cybersecurity ecosystem by bridging experts, companies and enthusiasts in an open environment for information sharing, networking, and technical training. Launched in August 2024 during the RNP Forum in Brasília, the hub is designed to be an interactive platform that fosters a self-sustaining and autonomous community dedicated to advancing digital security in the country.

The *Hackers do Bem* hub host events, courses and forums to solidify Brazil’s defence against cybersecurity threats and connect professionals to job opportunities. It will also serve as a resource for students of the *Hackers do Bem* programme, which has already seen more than 100,000 enrolments since its inception in 2023. The hub, developed in partnership with Cisco and Rustcon, aims to enhance the training of cybersecurity professionals by providing additional courses and specialised activities – thereby ensuring that graduates are well equipped to tackle the evolving challenges in the field.

[Aviation sector](#)

The National Civil Aviation Agency (*Agência Nacional de Aviação Civil*, or ANAC) has made significant strides in enhancing cybersecurity within the aviation sector in Brazil. The publication of the new National Civil Aviation Security Programme Against Acts of Unlawful Interference (*Programa Nacional de Segurança da Aviação Civil contra Atos de Interferência Ilícita*, or “PNAVSEC”) on 8 September 2022, marked a pivotal moment for aviation security. This programme, approved by Decree No 11,195/2022, aligns Brazil’s aviation security regulations with international standards set by the Internation-

al Civil Aviation Organization (ICAO). Decree No 11,195/2022 introduces innovative security measures, including risk assessments and security protocols for public and airport areas, and addresses threats from man-portable air defence systems (MANPADS). Notably, it incorporates cybersecurity regulations to identify vulnerabilities and implement protective measures for data and communication systems, ensuring the confidentiality, integrity and availability of information.

In April 2023, ANAC established the Cybersecurity Committee (“CSC/ANAC”) through Portaria No 11.126. This committee aims to co-ordinate, harmonise and consolidate ANAC’s efforts in cybersecurity, implementing policies to protect civil aviation against cybersecurity threats. The CSC/ANAC takes over the responsibilities of the Cybersecurity Working Group (*Grupo de Trabalho de Segurança Cibernética*, or GTSC), established in August 2020, and serves as the sectoral co-ordination team (*Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Coordenação Setorial*, or “ETIR Setorial”) as per Decree No 10.748, which created the Federal Network for Cyber Incident Management (*Rede Federal de Gestão de Incidentes Cibernéticos*, or ReGIC). The CSC/ANAC comprises representatives from various organisational units within ANAC – each responsible for different aspects of aviation security – and is co-ordinated by the Superintendence of Airport Infrastructure (*Superintendência de Infraestrutura Aeroportuária*, or SIA).

Throughout 2023, ANAC faced numerous challenges and achieved significant milestones in cybersecurity. Recognising the growing reliance on ICT in civil aviation, [ANAC took proactive measures to mitigate emerging risks and vulnerabilities](#). The agency released two key manuals,

the *Civil Aviation Cybersecurity Awareness Manual* and the *Cybersecurity Assessment Manual*, based on international standards. These documents aim to raise awareness among aviation professionals and help organisations assess and improve their cybersecurity maturity. Additionally, ANAC engaged in international co-operation with organisations such as ICAO, the European Union Aviation Safety Agency (EASA) and the European Organization for Civil Aviation Equipment (“EUROCAE”), fostering collaboration and information exchange on cybersecurity.

In 2024, ANAC continued its efforts to modernise and enhance aviation security with the publication of Resolution No 753 on 9 August 2024. This resolution, approved during the 12th deliberative meeting of ANAC’s collegiate board, mandates the adoption of technical and technological solutions to improve civil aviation security against unlawful interference and elevate operational safety. The resolution aims to enhance passenger services and airport capabilities by implementing new equipment and procedures. ANAC will define the minimum criteria for the acceptance of these technologies and methodologies, tailored to the size, resources, and needs of each aerodrome. This resolution is part of the broader [Airports+Security programme](#), which was launched in June 2023 by the federal government to ensure that Brazilian airports meet the highest standards of safety and security.

Telecommunications sector

The National Telecommunications Agency (*Agência Nacional de Telecomunicações*, or ANATEL) has a range of publications on cybersecurity, encompassing regulations (such as Resolution No 767/2024), public policies, guidelines, and other documentation and studies aimed at bolstering cybersecurity within its domain.

Mainly, ANATEL relies on the Cybersecurity Regulation Applied to the Telecommunications Sector (*Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações*, or “R-Ciber”). The R-Ciber sets forth the obligations of regulated agents (eg, the development, maintenance and implementation of a cybersecurity policy), as well as the principles to be followed by them (eg, confidentiality, availability, integrity and liability).

Besides that, the R-Ciber also establishes a governance model within ANATEL, through the Cybersecurity and Critical Infrastructure Risk Management Technical Group (*Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica*, or “GT-Ciber”). This group has a series of obligations related to monitoring cybersecurity policy and critical infrastructure management, equipment configuration, technical requirements, and suppliers – sharing information and best practices as well as awareness, training, studies and interaction with the Brazilian Communications Commissions (*Comissões Brasileiras de Comunicações*, or CBCs).

Right after the R-Ciber was published, ANATEL took another step to promote the cybersecurity of the sector on 5 January 2021, when it approved the [Cybersecurity Requirements for Telecommunications Equipment](#). This authorises ANATEL to carry out the certification and approval of telecommunications equipment – from the simplest (eg, sensors with wireless communication interfaces) to the most complex (eg, operator network core equipment). One of the principles of this approval activity is the protection and security of the users of these products. The aim of establishing the requirements together with the creation of a market oversight programme is to:

- encourage manufacturers to develop their products with security in mind from the outset (“security by design”);
- monitor the market for insecure products;
- ensure that manufacturers implement fixes for identified flaws/vulnerabilities; and
- prevent insecure equipment from being commercialised.

Finally, ANATEL also promotes campaigns to increase society’s awareness of cybersecurity practices, including campaigns to prevent fraud and other digital crimes.

Financial sector

The Central Bank of Brazil (*Banco Central do Brasil*, or “BACEN”) has taken further steps by enacting regulations pertaining to cybersecurity, thereby imposing specific obligations on financial and payment institutions under its purview. This is notably evident through the implementation of Resolution No 4.893/2021 and Resolution No 85/2021. Both regulations aim to enhance the regulatory framework governing the financial system’s stability and integrity. This is part of BACEN’s ongoing efforts to align with international standards and best practices, ensuring that financial institutions operate under robust and transparent guidelines. The primary objective of Resolution 4.893/2021 is to establish comprehensive rules for the management of risks and capital adequacy, thereby promoting a more resilient financial sector.

The regulatory framework regarding cybersecurity for financial institutions authorised to operate under the BACEN is outlined by Resolution No 4.893/2021, which delineates the cybersecurity policy and the prerequisites for engaging data processing, storage services, and cloud computing. Similarly, Resolution No 85/2021 addresses the same subject matter but applies

Contributed by: Juliana Abrusio and Mario Cosac, **Machado Meyer**

to payment institutions, securities brokerages, securities distributors, and authorised foreign exchange brokerages operating under BACEN.

Given the importance of safeguarding transactions within its purview, BACEN has been actively promulgating regulations in this sector to enforce stringent obligations and standards for the entities under its regulation, thereby ensuring the security of transactions.

CHILE

Law and Practice

Contributed by:

Claudio Magliona, Bárbara Reyes and Diego Lisoni
Magliona Abogados



Contents

1. General Overview of Laws and Regulators p.73

- 1.1 Cybersecurity Regulation Strategy p.73
- 1.2 Cybersecurity Laws p.74
- 1.3 Cybersecurity Regulators p.76

2. Critical Infrastructure Cybersecurity p.77

- 2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.77
- 2.2 Critical Infrastructure Cybersecurity Requirements p.79
- 2.3 Incident Response and Notification Obligations p.80
- 2.4 State Responsibilities and Obligations p.82

3. Financial Sector Operational Resilience Regulation p.82

- 3.1 Scope of Financial Sector Operational Resilience Regulation p.82
- 3.2 ICT Service Provider Contractual Requirements p.83
- 3.3 Key Operational Resilience Obligations p.84
- 3.4 Operational Resilience Enforcement p.85
- 3.5 International Data Transfers p.86
- 3.6 Threat-Led Penetration Testing p.86

4. Cyber-Resilience p.86

- 4.1 Cyber-Resilience Legislation p.86
- 4.2 Key Obligations Under Legislation p.87

5. Security Certification for ICT Products, Services and Processes p.87

- 5.1 Key Cybersecurity Certification Legislation p.87

6. Cybersecurity in Other Regulations p.87

- 6.1 Cybersecurity and Data Protection p.87
- 6.2 Cybersecurity and AI p.89
- 6.3 Cybersecurity in the Healthcare Sector p.90

Magliona Abogados specialises in corporate matters, tax services, complex business litigation and finance structures, telecommunications, technology law, intellectual property, and government relations and public policy, including corporate structuring, due diligence planning, M&A, financial assistance, syndicated loans, liability restructuring and leasing. It has expertise in licensing and software development agreements, technological platforms,

franchises, data protection and computer crime, as well as the distribution, production and financing of film and television. The firm's clients encompass a wide range of enterprises, both local and multinational, engaged in banking and finance, technology and software, leasing and insurance. It also counsels public agencies and companies in the movie industry, as well as other diverse fields.

Authors



Claudio Magliona is founding partner of Magliona Abogados. He has a wealth of experience in data protection, IP and TMT, and an extensive practice in corporate and financing,

technology law, telecommunications, intellectual and industrial property, and entertainment law, including corporate structures, M&A, financing, licensing and software development agreements, franchising, data protection, prevention of computer crimes as well as film distribution, production and financing. Claudio, who also handles government relations and policy matters, has spoken at numerous conferences around Latin America. He is the author of various publications on technology and law, data protection, IP and film financing.



Bárbara Reyes is an attorney of Magliona Abogados. She has a wealth of experience in privacy and data protection, cybersecurity, compliance, fintech services, public affairs

and government relations management. Bárbara has a Diploma in Compliance from the PUCV, and a Postgraduate Diploma in Regulation in the Digital Economy from the Universidad de Chile. In addition, she has an International Certification in Personal Data Protection ALAP-APEP (2024).



Diego Lisoni is a researcher who joined Magliona Abogados in 2021. Diego focuses on researching corporate, jurisprudential, regulatory and public policy matters. He

studied Law at Universidad de Chile and is an assistant professor in Administrative Law and E-Commerce and New Technologies. In addition, he is a co-ordination team member of the Youth Working Group of the Chilean Chapter of ISOC.

Magliona Abogados

Avda Andrés Bello 2687
Piso 24
Las Condes
Santiago de Chile
Santiago
Chile

Tel: +56 232 100 030
Fax: +56 2377 9451
Email: contacto@magliona.cl
Web: www.magliona.cl

MAGLIONA
— ABOGADOS —

1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

Chile has two sources of regulation and public policies that guide the country's cybersecurity strategy.

The National Cybersecurity Policy 2023–2028

The National Cybersecurity Policy 2023–2028 has five main objectives.

- Resilient infrastructure – the country will have a robust and resilient information infrastructure, prepared to resist and recover from cybersecurity incidents and socio-environmental disasters, from a risk management perspective.
- Rights of people – the state will protect and promote the protection of people's rights on the internet through strengthening the existing institutional framework in cybersecurity and generating, adopting and promoting the mechanisms and technological tools necessary for each person to integrate into society and develop and express themselves fully.
- Cybersecurity culture – Chile will develop a cybersecurity culture based on education, best practices, responsibility in the handling of digital technologies, and promotion and guarantee of people's rights.
- National and international co-ordination – the state will create public governance to co-ordinate the necessary actions in cybersecurity. Public and private organisations will create, together, co-operation instances to communicate and disseminate their activities in cybersecurity, avoid duplication of work and loss of resources, and make efforts in this area efficient.
- In the international arena, the state will co-ordinate with countries, organisations, institutions and other international actors to allow the country to better face malicious activities and incidents in cyberspace.
- Promotion of industry and scientific research – the country will promote the development of a cybersecurity industry that protects people and organisations and serves its strategic objectives. For this, it will promote the focus of applied scientific research on cybersecurity issues, according to the country's needs.

The transversal dimensions of this policy include:

- gender equality – giving preferential consideration to women, both to increase their safety in the digital environment, and to improve their inclusion through positive actions to correct existing inequalities in society;
- protection of children – all initiatives must give preferential consideration to the protection of girls, boys and adolescents;
- protection of the elderly – all initiatives must give preferential consideration to the protection of the elderly; and
- protection of the environment – all initiatives must minimise their negative impact on the environment.

The Cybersecurity Framework Law

For its part, the Cybersecurity Framework Law No 21.663, which entered into force together with the creation of the National Cybersecurity Agency (ANCI) in January 2025, aims to establish the institutional framework, principles and general regulations that allow structuring, regulating and co-ordinating cybersecurity actions of state agencies and between them and private parties. It also establishes the minimum requirements for the prevention, containment, resolution and response to cybersecurity incidents.

The guiding principles for this law are the following.

- Principle of damage control – in the face of a cyber-attack or cybersecurity incident, action must always be co-ordinated and diligent to prevent escalation or spread to other computer systems.
- Principle of co-operation with the authority – to resolve cybersecurity incidents, due co-operation with the competent authority must be provided, and if necessary, co-operation

between different sectors is needed, considering the interconnection and interdependence of systems and services.

- Principle of co-ordination – the ANCI and sectorial authorities must co-ordinate their tasks, strive for unity of action, and avoid duplication or interference of functions.
- Principle of security in cyberspace – the state must safeguard security in cyberspace, ensuring that all people can participate in a safe cyberspace, and grant special protection to computer networks and systems that contain information of those groups that are often the object of cyber-attacks.
- Principle of responsible response – the application of measures to respond to cybersecurity incidents or cyber-attacks may not involve offensive operations.
- Principle of computer security – every person has the right to adopt the technical computer security measures they deem necessary, including encryption.
- Principle of rationality – measures for the management of cybersecurity incidents, cybersecurity obligations, and the exercise of the Agency's powers must be necessary and proportional to the degree of exposure to risks and the potential social and economic impact.
- Principle of security and privacy by default and by design – computer systems, applications and information technologies must be designed, implemented, and managed considering the security and privacy of the personal data they process.

1.2 Cybersecurity Laws Cybersecurity Framework Law

The Cybersecurity Framework Law establishes the institutional framework, principles and general regulations to co-ordinate cybersecurity actions between state agencies and between

them and private entities. It also sets out the minimum requirements for the prevention, containment and response to cybersecurity incidents. This law defines essential services and the procedure for qualifying among these essential service providers the operators of vital importance, who will be subject to stricter obligations.

The law also creates the ANCI, a decentralised public service responsible for advising the President on cybersecurity issues, co-ordinating competent institutions, and ensuring the protection of the right to computer security. The ANCI has the power to issue mandatory protocols and standards for public and private institutions.

In addition, the Cybersecurity Framework Law creates the National Computer Security Incident Response Team (*CSIRT Nacional*) within ANCI. This team is responsible for responding to significant cyber-attacks and co-ordinating other CSIRTs.

As of 1 January 2025, the Law and the ANCI came into force. Thus, the Agency can start exercising its regulatory powers, for example by issuing general instructions. In addition, it will have to set up and manage the National Incident Register and will also be able to set the standards to be met by institutions providing goods or services to the state, as well as cybersecurity standards and duties to inform the public about the security risks of digital devices available to end consumers. The Regulation on Notification of Cybersecurity Incidents with Significant Effects is already in force, and the Agency has enabled a web portal and APIs for both essential service providers and operators of vital importance to make reports to the National CSIRT.

The first qualification process for Operators of Vital Importance is expected to be finalised dur-

ing Q3 2025. This regulatory framework also includes other relevant regulations, such as the rules on the (i) Functioning of the Secure Connectivity State Network and Special Obligations of State Administration Bodies; (ii) Registry of Cybersecurity Standards Certification Entities; (iii) Functioning of the Interministerial Cybersecurity Committee; and (iv) one that establishes rules for the functioning of the Multisectoral Cybersecurity Council.

The Computer Crimes Law

The Computer Crimes Law No 21,459 establishes rules on computer crimes and their penalties. This law seeks to adapt Chilean legislation to the Budapest Convention. Some of the crimes it typifies are:

- attack on the integrity of a computer system;
- unlawful interception;
- computer forgery;
- handling of illegally obtained computer data;
- computer fraud;
- illicit disposition of devices or programs to commit computer crimes.

Regarding the crime of illegal access – ie, accessing a computer system without authorisation, the penalties are increased if the access is made with the intention of seizing or using information, or if the illegally obtained information is disclosed. However, there is an exemption from criminal sanctions for those who access a computer system in a responsible manner (ethical hacking), fulfilling certain requirements such as registration with the ANCI, prior notification of the access to the Agency and communication of the vulnerabilities to the system operator and the Agency.

1.3 Cybersecurity Regulators

The National Cybersecurity Agency (ANCI)

The ANCI is a functionally decentralised public service, endowed with its own legal personality and assets, and of a technical and specialised nature. Its primary goal is to advise the President of the Republic on cybersecurity matters, to collaborate in the protection of national interests in cyberspace, to co-ordinate the relevant institutions, and to ensure the protection of the right to computer security. The Agency reports to the President through the Ministry in charge of public security.

The functions and powers of ANCI are varied and aim to cover all relevant aspects of cybersecurity in the country.

- Advisory role – to advise the President in the development of the National Cybersecurity Policy and its implementation plans.
- Regulation – to issue mandatory protocols, standards and instructions for public and private institutions. The Agency also administratively applies and interprets laws and regulations regarding cybersecurity.
- Co-ordination – to co-ordinate and supervise the National CSIRT (Computer Security Incident Response Team) and other CSIRTs of the State Administration. It must also establish co-ordination with the CSIRT of National Defence.
- Registry – to create and manage a National Registry of Cybersecurity Incidents.
- Qualification – to classify and qualify essential services and operators of vital importance.
- Information to the public – to require entities affected by cybersecurity incidents to provide truthful and timely information to potential victims.
- Training and education – to design and implement citizen training and education plans in cybersecurity.
- Access to information – to require state agencies and private institutions to provide access to information necessary to prevent or manage incidents. The Agency may request the delivery of the activity log of computer networks and systems.
- Co-operation – to co-operate with public bodies and private institutions, as well as with foreign cybersecurity authorities and international organisations.
- Technical advice – to provide technical advice to state agencies and private institutions affected by cybersecurity incidents.
- State intelligence – to collaborate with the State Intelligence System in identifying threats.
- Oversight – to oversee compliance with the law, regulations, protocols and standards issued by the Agency. It can carry out inspections, audits and security analyses.
- Access to computer systems – the Agency may require access to computer systems, data and documents for its supervisory functions. It can also request tests to demonstrate the implementation of operational continuity and cybersecurity plans.
- Research and development – to promote research, innovation and training in cybersecurity.
- Incident reporting – to inform the CSIRTs of the National Defence and other state agencies about cybersecurity incidents and vulnerabilities.
- Certification – to certify compliance with cybersecurity standards by state agencies and to grant accreditations to certification centres.
- Setting standards – to establish cybersecurity standards for suppliers of goods and services

to the state and for the development of computer systems used by state agencies. It can also establish standards for digital devices available to the public.

- State secure connectivity network – to administer the State Secure Connectivity Network.
- National exercise– to annually co-ordinate a national exercise to check cybersecurity capabilities.

ANCI, through its National Director, has the power to issue resolutions and administrative acts necessary for its operation, as well as to delegate powers to its officials. It also has the power to impose sanctions for breaches of the law.

Sectoral Authorities

ANCI is required to co-ordinate its actions with other sectoral authorities, and there are specific rules that govern this co-ordination. When ANCI issues protocols, technical standards or general instructions that affect the areas of competence of another sectoral entity, it must follow a particular procedure.

With regard to this duty of co-ordination, the following stands out.

- Prior report request – ANCI must send relevant information to the sectoral entity and request a report before issuing any regulations that affect their areas of competence. This aims to prevent regulatory conflicts and ensure co-ordination and collaboration.
- Sectoral administrative acts – if a sectoral authority issues administrative acts that affect ANCI's areas of competence, it must also send the relevant information to ANCI and request a report.
- Consideration of ANCI regulations – sectoral authorities, when issuing their administrative acts, must take into account the protocols,

standards and general instructions that ANCI has previously issued.

- Prevalence of sectoral regulations – it should be noted that, in addition, a sectoral authority would be competent to monitor, take cognisance of and sanction infringements, as well as to execute the sanctions to the cybersecurity regulations that it has issued and whose effects are at least equivalent to those of the regulations issued by the ANCI. This does not affect the duties of co-ordination. However, if sectoral regulations do not cover all entities in the sector, ANCI protocols still apply. For this, the Agency and the sectoral authority must issue a joint rule to evaluate the equivalence of the effects.

Among the main sectoral authorities with competences in cybersecurity, and which have to co-ordinate with the ANCI, are the Undersecretariat of Telecommunications; the Ministry of Health; the future Personal Data Protection Agency (when it takes office in December 2026), and the Financial Market Commission (CMF). See 3. **Financial Sector Operational Resilience Regulation**.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation General Scope of Application

The Cybersecurity Framework Law applies to state agencies, including ministries, presidential delegations, regional governments, municipalities, armed forces, law enforcement agencies, public enterprises and other public bodies and services.

It also applies to state enterprises and companies in which the state has a shareholding of

more than 50% or a majority on the board of directors.

In addition, the law applies to institutions that provide services qualified as essential and to those that are qualified as operators of vital importance.

Essential Services

The list of essential services outlined in the Framework Law is as follows:

- those services provided by the agencies of the State Administration and by the National Electricity Co-Ordinator;
- those services provided under a public service concession; and
- those services provided by private institutions that carry out the following activities:
 - (a) electricity generation, transmission or distribution;
 - (b) transportation, storage or distribution of fuels;
 - (c) provision of drinking water or sanitation;
 - (d) telecommunications;
 - (e) digital services;
 - (f) digital infrastructure;
 - (g) information technology services managed by third parties;
 - (h) land, air, rail or maritime transport, as well as the operation of their respective infrastructure;
 - (i) banking, financial services and means of payment;
 - (j) administration of social security benefits;
 - (k) postal and courier services;
 - (l) institutional provision of health by entities such as hospitals, clinics, doctors' offices and medical centres; and
 - (m) production and/or research of pharmaceutical products.

The ANCI can issue a resolution through which it will identify which specific activities and functions will be considered as essential services (eg, the ANCI could eventually identify the provision of domain name systems as a specific activity within the category “digital infrastructure”).

Operators of Vital Importance

The ANCI must, at least every three years, through an administrative procedure in which sectoral authorities must also participate, identify those essential service providers that will be classified as operators of vital importance. The procedure includes a public consultation process and in addition, the ANCI's decision could be claimed through administrative appeals and a judicial claim, if applicable.

The ANCI may classify as operators of vital importance those essential service providers which meet the following requirements:

- that the provision of such service depends on computer networks and systems; and
- that the affecting, interception, interruption or destruction of its services has a significant impact on security and public order, the continuous and regular provision of essential services, the effective performance of the functions of the state, or, in general, of the services that it must provide or guarantee.

The Regulation for the Qualification of Operators of Vital Importance published in March 2025 establishes that, in addition, the ANCI must consider one or more of the following criteria to identify the significant impact that the affectation, interruption, interception or destruction of the services could have:

- Number of potentially affected: Including direct and indirect dependencies, consider-

ing the magnitude, territorial coverage (local, communal, provincial, regional or national) and nature of the market.

- Redundancy of the service: Availability of alternative providers, their technical and operational capacity, response time and costs associated with the change.
- Mono-provision of the service: Existence of a single provider, barriers to entry for new providers, existence of viable substitutes and impact of the absence of the single provider.
- Service dependency: Interdependency between services, effect on the supply chain, criticality of the dependent service and resilience to the lack of the service on which it depends.
- Relevance of the affected institution: its direct or indirect impact on the protection of legal assets identified by law (e.g. security; public order; etc).

In addition, the ANCI may classify as operators of vital importance private institutions that, although they do not have the quality of providers of essential services, meet the requirements indicated previously and whose qualification is essential because they have acquired a critical role in the supply of the population, the distribution of goods or the production of a good/service that is indispensable or strategic for the country; or by the degree of exposure of the entity to risks and the likelihood of cybersecurity incidents, including their severity and the associated social and economic consequences.

2.2 Critical Infrastructure Cybersecurity Requirements

General Cybersecurity Obligations

Both essential service providers and operators of vital importance will need to permanently apply the measures to prevent, report and resolve cybersecurity incidents. These measures

may be technological, organisational, physical or informational in nature, as the case may be.

Compliance with these obligations requires the proper implementation of the protocols and standards that will be established by the ANCI, as well as the particular cybersecurity standards issued in accordance with the respective sectoral regulation. The purpose of these protocols and standards will be the prevention and management of risks associated with cybersecurity, as well as the containment and mitigation of the impact that incidents may have on the operational continuity of the service provided or the confidentiality and integrity of information or computer networks or systems in accordance with the provisions of the Framework Law.

Specific Cybersecurity Obligations of Operators of Vital Importance

Public or private entities that are classified by the ANCI as operators of vital importance, must comply with a series of obligations that will be complemented and detailed in the Regulations of the Framework Law.

- Implement a continuous information security management system in order to determine those risks that may affect the security of networks, computer systems and data, and the operational continuity of the service. This system should make it possible to assess both the likelihood and potential impact of a cybersecurity incident.
- Maintain a record of the actions carried out that make up the information security management system, in accordance with the provisions of the Regulation.
- Prepare and implement operational continuity and cybersecurity plans, which must be certified and must be subject to periodic

reviews by the obliged entities, at least every two years.

- Continuously carry out review operations, exercises and analyses of networks, computer systems or computer programs that compromise cybersecurity and communicate the information related to such actions or programs to the National CSIRT, in the manner determined by the Regulation.
- Take the necessary measures in a timely and expeditious manner to reduce the impact and spread of a cybersecurity incident, including restricting the use of or access to computer systems, if necessary.
- Have the certifications provided for in the Regulation.
- Have training, education and continuing education programmes for its workers and collaborators, including cyber-hygiene campaigns.
- Designate a cybersecurity delegate which will act as a counterpart to the ANCI and who will report to the authority or head of the body or service of the state administration or to the directors, managers, administrators or principal executives, as defined by private institutions.

Infringements

General infringements

- Minor – minor breaches such as submitting information after the deadline or not following ANCI's general instructions.
- Serious – failure to implement security protocols, submitting false information to ANCI, failure to report incidents to the National CSIRT, among others.
- Very serious – submitting false information in incidents with significant effects, failing to follow ANCI instructions in serious incidents or recidivating serious infringements.

Infringements for operators of vital importance

These operators have additional responsibilities, and the infringements are also classified as minor, serious and very serious depending on the breach of their specific obligations.

- Minor – failure to maintain records, failure to report security drills to the CSIRT, failure to train workers, etc.
- Serious – failure to implement security management systems, failure to draw up business continuity plans, failure to inform those affected by incidents, etc.
- Very serious – failure to take measures to reduce the impact of incidents with significant effects or recidivism of serious infringements.

Sanctions

Penalties vary according to the seriousness of the infringements.

- Minor infringements – warning or fine of up to 1,000 Monthly Tax Units (UTM).
- Serious infringements – fine of up to 10,000 UTM (approximately USD725,000).
- Very serious infringements:
 - (a) fine of up to 20,000 UTM (approximately USD1,450,000); or
 - (b) if the offender is a vital operator, the fine can be up to 40,000 UTM (approximately USD2.9 million).

2.3 Incident Response and Notification Obligations

Cybersecurity Incident

The Framework Law defines a cybersecurity incident as any event that impairs or compromises the confidentiality or integrity of information, the availability or resilience of computer networks and systems, or the authentication of processes

executed or implemented in computer networks and systems.

The Framework Law establishes the duty for providers of essential services and operators of vital importance to report cybersecurity incidents with significant effects to the National CSIRT.

The Regulation on Reporting of Incidents of Significant Effects in force from 1 March 2025 states that a cybersecurity incident shall be considered to have a significant impact if it is capable of producing any of the following effects:

- disrupting the continuity of an essential service. In such a case, both the services provided by providers, as well as the supply chain, of an institution providing essential services or of an operator of vital importance shall be considered;
- affecting the physical integrity or health of persons;
- affecting the integrity or confidentiality of IT assets, or the availability of any network or IT system, even if this does not or would not have had an immediate impact on the provision of the service;
- unauthorised use of or unauthorised access to networks or computer systems, even if this does not or has not immediately affected the provision of the service; or
- affecting computer systems containing personal data.

In determining the significance of the effects of an incident, the following criteria shall be taken into account:

- the number of persons affected;
- the duration of the incident; and
- the geographical extent of the area affected by the incident.

The Framework Law establishes a procedure for reporting cybersecurity incidents with significant effects as soon as possible and in accordance with a scheme which considers a series of different stages:

- an early warning within three hours of becoming aware of the cyber-attack or cybersecurity incident;
- a report of the incident within 72 hours, including an initial assessment of its severity and impact, including indicators of compromise;
- a final report within 15 days of the early warning containing a detailed description of the incident, the type of cause or threat likely to have caused the incident, mitigation measures to be implemented and in progress, and the cross-border impact (if any) of the incident;
- in the event that the incident is still ongoing after the final report, a status update must be made; and
- again, after a period of 15 days from that update, a new final report must be made.

Notwithstanding the foregoing, both the National CSIRT and the competent sectoral authority may request relevant updates on the situation.

The Regulation on Reporting of Incidents with Significant Effects in force since 1 March 2025 sets out the specific content that each report and early warning must contain. In addition, it should be noted that an incident will be considered as managed when the background information provided by the affected institutions allows the Agency to declare it as closed.

2.4 State Responsibilities and Obligations

In the Cybersecurity Framework Law

The heads of service of the state administration agencies shall require information technology service providers to share information on vulnerabilities and incidents that may affect the computer networks and systems of state agencies, and provided that doing so is intended to prevent, detect, respond to, recover from or reduce incidents; or strengthen the level of cybersecurity, while ensuring that the potentially sensitive nature of the information shared is respected.

In order to comply with the above, the contracts for the provision of services may not contain any clause that could restrict or hinder in any way the communication of information about threats by the service provider, as long as this does not compromise the security and protection of data, including confidentiality and protection of intellectual property.

In the State Digital Transformation Law No 21,180

The “Technical Standard for Information Security and Cybersecurity” of the State Digital Transformation Law establishes guidelines and responsibilities for Chilean government bodies regarding information security and cybersecurity.

Responsibilities are structured around key functions:

- identification – bodies must identify and manage security risks associated with their processes, personnel, and electronic platforms;
- protection – implement security measures to ensure proper, timely and secure service delivery;
- detection – develop processes for timely detection of security incidents;

- response – implement technical and organisational measures in response to security incidents; and
- recovery – maintain recovery plans and restore any capacity or service affected by a security incident.

Additionally, each body must:

- conduct an initial cybersecurity assessment;
- develop an Information Security and Cybersecurity Policy;
- appoint individuals responsible for information security and information assets; and
- participate in the gradual implementation of this technical standard depending on the type of entity and the gradual implementation schedule, which will extend until 2028.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

In banking and financial matters, Chapter 20-10 of the Updated Compilation of Standards (RAN) establishes the obligation for financial institutions (mainly banks) to define an organisational structure with specialised and dedicated personnel, with the necessary powers and competencies to manage IT security and cybersecurity. In addition, the function of an information security and cybersecurity officer in charge of these matters must be part of this organisational structure.

The board of directors of banking and financial institutions subject to Chapter 20-10 of the Updated Compilation of Standards (RAN) shall establish the above and other matters in relation to their information security and cybersecurity management systems, such as:

- policies for the management of information security and cybersecurity risks;
- promotion of risk-awareness in terms of information security and cybersecurity;
- permanent monitoring of the infrastructure connected with external providers, and analysis and implementation of measures to detect and mitigate potential threats to the cybersecurity of the entity; and
- internal behaviour policy.

There are a large number of other specific operational risk and cybersecurity regulations applicable to other entities participating in the banking and financial system – eg, mutual fund administrators; entities providing fintech services, including investment advisers or alternative transaction platforms; and even entities that will participate in the Open Finance System, which is being implemented gradually until 2027.

Thus, Chapter 20-10 is of general application to certain financial entities (banks, payment card operators and issuers) but shares several provisions with the specific regulations mentioned above.

3.2 ICT Service Provider Contractual Requirements

The contractual requirements for Information and Communication Technology (ICT) service providers are detailed in Chapters 20-7 and 20-10 of the Updated Compilation of Standards (RAN). The most relevant aspects are described below.

Definition of ICT Service Providers

According to the regulations, a service provider is any entity, related or not to the contracting institution, that provides services or supplies goods and facilities. This includes ICT service

providers. ICT services can range from data processing to the provision of cloud infrastructure.

General Contractual Requirements

- Clear definition of rights and obligations – the contract must clearly specify the responsibilities of both parties.
- Service level agreements (SLAs) – clear and measurable service levels must be established.
- Early termination clauses – the contract must include conditions for the early termination of the contractual relationship.
- Pricing method – the contract must detail an appropriate method for pricing, with a breakdown for each service if several are purchased for a single price.
- Business continuity – the contract must include clauses that guarantee business continuity.
- Information security – clauses must be established on the ownership and confidentiality of information, restrictions on the use of software and the secure deletion of customer data.
- Audits – the CMF and the audited entity must be allowed to examine on-site or remotely all aspects of the contracted service.
- Subcontracting – there must be veto clauses for subcontracting to third parties by the main provider. Also, the subcontracted company must comply with the conditions agreed between the entity and the initial service provider.
- Personnel – the suitability and responsibility of the provider's personnel, as well as the applicable legal and labour aspects, must be clearly established.
- Language – contracts, subcontracts and annexes must be in Spanish or translated into this language.

- Documentation – the operational, administrative and technological procedures of the contracted service must be documented, updated and available for review.
- Location – data, platforms and applications must be in specific processing sites and, in the case of processing abroad, in a defined and known jurisdiction. The city where the data centres operate must be known.

Critical ICT Services

Significant or strategic (critical) activities are considered to be those in which a failure in the provision of the service has a significant impact on regulatory compliance, business continuity, information security, or the quality of the entity's services.

Also considered critical are activities that involve the processing of data subject to secrecy or banking secrecy, activities with a significant impact on risk management, and those with high systemic interaction in the market.

Cloud Service Providers

Not all cloud service providers are automatically classified as critical. The classification depends on the criticality of the service being outsourced to the cloud.

- Non-critical services – can be outsourced in the public or private cloud without additional considerations to those already mentioned in the preceding titles.
- Critical services – in the event that a strategic or critical activity is outsourced to the cloud, enhanced due diligence of the provider and the service must be carried out, which includes:
 - (a) prestige and experience of the provider – the provider must be of recognised prestige and experience;

- (b) certifications – the provider must have independent and internationally recognised certifications in information security management, business continuity and quality of services;
- (c) direct contracts – contracts must be entered into directly between the institution and the provider;
- (d) legal reports – the entity must have legal reports on the regulation of privacy and access to information in the jurisdictions where the service is provided;
- (e) audits – the provider must make audit reports available to the contracting entity and the CMF;
- (f) security – there must be physical and logical security mechanisms that isolate the entity's infrastructure from that of other clients; and
- (g) encryption – sensitive data must have strong encryption mechanisms.

3.3 Key Operational Resilience Obligations

According to Chapter 20-10, the implementation of an adequate risk management process should include as a minimum:

- a risk analysis process, which considers elements such as the assessment of the probability of occurrence of incidents and their consequence or impact on information assets, based on the degree of damage or costs caused by an information security and cybersecurity event, thus determining its level of risk;
- a risk assessment process;
- a risk treatment plan; and
- at least an annual review of the information security and cyber security risk management process.

Moreover, Chapter 20-10 contains a robust set of cybersecurity defensive measures. Within the measures, it is important to highlight the following:

- inventory of critical cybersecurity assets;
- change management process that allows modifications made to the ICT infrastructure to be carried out in a secure and controlled manner;
- capabilities management process;
- technological obsolescence management process;
- configuration management process that ensures adequate controls to the configurable elements of the ICT infrastructure;
- patch management programme to ensure that patches are applied to both software and firmware in a timely manner;
- implementation of tools such as firewalls, web application firewalls (WAF), intrusion prevention systems (IPS), data loss prevention systems (DLP), anti-denial of service systems, email filtering, anti-virus and anti-malware;
- back-up management process to ensure the integrity and availability of information and processing media in the event of an incident or disaster;
- mechanisms to cover the costs associated with possible cyber-attacks; and
- a Security Operation Centre (SOC), either in-house or through an external service, which operates 24 hours a day, with facilities, technological tools, processes and dedicated and trained personnel.

Incident Reporting

The CMF in Chile has established a regulatory framework for the management of operational and cybersecurity incidents in the financial sector, with the aim of protecting users and the stability of the system. This framework applies to

various entities, including banks, card issuers, insurers and fintechs, with specific regulations for each type of entity.

With the entry into force of the Cybersecurity Framework Law, it is expected that there will be co-ordination between the CMF and the ANCI.

- Sanctions – failure to comply with these regulations can result in fines of up to 15,000 UF (approximately USD420,000), which can increase fivefold in the case of repeat offences.
- Incident reporting – all entities regulated by the CMF are required to report operational incidents, although deadlines vary. For example, banks and insurers must do so within 30 minutes of the incident, while some fintech service providers have a deadline of two hours. These reports must include detailed information about the incident, such as its description, date and time, causes, impact on customers and services, and measures taken for mitigation.
- Communication – in general terms, entities should consider the need to inform their customers about incidents that affect the quality of services or that are publicly known. In addition, they should share relevant information about cybersecurity incidents with the rest of the industry, encouraging collaboration and prevention.

3.4 Operational Resilience Enforcement

The CMF requires entities to guarantee access to the information and records of suppliers, both on-site and remotely, even if the supplier is abroad. The CMF reviews the audit reports carried out by the suppliers.

Entities must report to the CMF any operational incident that affects an outsourced ser-

vice, allowing the CMF to supervise the incident response capacity and recovery plans.

In the event of non-compliance with the regulations, the CMF may require that the services be carried out in the country or that the entity execute them internally, ensuring that the entity maintains a plan that allows it to comply with these requirements.

3.5 International Data Transfers

According to Chapters 20-7 and 20-10 of the RAN, entities must have defined specific data processing sites. In the case of processing abroad, the jurisdiction must be defined and known. The city where the data centres operate must be known.

Moreover, if an entity outsources data processing services outside the country, it must have a contingency data processing centre located in Chile and demonstrate a recovery time compatible with the criticality of the outsourced service. There is the possibility of exemption from this requirement if the entity maintains adequate operational risk management and can ensure preventive measures such as a recovery time objective (RTO) approved by the board of directors, sites with adequate availability time, and sites in different locations that mitigate both geographical and political risks.

In addition, if the outsourced service includes the transmission of data outside the country that is subject to secrecy or banking secrecy (according to Article 154 of the General Banking Law), prior authorisation from each client is required.

Regarding country risk, services can only be outsourced in jurisdictions that have an investment grade country risk rating. If the country does not have this rating, the board of directors may make

an exception to this requirement as long as the country has adequate personal data protection and security laws.

Finally, it stands out that communication connections between the entity and the provider must have a level of encryption that ensures the confidentiality and integrity of data from end to end. The processed information must be stored and transported in encrypted form, with the decryption keys held by the entity.

3.6 Threat-Led Penetration Testing

Threat-led penetration testing has not arisen in this jurisdiction.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

The Cybersecurity Framework Law refers to the concept of resilience, defining it as the ability of networks and computer systems to maintain their availability and operation, as well as to recover quickly from cybersecurity incidents.

For its part, the National Cybersecurity Policy 2023–2028 establishes as one of its five fundamental objectives the development of a “resilient infrastructure” in the country. This implies that the country must have a robust information infrastructure prepared to withstand and recover from cybersecurity incidents and socio-environmental disasters. To advance this objective, the need to strengthen essential services and improve the response capacity to incidents, both in the public and private sectors, is established.

However, neither the National Cybersecurity Policy nor the Cybersecurity Framework Law specifically establish detailed obligations related to cyber-resilience. It is expected that in the

future, the National Cybersecurity Agency will issue general and specific instructions to promote cyber-resilience in the country, especially taking into account the advancement of this type of regulation in the world and the fact that the Cybersecurity Framework Law is especially inspired by the Network and Information Security Directives 1 and 2 of the European Union.

4.2 Key Obligations Under Legislation

For more information, see 4.1. **Cyber-Resilience Legislation.**

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

The Cybersecurity Framework Law establishes a cybersecurity standards certification scheme, mainly focused on operators of vital importance, although it also affects state bodies.

- Mandatory certification – operators of vital importance must obtain cybersecurity certifications as determined by law and the regulations of the ANCI.
- Authorised certification centres – valid certifications can only be issued by bodies that are registered and authorised by the ANCI. To be part of this register, entities must prove compliance with the requirements established in the regulations and, to remain so, comply with the aforementioned requirements. The Regulation on accredited Certification Centres is expected to be published in the Official Gazette during 2025.
- International certifications – the ANCI may approve international or foreign technical certifications on cybersecurity, by means of a reasoned resolution of its Director.

- Certification of operational continuity and cybersecurity plans – operators of vital importance must prepare and implement operational continuity and cybersecurity plans. These plans must be certified and must be subject to periodic reviews by the obligated parties, with a minimum frequency of two years. The Agency also has the power to request certifications in shorter terms if there are serious supervening reasons.
- Cybersecurity standards for the state – the ANCI will be in charge of certifying compliance with cybersecurity standards by the bodies of the State Administration.

It is expected that there will be greater clarity on the specific certifications that operators of vital importance must have during the first semester of 2025, after the ANCI issues the respective secondary regulations.

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

In matters of personal data protection, Law No 19,628 on the Protection of Private Life from 1999 is currently in force. This law does not specifically establish cybersecurity obligations. At most, it contains a provision stating that the party responsible for records or databases where personal data is stored after collection must take due care, making them liable for any damages.

Currently, there isn't a single supervisory authority for personal data protection. The Undersecretariat of Telecommunications, the Financial Market Commission, and the Council for Transparency in the public sector have issued regulations or recommendations that, in some sense,

also consider the adoption of cybersecurity measures.

One of the most relevant of these authorities is the National Consumer Service (SERNAC), which, thanks to the Pro-Consumer Law, is – temporarily – the supervisory authority for personal data protection within consumer relations. This is until the new Personal Data Protection Law and the new Data Protection Agency come into effect in December 2026.

SERNAC has issued interpretative circulars on the law, which, while not binding for providers, are binding for SERNAC officials in charge of oversight. This could lead to infringement complaints before the courts (SERNAC does not have direct sanctioning powers). Among the most important circulars are the following.

- Interpretative Circular on good practices in electronic commerce – security in electronic contracting. SERNAC stated that providers of services and products through electronic means must inform and adopt necessary technical measures to guarantee consumer security, integrity and confidentiality of transactions, payment methods and personal data. This includes indicating the levels of protection applied to each. Additionally, SERNAC considers that companies must take corresponding safeguards in cases of electronic contracting by minors, vulnerable consumers, or those who lack the capacity to understand the information provided on the website.
- Interpretative circular on criteria of equity in the stipulations contained in adhesion contracts referring to the collection and processing of personal data of consumers – abusive clauses that make the consumer responsible for the effects of possible deficiencies, omissions, or errors, such as limiting the liability of

the supplier in case of unauthorised access, losses, alterations, or leaks of the consumer's personal data. SERNAC considers that the duty of professionalism falling on suppliers, considering the obligation of security in data processing, entails applying comprehensive security measures. This includes technical, organisational and human capital formation to safeguard the confidentiality, integrity, and availability of consumers' personal data to prevent alteration, loss, transmission and unauthorised access.

In the field of consumption, SERNAC has interpreted that providers responsible for processing consumers' personal data must compensate for damage caused by collection, processing, use, disclosure or other processing operations when they have not met the security and professionalism standards of Law No 19,496 on the protection of consumer rights and 19,628 on the protection of privacy.

New Personal Data Protection Law

After extensive legislative discussion that took over seven years, Law No 21,719 was enacted, reforming Law No 19,628. This new law will come into force in December 2026, along with the creation of the National Personal Data Protection Agency. From that moment on, SERNAC will cease to be the controlling authority in this matter.

The new law establishes a Security Principle, according to which the processing of personal data must guarantee adequate security standards, protecting it against unauthorised or illicit processing, loss, leakage, accidental damage or destruction. In addition, security measures must be appropriate and consistent with the type of processing and the nature of the data.

Furthermore, the new law recognises the principle of data protection by design and by default, according to which the data controller must implement technical and organisational measures from the design of the processing of personal data and during its execution, taking into account the state of the art, the costs of implementation, the nature of the data, the context and purposes of the processing, as well as the associated risks. Likewise, by default, only the specific personal data strictly necessary for the activity should be processed.

The new law also includes various obligations related to information security and cybersecurity. Thus, the data controller must adopt the necessary measures to guarantee compliance with the security principle, ensuring the confidentiality, integrity, availability and resilience of data processing systems. They must also prevent the alteration, destruction, loss, processing or unauthorised access to data.

Security measures may include:

- pseudonymisation and encryption of personal data;
- guaranteeing the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- ability to restore the availability and access to data quickly in case of incidents; and
- regular processes for verification, evaluation and assessment of the effectiveness of security measures.

In addition, the data controller must report to the Agency any security breach that results in the destruction, leakage, loss or unlawful alteration of data, or unauthorised access to it, especially if there is a risk to the rights of data subjects.

- These communications must be recorded, detailing the nature of the breach, its effects, categories of data, the approximate number of data subjects affected and the measures taken.
- If the breach affects sensitive personal data, data of children under 14 years of age or relating to financial obligations, the data controller must notify the data subjects. If individual notification is not possible, it must be done through a mass media outlet with national reach.

Finally, the data controller must prove the existence and functioning of the implemented security measures in case of dispute.

6.2 Cybersecurity and AI

On the subject of cybersecurity and AI, there are no specific regulations in Chile. Therefore, general rules apply, including the Cybersecurity Framework Law and any specific or general instructions that the National Cybersecurity Agency may issue in this regard.

However, the National Consumer Service (SERNAC), the – temporary – controlling authority for personal data protection in the context of consumer relations, issued an interpretative circular regarding AI systems and consumer safety. It is important to remember that these circulars are not generally binding but only apply to SERNAC officials in the context of supervisory activities, which could result in a complaint being filed with the courts (SERNAC does not have direct sanctioning powers).

In the Interpretative Circular on consumer protection against the use of AI systems – consumer safety, SERNAC has interpreted that, in view of the general obligation incumbent on suppliers to provide security to consumers, AI systems in the

context of a consumer relationship must present adequate standards of precision, reliability and technical effectiveness to obtain well-founded results and to avoid causing harm to consumers of a material or immaterial nature.

Thus, suppliers must act responsibly and with due diligence, which implies the need for a prior and continuous assessment of the risks that may arise for consumers from the use of AI systems. In the context of the protection of personal data, SERNAC interprets that in accordance with the regulations on protection of personal data, the data controller responsible for the processing must undertake this processing with “due diligence” (Article 11, Law No 19,628), assuming responsibility for the damages caused.

Specifically, SERNAC interprets this duty as translating into the need to apply appropriate technical and organisational security measures, which guarantee the confidentiality, integrity and availability of the personal data in question, considering especially the risks involved in the processing activities and the nature of the data stored (including, among other elements, their level of sensitivity).

6.3 Cybersecurity in the Healthcare Sector

In matters of health services, the Decree No 6/2022 of the Ministry of Health established the “Regulation on actions related to health care carried out remotely”, which is applicable to both public and private health providers. Thus, health providers who provide their services remotely must:

- guarantee the secure transmission of data and clinical information necessary for the granting of the benefit, using reliable mechanisms and reusable formats that integrate rules for the protection of personal data, the reservation of the clinical record, biomedical ethics, and the rights and duties of patients;
- ensure the traceability and registration of actions carried out with the support of ICTs;
- have specific procedures for ensuring confidentiality, according to the action or benefit granted;
- have privacy risk management plans, which allow the provider to minimise the risks associated with security breaches, especially if it is feared that this has resulted in some improper access or disclosure, alteration or modification of personal data relating to patients;
- keep a record of information security incidents; and
- report cyber-incidents to the Information Security Committee (CSI) of the Ministry of Health.

HUNGARY

Law and Practice

Contributed by:

Adam Liber and Tamás Bereczki
PROVARIS Varga & Partners



Contents

1. General Overview of Laws and Regulators p.93

- 1.1 Cybersecurity Regulation Strategy p.93
- 1.2 Cybersecurity Laws p.95
- 1.3 Cybersecurity Regulators p.98

2. Critical Infrastructure Cybersecurity p.101

- 2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.101
- 2.2 Critical Infrastructure Cybersecurity Requirements p.101
- 2.3 Incident Response and Notification Obligations p.104
- 2.4 State Responsibilities and Obligations p.105

3. Financial Sector Operational Resilience Regulation p.108

- 3.1 Scope of Financial Sector Operational Resilience Regulation p.108
- 3.2 ICT Service Provider Contractual Requirements p.108
- 3.3 Key Operational Resilience Obligations p.109
- 3.4 Operational Resilience Enforcement p.109
- 3.5 International Data Transfers p.110
- 3.6 Threat-Led Penetration Testing p.111

4. Cyber-Resilience p.111

- 4.1 Cyber-Resilience Legislation p.111
- 4.2 Key Obligations Under Legislation p.111

5. Security Certification for ICT Products, Services and Processes p.111

- 5.1 Key Cybersecurity Certification Legislation p.111

6. Cybersecurity in Other Regulations p.112

- 6.1 Cybersecurity and Data Protection p.112
- 6.2 Cybersecurity and AI p.112
- 6.3 Cybersecurity in the Healthcare Sector p.113

PROVARIS Varga & Partners is an independent Hungarian law firm comprising five partners and more than 20 lawyers with a prominent international clientele. The firm's lawyers are highly qualified legal experts with outstanding business and academic backgrounds and specialised knowledge in the fields of dispute resolution, technology and digitalisation, data protection, intellectual property, projects and

energy, life sciences, public procurement, corporate and commercial law, real estate, European and constitutional law, tourism and sports law. The firm serves clients across a wide range of sectors and takes great pride in the widespread recognition of its services. The team continues to attract domestic and international clients by providing outstanding legal services.

Authors



Adam Liber is a seasoned partner at Provaris, specialising in data protection, IT, intellectual property, and competition law. With over fifteen years in the field, he co-leads legal teams

and is a certified intellectual property expert. He holds LL.M. degrees in Global and US Business Law and Competition Law, along with various international data protection certifications. Adam advises multinational corporations on EU data protection laws, oversees complex outsourcing transactions, and manages international data transfers. He represents clients across multiple sectors in investigations, audits, and disputes involving digital technology and compliance. Additionally, Adam is an external expert for the European Data Protection Board's Support Pool and serves on the Legal Advisory Committee of the ADR Forum at the Council of Hungarian Internet Service Providers.



Tamás Bereczki is a partner at Provaris, specialising in data protection, cyber-law, information security, IT and technology matters. Tamás has hands-on experience in

information security management, risk assessments, ISO 27001 management systems, privacy frameworks, incident and cybersecurity management, third-party risk management, cloud service risk management in the financial, aviation, pharmaceutical and e-commerce industries. He holds degrees in Law and Computer Science and CISM, CRISC certifications from ISACA and a CIPP/E certification from the International Association of Privacy Professionals. Tamás is a co-chair of the IAPP KnowledgeNet Hungary Chapter and was admitted as an expert to the European Data Protection Board's Support Pool of Experts.

PROVARIS Varga & Partners

H-1053 Budapest
Károlyi street 9.
Central Palace
5th Floor
Hungary

Tel: +36 706 051 000
Email: info@provaris.hu
Web: www.provaris.hu



1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy The 2013 Cyber Strategy and its Implications

Hungary adopted a dedicated cybersecurity strategy in 2013 through Government Decision 1139/2013 (21 March) on Hungary's National Cybersecurity Strategy ("2013 Cyber Strategy"). The 2013 Strategy aimed to align with constitutional principles and national interests while addressing the challenges of the digital age. It set national goals, strategic directions, and government measures to ensure a free and secure cyberspace, protect national sovereignty, and safeguard economic and societal activities. The strategy emphasised securely adapting technological innovations, fostering international co-operation, and strengthening governmental co-ordination to address cybersecurity threats. It also integrated core values such as freedom, security, and the rule of law, aligning with Hungary's National Security Strategy, EU and NATO cybersecurity principles, and the Budapest Convention on Cybercrime.

This previous 2013 Cyber Strategy paved the way for the Hungarian Parliament and the gov-

ernment to adopt legislation such as the Act L of 2013 ("Information Security Act") on the Electronic Information Security of State and Municipal Bodies, and its executive regulation, namely Decree 42/2015 (VII. 15.) of the Ministry of Interior on the Procedure for the Official Registration of Certain Organisations Covered by the Act on Electronic Information Security. The Information Security Act aimed to protect national electronic data assets, critical information systems, and their components, recognising their importance in addressing modern threats. Ensuring the confidentiality, integrity, and availability of data and systems is a societal expectation essential for safeguarding cyberspace.

NIS1 Implementation

Later, Hungary implemented the Directive (EU) 2016/1148 (NIS Directive) in various laws, including the Act CVIII of 2001 on Certain Issues of Electronic Commercial Services and Information Society Related Services (E-commerce Act). Detailed rules regarding cybersecurity event management and supervision were laid down in Government Decree 270/2018 (XII. 20.) on the Supervision of the Electronic Information Security of Information Society Services and the Procedure on Security Events. Further to this,

critical assets and pieces of critical infrastructure were defined in Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Facilities.

The 2020 National Security Strategy

Hungary updated its National Security Strategy in 2020 (Government Decision 1163/2020) to address significant changes in the global security environment since 2012. The strategy highlights factors such as a shifting world order, climate change, migration, resource depletion, and technological advancements. It emphasises preserving security levels, national values, economic priorities, and defence industry development to ensure Hungary's stability and growth amid global, European, and national challenges.

Cybersecurity features prominently in the updated strategy, which recognises cyberspace as a critical operational domain alongside land, sea, air, and space. It underscores the increasing frequency and sophistication of cyber threats, including attacks on critical systems by state and non-state actors such as cybercriminal groups and international terrorist organisations. The strategy prioritises enhancing resilience to hybrid attacks through national unity, strong democracy, efficient decision-making, and collaboration across defence, law enforcement, and civilian infrastructure. Key measures include bolstering cybersecurity to protect critical information infrastructure and governmental IT systems, addressing risks, and fostering public-private partnerships. The strategy highlights the importance of AI-based systems' secure development, international co-operation, and the establishment of global norms for cyberspace security. It considers cyber capabilities causing physical harm or material damage as weapons, warranting potential physical responses, with attribution requiring careful governmental evaluation.

Hungary's approach focuses on strengthening cybersecurity through enhanced regulations, sectoral alignment with national security goals, and partnerships to address rising cyber threats targeting governmental platforms, utilities, and critical infrastructure.

NIS2 Implementation and Harmonisation of Requirements

In line with its National Security Strategy, Hungary has enacted several pieces of legislation to implement the EU's NIS2 Directive into Hungarian law. This included the Act XXIII of 2023 on Cybersecurity Certification and Supervision ("2023 Cybersecurity Act"), MK Decree 7/2024 (VI. 24.) on Security Classification Requirements ("MK Decree"), and SZTFH Decree 23/2023 (XII. 19.) on the cybersecurity register of affected entities. However, due to significant shortcomings in implementing NIS2 Directive requirements in the 2023 Cybersecurity Act, the European Commission initiated an infringement procedure against Hungary for failing to fully transpose the NIS2 Directive and ensure the protection of critical infrastructure and the resilience of critical entities. Consequently, Act No LXIX of 2024 on Hungary's Cybersecurity ("2024 Cybersecurity Act"), published in Hungarian Official Journal No 130 on 20 December 2024, and effective as of 1 January 2025, repealed the 2023 Cybersecurity Act. Additionally, Act No LXXXIV of 2024 on the Resilience of Critical Organisations ("Critical Infrastructure Act"), published in Official Journal No 131 on 20 December 2024, also took effect on 1 January 2025, albeit in stages, repealing the 2012 Act on the Identification, Designation, and Protection of Critical Systems and Facilities.

Several lower-level pieces of legislation, such as the presidential decree of the supervisory authority regarding the applicable audit methodology and auditor fees, are not yet published.

1.2 Cybersecurity Laws

General

In general, requirements regarding the cybersecurity-related protection and processing of personal data are laid down in the EU's General Data Protection Regulation and in general, organisations processing personal data must comply with privacy by design, privacy by default and data security requirements laid down by Article 32 GDPR.

NIS2 Regulations

As opposed to the legislative landscape in 2024 and previous years, the 2024 Cybersecurity Act, its executive regulation, the Government Decree 418/2024 (XII. 23.) on the Implementation of the 2024 Cybersecurity Act ("Execution Decree") and the MK Decree harmonised requirements for both private and public sector entities falling within the scope of the 2024 Cybersecurity Act. According to the justification to the draft of the 2024 Cybersecurity Act, the Act "uniformly regulates the legal framework for defense against cyberattacks and harmonizes it with European Union legislation. At the same time, it establishes a new and effective defense structure that simplifies the protection of state information systems and provides guidance for market players as well." According to the justification for the proposal, "[t]he transposition of the NIS2 Directive into Hungarian law was initiated by Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision (hereinafter: Cybersecurity Act). However, considering the increasing number of cyberattacks and incidents affecting various sectors across Europe, the state organizational framework dealing with cybersecurity has been reviewed, and it has become expedient to unify the fundamental cybersecurity rules in a single law."

The 2024 Cybersecurity Act, along with its Execution Decree and the MK Decree, harmonised requirements for both private and public sector entities. These include administrative bodies, state-owned enterprises, entities designated as essential or important but not covered under the 2024 Cybersecurity Act or the EU Digital Operational Resilience Act (DORA), NIS2 entities qualifying as at least medium-sized enterprises, and entities covered by NIS2 regardless of their size. The 2024 Cybersecurity Act also introduced changes to the scope of entities covered by the 2023 Cybersecurity Act. While the 2023 Act applied to all food businesses, including retailers, the 2024 Act limits its scope to food businesses involved in wholesale distribution, industrial production, and food processing. Additionally, holders of pharmaceutical wholesale distribution authorisations under Article 79 of Directive 2001/83/EC are excluded from the new legislation, though pharmaceutical wholesalers remain covered.

The 2024 Cybersecurity Act does not apply to electronic information systems handling classified data, operational electronic information systems, programmable systems covered by the government decree on physical protection and related licensing, reporting, and inspection in the application of nuclear energy, and cybersecurity services provided by entities designated in a separate government decree. Furthermore, the 2024 Cybersecurity Act did not implement Annex I, Section 3 (banking sector) and Annex I, Section 4 (financial market infrastructures) of the NIS2 Directive, as these fall within the scope of DORA.

The 2024 Cybersecurity Act is applicable to the following entities:

- organisations established in Hungary or represented by a local representative;
- electronic communications service providers offering services in Hungary; and
- DNS providers, top-level domain registries, domain name registration providers, cloud service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, online marketplace operators, online search engines, and social media platforms, whose main business establishment is in Hungary.

An organisation's main business establishment is considered to be in Hungary if:

- decisions regarding cybersecurity risk management measures are predominantly made in Hungary;
- cybersecurity operations for the organisation's electronic information systems are conducted in Hungary; or
- the organisation's largest workforce is based in Hungary.

Non-Hungarian organisations operating electronic information systems under the 2024 Cybersecurity Act must appoint a Hungarian-based representative responsible for compliance, without affecting the organisation's or its head's liability.

The head of the entity must establish and operate a risk management framework for protecting electronic information systems, adhering to applicable EU laws or national regulations where EU laws do not apply. Periodic reviews, includ-

ing security classifications, must occur at least every two years. Key responsibilities include:

- registering and assessing all electronic information systems, central services, and supporting systems used by the organisation;
- assigning roles, responsibilities, and appointing a person responsible for system security;
- conducting risk assessments, impact analyses, and security classification of systems;
- implementing proportional protective measures and ensuring compliance with EU and national cybersecurity regulations;
- regularly reviewing protective measures and addressing identified deficiencies;
- overseeing internal cybersecurity assessments and ensuring system security through periodic evaluations; and
- deciding on system usage and complying with cybersecurity authority mandates.

To ensure the protection of electronic information systems, the head of the entity must, among other duties:

- provide training on cybersecurity responsibilities for themselves and staff, including mandatory and continuing education as specified by the responsible minister;
- ensure participation in mandatory national cybersecurity exercises or conduct independent exercises;
- maintain traceability of events within electronic information systems;
- ensure third-party service providers comply with cybersecurity requirements through contractual obligations when involved in system creation, operation, auditing, maintenance, or incident handling;
- respond swiftly and effectively to cyber threats, incidents, or near-incidents, including reporting to the cybersecurity incident

response centre and overseeing recovery efforts;

- notify affected parties promptly about cybersecurity incidents and potential threats;
- implement recommendations and guidelines from the cybersecurity authority and incident response centre;
- strive to execute tasks outlined in the legislation as quickly as possible;
- allocate at least 5% of the organisation's annual IT development budget to cybersecurity improvements for applicable organisations; and
- take any additional necessary measures to safeguard electronic information systems.

Organisations must classify their electronic information systems as “basic”, “significant”, or “high” security classes to ensure proportional protection for their systems, data, and services. Classification is based on the risks to system integrity and availability, as well as the confidentiality, integrity, and availability of the data processed. The organisation's head is responsible for making the classification decision, ensuring compliance with regulations, and verifying the completeness and timeliness of the data used. The classification results must be documented in the organisation's system registry or internal policies. The security classification must be reviewed at least every two years or promptly following any legally defined changes affecting the system's security, with the review process documented. Further details are set out in the MK Decree.

The head of the entity must appoint an individual responsible for the security of electronic information systems or enter into an agreement with an external party to fulfil these responsibilities. This includes operating the risk management framework, reporting cybersecurity incidents,

and liaising with the cybersecurity incident response centre. For certain organisations, the mandatory elements of such agreements are specified in the Execution Decree. Even when outsourcing, a designated individual must be named as the responsible person. The role can only be performed by someone who is legally competent, has a clean criminal record, and, for specific organisations, meets the qualifications, certifications, or experience requirements outlined by the decree of the minister responsible for IT.

Enterprises under majority state ownership that exceed the thresholds defined for medium-sized enterprises and entities covered by Annex 2 and Annex 3 of the 2024 Cybersecurity Act (whose scope corresponds to Annex I and Annex II of the NIS2 Directive) must conduct a cybersecurity audit every two years to demonstrate compliance with the 2024 Cybersecurity Act's requirements. Additionally, audits may be mandated by the competent cybersecurity authority. Organisations are required to enter into an agreement with an auditor listed in the supervisory authority's registry within 120 days of their registration and conduct their first cybersecurity audit within two years of their registration. The related audit methodology and auditor fee regulation is not yet published.

Requirements regarding risk management, risk assessment methodology, security classification and technical and organisational controls are detailed in the MK Decree, while the Execution Decree sets out procedural and detailed requirements regarding entities falling within the scope of the 2024 Cybersecurity Act.

Financial Sector

Cybersecurity-related requirements, including mandatory and regular audits of relevant sys-

tems and procedures, are outlined in Government Decree 42/2015 (III. 12.) on the Protection of IT Systems for Financial Institutions, Insurance and Reinsurance Companies, and Investment Firms and Commodity Exchange Service Providers. Additionally, EU-level legislation, such as the PSD2 Directive, has been incorporated into Hungarian law through amendments to various financial sectoral regulations. From 17 January 2025, the DORA regulation, governing cybersecurity and supply chain risk management requirements alongside Government Decree 42/2015 (III. 12.), came into effect in Hungary.

Healthcare Providers

Public and private healthcare providers must connect to the Electronic Health Service Space (EESZT). IT systems used to connect to the EESZT must comply with strict requirements, including with regard to secure access, identification, communication protection, service handling, and adherence to technical and security standards. Developers with appropriate rights can apply for authorisation, specifying the system's intended use. Authorised systems must ensure continuous compliance during updates, version changes, or technical modifications for system integration, with significant changes reported within eight days. Operators monitor system performance to verify ongoing compliance, with the authority to revoke authorisation if requirements are unmet. Additionally, operators maintain and publish a registry of authorised systems for transparency. These regulations aim to enhance the security, functionality, and reliability of IT systems, ensuring they meet technical and operational standards.

Criminal Law

Act C of 2012 on the Criminal Code defines penalised behaviours related to cybersecurity, such as intercepting electronic communica-

tions, computer abuse, and fraud committed using computer devices. Act LXXVIII of 2024 on Combating Online Aggression, which entered into force on 1 January 2025, amends the Criminal Code to introduce the offence of "Internet Aggression". This offence penalises publishing or using expressions, depictions, or audio-visual content via electronic communication networks that express intent or desire for violent crimes (causing death or extreme cruelty) against identifiable persons, with up to one year of imprisonment unless a more severe crime is committed. Exceptions are provided for educational, scientific, artistic, or informational purposes, as long as the act does not incite fear.

1.3 Cybersecurity Regulators

NIS2

Under the 2024 Cybersecurity Act, the cybersecurity oversight of electronic information systems under this law is handled by:

- the national cybersecurity authority, the Special Service for National Security (*Nemzetbiztonsági Szakszolgálat*, NBSZ) designated by government decree for systems of administrative bodies, state-owned enterprises, entities designated as essential or important but not covered under the 2024 Cybersecurity Act or DORA (the NBSZ operates independently, with sole accountability to legal regulations, and performs its tasks autonomously, free from instructions, except for directives to complete tasks or address omissions);
- the SZTFH for systems of NIS2-related organisations not covered by the above; and
- for defence-related electronic information systems, the defence cybersecurity authority within the defence sector, the Hungarian Minister of Defence is responsible; its operations follow the regulations applicable to the national cybersecurity authority.

The NBSZ is responsible for a wide range of tasks to ensure the security of electronic information systems. Key responsibilities include:

- verifying compliance of individuals responsible for system security and registering their qualifications;
 - reviewing and approving security classifications for systems and ensuring compliance with relevant regulations and standards;
 - issuing guidelines, recommendations, and technical requirements for system security and mandating adherence to international and European standards;
 - addressing and rectifying identified security deficiencies and monitoring the effectiveness of corrective measures;
 - overseeing system security during development and approving their deployment while restricting usage if requirements are unmet;
 - managing cybersecurity incidents, notifying the incident response centre, and participating in national and international cybersecurity exercises and events;
 - representing Hungary in EU and international cybersecurity bodies;
 - identifying critical or important organisations and recommending their designation to the relevant authorities;
 - organising or mandating cybersecurity drills for organisations and issuing guidance on their exercises.
- The SZTFH:
- defines guidelines, recommendations, and requirements for the security of electronic information systems;
 - may issue guidance on the compatibility of protective measures specified in EU legislation and regulations issued by the minister responsible for IT;
 - ensures compliance with electronic information security requirements, may mandate the application of relevant European and international standards and technical specifications for the security of electronic information systems, without prescribing or favouring specific technologies;
 - verifies compliance with statutory or self-defined requirements for the classification of electronic information systems;
 - orders the remediation of security deficiencies identified during inspections or brought to its attention, oversees the implementation of corrective measures, and evaluates their effectiveness;
 - participates in cybersecurity-related exercises and represents Hungary in international cybersecurity exercises upon request;
 - represents Hungary in domestic and international cybersecurity and information security events;
 - may participate in expert evaluations under Article 19 of the NIS2 Directive or initiate evaluations;
 - monitors the Hungarian implementation of the NIS2 Directive;
 - contributes to awareness-raising activities to protect Hungarian cyberspace;
 - may order and verify any measures necessary to mitigate threats to electronic information systems;
 - maintains a registry of reported registration data;
 - conducts extraordinary inspections or orders audits in the event of significant security incidents or suspected non-compliance;
 - may request and review, for oversight purposes, the following from organisations:
 - (a) documents supporting the appropriateness of security classifications and measures;
 - (b) reports on internal IT security audits; and

- (c) other documents, data, or information confirming regulatory compliance.

The cybersecurity authority is authorised to take supervisory actions or apply legal consequences for:

- organisations providing services in Hungary or operating network and information systems located in Hungary, based on mutual assistance requests from other EU member states' cybersecurity authorities; and
- organisations providing services in Hungary without a designated representative in any EU member state.

Additionally, the authority may prioritise its supervisory tasks based on risk analysis to effectively fulfil its legally defined responsibilities. The detailed rules for conducting oversight inspections are determined by a decree issued by the president of the SZTFH.

Generic Data Security Requirements for Personal Data

The Hungarian Data Protection and Freedom of Information Authority (NAIH) supervises data protection-related matters. The NAIH is one of the most numerous staffed data protection authorities in EU member states, and data protection enforcement in Hungary is rigorous and stringent. However, investigations usually initiated upon individual complaints and ex officio inspections are quite rare. Penalties that the NAIH may apply are defined by the Information Act, the GDPR and the Hungarian Sanctions Act. The GDPR imposes two tiers of fines for non-compliance: lower-level penalties up to EUR10 million or 2% of worldwide annual turnover, for issues like data security and co-operation with authorities, and upper-level penalties up to EUR20 million or 4% of annual turnover, for seri-

ous infringements like violating data subjects' rights and unlawful data transfers. These fines are discretionary, considering factors like the infringement's nature and any mitigating actions taken by the organisation.

Financial Sector

The Hungarian National Bank (MNB) supervises entities within the financial sector, including banks, insurance companies, payment providers, etc. The MNB also takes a very rigorous and stringent approach to compliance with applicable financial regulations and laws. It is well-known for its extensive written guidance that also covers cybersecurity requirements, cloud services and outsourcing within the financial sector and acts as actual "soft law" and represents the MNB's legal interpretation of applicable laws.

The MNB regularly conducts audits on actors within the financial sector, which also include thorough IT audits and reviews. During an audit, the MNB assesses if a financial institution follows the MNB's guidance, has the required documentation in place that can confirm compliance with applicable cybersecurity requirements (eg, conducting penetration tests on banking systems, software, consumer-facing applications, conducting regular user access reviews, holding the necessary information security trainings and awareness campaigns, etc).

The MNB enforces financial regulations by imposing fines, restricting banking operations, and in severe cases, suspending or revoking licences. It can also mandate corrective actions, issue public warnings affecting an institution's reputation, and initiate legal proceedings. These measures ensure compliance and stability in Hungary's financial sector, with penalties based on the severity of violations, impact on

the financial system, and the institution's past conduct. Furthermore, the MNB is empowered to impose fines not only on the inspected organisation itself, but also on its leadership and any individual classified as holding a senior position under applicable laws. The level of fines varies according to numerous circumstances, with different ranges applicable depending on the specifics of the case.

E-Privacy

The NMHH is in charge of the enforcement of e-privacy-related data security requirements applicable to public electronic communication service providers and can audit service providers in an administrative procedure. The NMHH Decree No 4/2012 (I. 24.) lays down the specific rules concerning data protection and confidentiality obligations related to the provision of public electronic communication services in Hungary and the decree is the local implementation of the EU ePrivacy Directive.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

The Critical Infrastructure Act, announced in Hungarian Official Journal No 131 on 20 December 2024, and technically effective from 1 January 2025, requires the designation authority to initiate procedures by 30 April 2025 to review and potentially revoke or uphold decisions made under the 2012 Act on the Identification, Designation, and Protection of Critical Systems and Facilities. Operators of critical system elements designated under the 2012 Act will continue to be treated as critical organisations until a final decision is made. Additionally, the Critical Infrastructure Act repealed the 2012 Act on the Identification,

Designation, and Protection of Critical Systems and Facilities.

The Critical Infrastructure Act regulates measures to enhance the resilience of critical organisations headquartered in Hungary, along with their support and supervisory systems. It applies to critical organisations, critical infrastructures, participating individuals and entities, administrative bodies, and relevant sectors and organisations. Additionally, the provisions of the Critical Infrastructure Act apply to the natural gas, hydrogen, and electricity subsectors, with exceptions as specified within the law. Furthermore, the Critical Infrastructure Act applies to the electricity transmission components of nuclear facilities in relation to electricity generation as an essential service. Its provisions do not affect EU treaties or regulations specifically governing nuclear elements. Measures, support, and supervisory systems aimed at enhancing the resilience of nuclear facility components fall under the authority of the regulatory body responsible for the peaceful, safe, and secure use of nuclear energy.

2.2 Critical Infrastructure Cybersecurity Requirements

The provisions of the Critical Infrastructure Act for critical organisations and critical infrastructures must be applied with priority given to the national legislation transposing the NIS2 Directive, meaning the 2024 Cybersecurity Act, the Execution Decree and the MK Decree.

Basic Principles and Obligations of Critical Organisations

In organising the resilience of critical organisations and implementing the tasks defined in the Critical Infrastructure Act, the following principles must be upheld by critical organisations and individuals:

- The resilience of critical organisations is a key component of the national resilience system.
- Ensuring the continuity of essential services and the resilience of critical organisations and infrastructures is a national interest.
- Authorities, critical organisations, and individuals must respect each other's rights and cooperate in good faith.
- Critical organisations must consider available resources, risks, and the impacts of extraordinary events when meeting resilience requirements.
- Attention must be given to cross-border interdependencies of essential services, critical infrastructures, organisations, subsectors, and sectors.
- Data related to critical organisations must be accessed only by those with a legitimate need for their duties, with confidentiality obligations persisting even after the relationship ends, and must not be disclosed to unauthorised individuals.
- Measures regarding the resilience of critical organisations must comply with the principle of proportionality, being necessary and appropriate to achieve the desired goal.
- In matters involving nuclear energy, the authority of the nuclear regulatory body must be respected, and safety must take precedence over all other considerations.

Critical organisations must enhance their resilience while ensuring the continuous delivery of essential services. The responsibility for maintaining and improving resilience, as well as implementing necessary measures, rests with the critical organisation. Resilience assessments and improvements should consider national risk assessments, resilience plans, risk management strategies, emergency prevention and recovery measures, physical security, organisational specifics, and applicable regulations. To

fulfil resilience requirements, authorised security personnel may inspect individuals, vehicles, and objects entering or leaving critical infrastructure, and restrict or prevent access if necessary. Employees, suppliers, and contractors must cooperate and fulfil assigned tasks, while employees in critical roles must adhere to the resilience plan. Suppliers are required to meet the organisation's standards, and individuals entering facilities must comply with organisational restrictions. These measures aim to safeguard critical infrastructure and enhance national resilience.

Risk Management

Critical organisations must assess, identify, evaluate, and manage risks that may impact the secure and continuous operation of critical infrastructure and the delivery of essential services. Risk assessments and the development of a resilience matrix must address mandatory general and sector-specific risks and additional risks identified by the organisation. The assessment and matrix must consider the potential consequences of risks that could lead to extraordinary events threatening the secure and continuous operation of the organisation and infrastructure. The detailed criteria for risk assessment and resilience matrix development are defined by government decree.

Resilience Plan and Responsible Person for the Resilience of a Critical Organisation

Critical organisations must prepare a resilience plan and its accompanying resilience matrix by the deadline set by the designation authority. These documents must be completed using a standardised form provided by the authority and submitted electronically for approval.

The general designation authority, with input from sector-specific or energy-related authorities, evaluates the submitted plan and matrix

for compliance with content and format requirements. General sections are reviewed by the general authority, while sector-specific sections are assessed by the relevant sectoral or energy authorities.

The resilience plan must include:

- a description of the critical organisation, infrastructure, and essential services;
- the rules, organisational structures, and tools ensuring service continuity and operational resilience; and
- risk assessments, resilience matrices, and measures to maintain and restore operations.

The plan must undergo regular annual reviews and immediate updates following significant changes, extraordinary events, or regulatory findings. Updates follow the same procedures as the initial submission. Sector-specific criteria are outlined by the sectoral authorities and updated as needed. For nuclear facilities, sector-specific requirements apply only to components related to electricity transmission.

Furthermore, critical organisations must establish the position of chief resilience officer (CRO) within 90 days of a designation decision. This individual shall report directly to the organisation's leadership and ensure compliance with resilience-related tasks. The organisation must submit details about the leader's qualifications, appointment, and any changes to the registry authority within eight days. This person is responsible for co-ordinating with authorities, conducting risk assessments, updating resilience plans and matrices, and evaluating the organisation's resilience. They organise co-ordination among units impacting resilience and regularly report to organisational leadership.

Each critical infrastructure and essential service operated by the organisation must have a designated CRO, who must meet qualification and background requirements. For nuclear facilities, the CRO must operate under senior management, adhering to specific nuclear requirements. The CRO may also join the advisory committee for CROs or register independently with the authority if not employed by a critical organisation. Individuals failing to meet required qualifications, training, or background checks cannot be registered.

Resilience Exercises

Critical organisations must conduct resilience exercises to evaluate the effectiveness of their resilience plans and capabilities. These include:

- **Regular Resilience Exercises:** These are held annually from the year following designation, addressing extraordinary event management at all sites and specific risks at at least one site.
- **Complex Resilience Exercises:** These are conducted in collaboration with the designation authority, focusing on the suitability of organisational and operational systems and cooperation with other entities during emergencies.
- **Stress Tests:** These are participated in upon request by the designation authority.

The organisation's CRO evaluates and documents exercise results, ensuring compliance with legal and regulatory obligations. Exercises may lead to updates of the resilience plan. Designated personnel must participate in all exercises and tests, with notifications sent at least 14 days in advance.

For nuclear facilities, other exercises specified by the OAH (Hungarian Atomic Energy Authority)

can fulfil resilience requirements if they meet relevant regulations. Non-compliance may result in mandated revisions to the exercise procedures or the necessity to repeat the exercises.

2.3 Incident Response and Notification Obligations

NIS2-Related Security Events

Administrative bodies, state-owned enterprises, entities designated as essential or important but not covered by the 2024 Cybersecurity Act or DORA, as well as those covered under the 2024 Cybersecurity Act, must promptly report all threats, near-cybersecurity incidents, and cybersecurity incidents, including operational cybersecurity incidents, to the NBSZ, which serves as the National Cybersecurity Incident Response Centre (CERT).

NIS2-relevant organisations under the 2024 Cybersecurity Act are specifically required to report incidents that significantly disrupt operations or services, cause substantial financial harm to the organisation, or result in significant financial or non-financial damage to others. Additionally, these organisations may voluntarily report cybersecurity incidents that fall below the mandatory reporting threshold.

All reporting must adhere to the procedures outlined in the applicable government decree.

Organisations must submit an initial cybersecurity incident report without undue delay and within 24 hours of becoming aware of the incident. The report should include the following information, if available:

- identification of the affected electronic information system;

- a brief description of the incident, including whether it qualifies as an operational cybersecurity incident;
- the status, duration, and geographical extent of the incident;
- the expected recovery time, if estimable;
- details of the affected data type, nature, and user impact;
- the extent of service disruption and potential cross-border effects;
- contact details of the designated liaison handling the incident;
- information on intermediary or central service providers involved;
- whether the incident is intentional; and
- any other relevant information to assess cross-border impacts.

Furthermore, organisations must comply with the following reporting requirements for cybersecurity incidents:

- report infection indicators as soon as such metrics become available;
- within 72 hours of becoming aware of the incident, submit an updated notification that includes information from the initial report and provides a preliminary assessment of the incident's severity and impact;
- provide status updates upon request from the NBSZ;
- submit a detailed final report within one month of the event notification, including:
 - (a) a comprehensive description of the incident, its severity, and impact;
 - (b) likely causes or threats behind the incident;
 - (c) mitigation measures implemented or ongoing; and
 - (d) cross-border impacts, if applicable;

- if the incident is unresolved when the final report is due, submit an update on progress; and
- within one month after resolving the incident, submit a final report summarising all actions and outcomes.

Organisations are exempt from reporting near-cybersecurity incidents and operational cybersecurity incidents that are automatically resolved during the incident management process without degrading services. However, repeated near-incidents or operational incidents must still be reported.

Additionally, trust service providers must notify the NBSZ without undue delay and within 24 hours of becoming aware of any cybersecurity incidents that impact their trust services.

Critical Infrastructure-Related Events

Critical organisations must report extraordinary events according to their resilience plan. Reporting requirements vary by resilience level:

- Level 1 organisations must report immediately, within four hours during working hours, or by 12:00 PM the next working day if the event occurs outside working hours.
- Level 2 and 3 organisations must report immediately, within four hours of detection.

Reports must be submitted using the designated form provided by the National Directorate General for Disaster Management of the Ministry of Interior, being the general designation authority. Notifications are sent to:

- Mandatory for All:
 - (a) regional disaster management authority; and
 - (b) general designation authority.

- Sector-Specific:
 - (a) ministry-designated sectoral duty service; and
 - (b) contact point specified by the sectoral authority.
- Energy Sector:
 - (a) energy designation authority for critical organisations or infrastructures.

These authorities notify the National Incident Management Centre as outlined in the law on defence and security co-ordination.

Critical organisations must notify their CRO about extraordinary events in the format and manner specified by the responsible. Reporting requirements, content, and submission rules are defined by government decree. After resolving the event, the CRO must submit a detailed report to the organisation's leadership, relevant designation authorities, and sectoral bodies, who forward it to the NBSZ. Reports include the event's origin, actions taken, and preventive measures for similar incidents.

Extraordinary events are analysed to enhance response, defence, and recovery efforts for critical organisations. Maintenance and repairs related to critical infrastructure must prioritise minimising service disruptions. Annual reports on controlled extraordinary events must also be submitted by the CRO to the relevant authorities. For incidents impacting six or more EU member states, authorities notify the affected states' contact points and the European Commission, adhering to confidentiality to protect security and business interests.

2.4 State Responsibilities and Obligations

The Critical Infrastructure Act defines the following responsibilities for the Hungarian state.

National Strategy for Enhancing the Resilience of Critical Organisations

The National Strategy for the Resilience of Critical Organisations is a medium-term strategic planning document issued by the government. Based on the National Security Strategy and other sectoral strategies, it outlines goals and measures to enhance the general resilience of critical organisations and ensure the continuity of essential services. Key elements include:

- strategic objectives and priorities considering cross-border and sectoral interdependencies;
- governance frameworks defining roles and responsibilities of critical organisations and involved authorities;
- measures to strengthen resilience and procedures to support critical organisations;
- actions to promote public-private collaboration;
- identification of key authorities, stakeholders, and processes for co-ordination; and
- a policy framework for co-ordinating cybersecurity risks, threats, and incidents under NIS2 compliance.

The strategy is reviewed every four years and provided to the European Commission within three months of its adoption.

National Risk Assessment for Enhancing the Resilience of Critical Organisations

The National Risk Assessment for Critical Organisations' Resilience (National Risk Assessment), approved by the Hungarian government, serves as a planning document to support the resilience of critical organisations and infrastructure. It covers:

- sectors listed in Annex 1 of the Critical Infrastructure Act;
- Hungary's national disaster risk assessment;

- general and sector-specific risks and defence plans;
- EU-based regulations addressing terrorism, energy supply security, flood risk, and hazardous materials;
- tasks related to defence and security planning under national law; and
- reporting and management of extraordinary events.

The assessment evaluates critical organisations' development of risk evaluations, resilience matrices, and resilience measures. It is reviewed every four years, and relevant information is submitted to the European Commission within three months of adoption.

Designation of Critical Organisations

The process for designating critical organisations in Hungary is governed by a comprehensive framework designed to ensure national resilience and the continuity of essential services. This involves evaluating both horizontal and sector-specific criteria to identify organisations that play a critical role in maintaining societal and economic stability. Horizontal criteria include factors such as the organisation's dependency on or relationship with other critical entities, its financial significance (eg, annual revenue exceeding HUF10 billion), or its role as the sole provider of a critical service in Hungary. Sector-specific criteria address risks and dependencies within specific industries, such as energy, transportation, or public health.

Designation authorities, in collaboration with sectoral authorities, monitor and evaluate the resilience of sectors, subsectors, and infrastructures. They initiate the designation process based on national resilience strategies, risk assessments, and relevant data. Organisations meeting the criteria are categorised into one of

three resilience levels, determined by the scope and impact of their services, geographic coverage, and the number of users reliant on their operations. These levels dictate the organisation's obligations to ensure preparedness and continuity in the face of extraordinary events.

Designation decisions are reviewed every four years or sooner if significant changes occur in the organisation's status or the broader operating environment. Critical organisations must comply with tailored obligations, including the development of resilience plans and implementation of specific measures to address identified risks. The designation process also emphasises cross-sectoral and cross-border dependencies, ensuring a comprehensive approach to resilience. The decisions are formally communicated to relevant oversight bodies, sectoral authorities, and stakeholders, including those responsible for cybersecurity and emergency communications. This collaborative and structured approach supports the integration of critical organisations into Hungary's national resilience framework, ensuring the continuity of essential services and preparedness for potential threats.

Designation of Critical Infrastructure

The process of designating critical infrastructure involves organisations providing data on their infrastructure and identifying those considered critical. The designation authority, with input from sectoral authorities, designates infrastructure as critical if it is essential for the basic services provided by a critical organisation, is located within Hungary, and meets at least one horizontal or sectoral criterion. The resilience level of the critical infrastructure is determined in the designation decision. A critical infrastructure cannot be designated in multiple sectors or subsectors. If eligible under multiple sectors, its

designation is based on the primary essential service it supports.

Supervision of Critical Organisations

The oversight of critical organisations and infrastructure is carried out by a designated supervisory authority through comprehensive inspections. These inspections are conducted regularly, periodically, and on an ad hoc basis, often involving relevant sectoral authorities to ensure a thorough evaluation. The primary focus is on assessing compliance with applicable laws, regulations, and directives issued by the designation authority. The inspections aim to verify the effectiveness of measures taken to maintain and enhance the resilience of critical organisations and infrastructure. Key elements of these evaluations include the adequacy of resilience plans, risk assessments, resilience matrices, leadership performance, and the organisation's collaboration with supply chain partners and other entities.

Sector-specific oversight is also conducted independently by sectoral authorities with expertise in their respective areas. These inspections follow an agreed methodology, and their plans are finalised annually after consultations with the supervisory authority. This ensures consistency and alignment with broader resilience objectives.

Resilience leaders within critical organisations play a crucial role in ensuring compliance and readiness through internal audits. They are responsible for evaluating the implementation of resilience measures, the accuracy of resilience plans, and the organisation's overall preparedness. If any deficiencies are identified, they are required to propose corrective actions to senior management or the organisation's leadership.

To further strengthen resilience and mitigate human risks, organisations may request background checks for key personnel responsible for resilience. These checks confirm the individual's identity and ensure they have a clean criminal record.

Supporting Critical Organisations

The framework for supporting critical organisations aims to enhance their resilience by providing resources, guidance, and collaboration opportunities. Key measures include the following:

- development and dissemination of manuals, templates, and methodological tools, accessible via the central designation authority's website;
- sharing best practices for resilience measurement and testing, organising central training programmes and sector-specific workshops for CROs;
- assigning advisers or creating advisory working groups to assist critical organisations;
- organising regular events to update organisations on regulatory changes, case studies, and best practices, facilitated by the designation authority and the CRO Advisory Committee, with input from sectoral authorities;
- offering expedited administrative processes and, where necessary and justified by public interest, financial aid for resilience development; and
- encouraging voluntary information sharing among critical organisations and publishing scientific research to support knowledge dissemination.

Additionally, the registry authority may verify the critical status of organisations, critical roles, and essential resources to facilitate access to support measures. If necessary and justified by pub-

lic interest, financial support may be provided to enhance the resilience of critical organisations.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

Act X of 2024 on the Harmonisation Amendments to Laws Affecting the Financial Intermediary System ("DORA Implementation Act") implemented DORA into Hungarian law. The implementation act greatly broadened the material scope of the application of DORA in Hungary to include all financial enterprises, insurance companies, payment service providers, stock exchanges and investment fund managers.

Most enterprises must comply with the simplified framework, except for banks, institutions that operate payment systems, are under consolidated supervision, or subject to equivalent prudential regulations, which must adhere to the full framework.

3.2 ICT Service Provider Contractual Requirements

The supervisory authority issued guidance on public cloud services in 2019 (MNB Guidance 4/2019 (IV. 1.)), which remains in effect until revoked. This guidance requires all financial enterprises to conduct a preliminary risk assessment and prepare an exit strategy before entering into contracts with any public cloud service providers. Additionally, the use of cloud services must be reported to the MNB.

It is expected that the MNB will align its practices with those of the ESAs regarding the use of cloud service providers, particularly in assess-

ing their criticality. However, details have not yet been communicated to the public.

3.3 Key Operational Resilience Obligations

DORA mandates all financial enterprises in Hungary to enhance their ICT risk management frameworks, with particular emphasis on third-party risk management. Before 17 January 2025, and at the time of writing, existing sector-specific laws, notably Government Decree 42/2015 (III. 12.) on the Protection of the IT Systems of Financial Institutions, Insurers, Reinsurers, Investment Firms, and Commodity Exchange Service Providers, already require financial enterprises to maintain a robust, closed, trusted, and secure IT environment, including considerations for physical security and business continuity.

The Government Decree mandates financial institutions to establish robust IT security frameworks to ensure resiliency and business continuity. These include regular risk assessments, proportional protective measures for IT systems, and secure operations supported by independent monitoring and robust controls. Institutions must implement comprehensive data back-up and recovery plans, maintain redundancy for critical services, and ensure the secure separation of development, testing, and production environments.

Compliance with national cybersecurity standards is required, along with the use of secure digital archiving solutions to preserve electronic records. Vulnerability assessments and mitigation plans are mandatory for high-security systems, with logging and monitoring mechanisms in place for incident management. Business continuity plans must address extraordinary events to minimise disruption and ensure service continuity. These measures collectively strengthen

operational stability and align with national and international cybersecurity standards.

The MNB has issued guidance on outsourcing requirements (MNB Guidance No. 7/2020 (VI. 3.)), emphasising the importance of conducting preliminary risk assessments, maintaining documented and tested exit strategies, and performing annual audits of outsourced service providers. Additionally, the MNB issued guidance on IT system security (MNB Guidance No. 8/2020 (VI. 22.)), which provides further details on the requirements established by the above-mentioned Government Decree.

DORA will expand the scope of these requirements, mandating financial enterprises to assess all ICT service providers. These providers must now be classified based on the criticality of their services concerning confidentiality, integrity, availability, and authenticity, thereby introducing a significant new element to the legislative framework.

3.4 Operational Resilience Enforcement

The MNB has extensive authority to enforce effective regulations in Hungary, including conducting regular audits of financial institutions. As part of these audits, the MNB also oversees technical and organisational compliance with its issued guidance, particularly on outsourcing, the use of public cloud services, and IT system security. Additionally, the MNB audits compliance with Government Decree 42/2015 (III. 12.) on the Protection of IT Systems of Financial Institutions, Insurers, Reinsurers, Investment Firms, and Commodity Exchange Service Providers. In practice, this includes a comprehensive IT and IT security audit that evaluates the effectiveness of technical and organisational controls and ensures alignment with the institution's own risk assessment.

3.5 International Data Transfers

Generally, the international data transfer provisions of the GDPR apply to the extent personal data is concerned by the international data transfer. Various financial sectoral provisions lay down additional requirements for international data transfers, such as those applicable to bank secrets, insurance secrets and securities secrets.

Bank Secrets

Under Section 54(1)(h) of Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises, the transfer of data constituting bank secrets from a financial institution to a foreign financial institution is permissible provided all the following conditions are met:

- **Client's Written Consent:** The client (data subject) must provide explicit written consent for the data transfer.
- **Adequate Data Protection Measures:** The foreign financial institution (data controller) must ensure that data processing conditions meet the requirements set forth by applicable laws and directly applicable legal acts of the European Union for each piece of data.
- **Adequate Data Protection Legislation:** The country where the foreign financial institution is headquartered must have data protection laws that satisfy the requirements imposed by applicable laws and directly applicable legal acts of the European Union.

Insurance Secrets

Under Section 140(1) of Act LXXXVIII of 2014 on Insurance Activities, the transfer of insurance secrets by an insurer or reinsurer to a third-country insurer, reinsurer, or data processor is permissible under the following conditions:

- the data subject (client) has provided explicit written consent for the data transfer; or
- in the absence of the data subject's consent, the data transfer complies with the regulations governing the transfer of personal data to third countries.

Securities Secrets

Under Section 120(e) of Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, the transfer of securities secrets by an investment firm or commodity dealer to a foreign investment firm or commodity dealer is permissible provided all the following conditions are met:

- the client has explicitly consented to the data transfer;
- the foreign investment firm or commodity dealer ensures that data processing conditions meet the requirements set forth by applicable laws and directly applicable legal acts of the European Union for each piece of data; and
- the country where the foreign investment firm or commodity dealer is headquartered has data protection laws that satisfy the requirements imposed by applicable laws and directly applicable legal acts of the European Union.

The MNB issued its Guidance 4/2019 (IV. 1.) on the use of public cloud services, which stipulates that institutions utilising public cloud services for data processing, storage, or management must establish appropriate safeguards in compliance with national and EU legal frameworks. These safeguards require data controllers and processors to handle, process, and store client data and financial sector secrets strictly in accordance with the principle of purpose limitation, ensuring that data is used only to the extent and for the duration necessary to fulfil the

intended purpose. Furthermore, if personal data is involved, institutions must ensure full compliance with applicable international and national data protection laws and regulations.

3.6 Threat-Led Penetration Testing

At the date of writing, DORA is not yet applicable and the MNB has not published any written guidance or requirement on conducting threat-led penetration testing (TLPT) in the Hungarian financial sector.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

See 1. General Overview of Laws and Regulations.

4.2 Key Obligations Under Legislation

See 1. General Overview of Laws and Regulations.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

The 2024 Cybersecurity Act establishes requirements for both cybersecurity certifications and certification bodies. The 2024 Cybersecurity Act incorporates the requirements of the EU Cybersecurity Act into Hungarian law.

The Hungarian National Cybersecurity Certification System aims to safeguard data and ICT processes across their life cycle by ensuring protection against unauthorised access, modification, or destruction and implementing mechanisms for data confidentiality, integrity, and availability. It mandates robust security measures, such as

logging access, detecting vulnerabilities, and enabling secure recovery post-security incidents. ICT products and services must be inherently secure by design, regularly updated, and supported with mechanisms for secure updates.

The system also specifies comprehensive certification requirements, including defining the scope, objectives, standards, reliability levels, and evaluation criteria. It establishes guidelines for self-assessment, compliance evaluation, and certification validity, including renewal and extension conditions. Evaluations cover technical elements like vulnerability testing, cryptographic assessments, and security source code analysis, ensuring documentation and post-certification monitoring.

The national cybersecurity certification system defines three reliability levels – basic, substantial, and high – for ICT products, services, and processes. These levels indicate compliance with security requirements and the degree of evaluation undertaken to mitigate risks. Basic reliability addresses fundamental and known risks, substantial focuses on cybersecurity risks posed by attackers with limited resources, and high reliability aims to counter advanced cyberattacks using state-of-the-art techniques.

Evaluations involve reviewing technical documentation at all levels. For substantial and high levels, additional assessments verify the absence of vulnerabilities and test security functionality. High-level certification includes advanced penetration testing to ensure resilience against skilled attackers. The reliability level must align with the risk associated with the intended use of the ICT solution.

The national cybersecurity certification authority in Hungary, primarily the SZTFH, oversees certi-

fication for ICT products, services, and processes, except for defence-related areas, which are managed by a government-designated authority. Responsibilities include monitoring European cybersecurity certification developments, participating in related standardisations activities, and maintaining national certification systems. These systems must align with EU standards and address evolving security risks.

The authority evaluates and revises national certification systems at least every three years, or immediately following significant developments, ensuring alignment with European frameworks. It supervises conformity assessment bodies (CABs), conducts inspections, and ensures that cybersecurity certifications meet high standards, particularly for “high” reliability levels.

Additionally, the authority manages a national registry of certification-related data, including technical documentation, certifications, and compliance details. It ensures data security, confidentiality, and compliance with applicable laws. Violations by CABs or manufacturers can result in warnings, penalties, or license revocation.

All actions and decisions by the certification authority adhere to strict confidentiality and data protection standards, with records maintained for up to ten years post-certification expiry. The SZTFH ensures compliance through audits, accreditation, and collaboration with the European Commission for maintaining EU-wide standards.

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

The NAIH oversees compliance with data protection laws, including GDPR requirements for data security (Article 32) and privacy by design and data protection by default (Article 25). The NAIH collaborates with other Hungarian authorities, such as the Hungarian Competition Office and the MNB. It is expected that the NAIH will also co-ordinate with the NBSZ and SZTFH on cybersecurity-related matters.

The 2024 Cybersecurity Act emphasises that incident reporting obligations under the Act do not exempt organisations from fulfilling other reporting obligations. As a result, organisations will likely need to review and align their internal data breach management and reporting procedures to meet both data protection and cybersecurity requirements.

Under the GDPR, data processing agreements must include provisions for defining, requiring, and auditing technical and organisational measures (TOMs) to ensure compliance with Article 32. Similarly, the 2024 Cybersecurity Act, particularly Section 19 of Annex 2 to the MK Decree, mandates that organisations contractually require third-party service providers to comply with the organisation’s cybersecurity requirements. These requirements must be based on risk assessments and security classifications. To avoid contractual conflicts, organisations are advised to harmonise these cybersecurity requirements with their existing TOMs.

6.2 Cybersecurity and AI

In Hungary, apart from the EU AI Act there are no specific cybersecurity requirements exclusively for AI systems. However, the 2024 Cybersecu-

Act outlines requirements for administrative bodies, state-owned enterprises, and entities designated as essential or important, which also apply to software and system development. These requirements must be adhered to when procuring or developing AI solutions.

Additionally, Hungary has not yet established a dedicated AI supervisory authority. Data protection-related requirements for the use and development of AI systems are currently overseen by the NAIH.

6.3 Cybersecurity in the Healthcare Sector

In general, the EU Medical Device Regulation's cybersecurity requirements apply to medical devices.

Moreover, public and private healthcare providers must connect to the Electronic Health Service Space (EESZT). IT systems used to connect to the EESZT must comply with strict requirements, including secure access, identification, communication protection, service handling, and adherence to technical and security standards. Developers with appropriate rights can apply for authorisation, specifying the system's intended use.

Authorised systems must ensure continuous compliance during updates, version changes, or technical modifications for system integration, with significant changes reported within eight days. Operators monitor system performance to verify ongoing compliance, with the authority to revoke authorisation if requirements are unmet. Additionally, operators maintain and publish a registry of authorised systems for transparency. These regulations aim to enhance the security, functionality, and reliability of IT systems, ensuring they meet technical and operational standards.

Trends and Developments

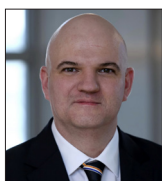
Contributed by:

Adam Liber and Tamás Bereczki
PROVARIS Varga & Partners

PROVARIS Varga & Partners is an independent Hungarian law firm comprising five partners and more than 20 lawyers with a prominent international clientele. The firm's lawyers are highly qualified legal experts with outstanding business and academic backgrounds and specialised knowledge in the fields of dispute resolution, technology and digitalisation, data protection, intellectual property, projects and

energy, life sciences, public procurement, corporate and commercial law, real estate, European and constitutional law, tourism and sports law. The firm serves clients across a wide range of sectors and takes great pride in the widespread recognition of its services. The team continues to attract domestic and international clients by providing outstanding legal services.

Authors



Adam Liber is a seasoned partner at Provaris, specialising in data protection, IT, intellectual property, and competition law. With over fifteen years in the field, he co-leads legal teams

and is a certified intellectual property expert. He holds LL.M. degrees in Global and US Business Law and Competition Law, along with various international data protection certifications. Adam advises multinational corporations on EU data protection laws, oversees complex outsourcing transactions, and manages international data transfers. He represents clients across multiple sectors in investigations, audits, and disputes involving digital technology and compliance. Additionally, Adam is an external expert for the European Data Protection Board's Support Pool and serves on the Legal Advisory Committee of the ADR Forum at the Council of Hungarian Internet Service Providers.



Tamás Bereczki is a partner at Provaris, specialising in data protection, cyber-law, information security, IT and technology matters. Tamás has hands-on experience in

information security management, risk assessments, ISO 27001 management systems, privacy frameworks, incident and cybersecurity management, third-party risk management, cloud service risk management in the financial, aviation, pharmaceutical and e-commerce industries. He holds degrees in Law and Computer Science and CISM, CRISC certifications from ISACA and a CIPP/E certification from the International Association of Privacy Professionals. Tamás is a co-chair of the IAPP KnowledgeNet Hungary Chapter and was admitted as an expert to the European Data Protection Board's Support Pool of Experts.

PROVARIS Varga & Partners

H-1053 Budapest
Károlyi street 9.
Central Palace
5th Floor
Hungary

Tel: +36 706 051 000
Email: info@provaris.hu
Web: www.provaris.hu



Analysing the Transition: From the 2023 Cybersecurity Act to the 2024 Cybersecurity Act in Hungary

Introduction

The NIS2 Directive, enacted by the European Union, represents a significant advancement in EU-wide cybersecurity legislation. Effective from 16 January 2023, this Directive expanded the scope of cybersecurity regulations to encompass a broader range of sectors and entities. Its primary goal was to bolster organisational cybersecurity across various industry ecosystems throughout the EU, requiring entities to adopt robust measures to secure their networks and information systems. It mandated that EU member states integrate these provisions into their national laws by 17 October 2024.

However, as of 28 November 2024, the European Commission identified that 23 member states, including Hungary, had failed to meet this deadline. Despite the European Commission's statement, Hungary was a forerunner in adopting the NIS2 Directive, implementing it through Act XXIII of 2023, known as the Cybersecurity Certification and Cybersecurity Supervision Act ("2023 Cybersecurity Act"). This Act, in line with the NIS2 Directive, defined a broad range of sectors subject to the new legislation. The 2023

Cybersecurity Act entered into force gradually by 17 October 2024 and required the registration of covered entities, the security classification of electronic information systems, and the implementation of certain cybersecurity measures in line with the MK Decree 7/2024 (VI. 24.) on the Requirements of Security Classification.

The authority designated to enforce the NIS2 requirements was the Supervisory Authority for Regulated Activities (*Szabályozott Tevékenységek Felügyeleti Hatósága*, or SZTFH). The deadline for registration before the SZTFH under the 2023 Cybersecurity Act was 30 June 2024 for entities that had already commenced operations prior to 1 January 2024. All other entities had to register within 30 days from starting the relevant operations. The SZTFH reviewed over 3,500 registration applications by the end of 2024 and also maintained the register for NIS2 auditors. The SZTFH was authorised to release delegated legislation on audit requirements, audit fees, and payment of the cybersecurity supervision fee.

However, the NIS2 implementation provided by the Act was incomplete and had several deficiencies and gaps. Therefore, the Hungarian government decided to replace the 2023

Cybersecurity Act with new legislation, providing a more complete implementation of the NIS2 Directive. The cybersecurity landscape in Hungary has undergone significant transformations with the replacement of the 2023 Cybersecurity Act by the 2024 Cybersecurity Act, which was passed by the Hungarian Parliament on 17 December 2024. This transition aligns with the broader implementation of the NIS2 Directive. While the 2023 Cybersecurity Act marked Hungary's initial compliance with NIS2, the 2024 Cybersecurity Act introduces a more unified and robust framework, addressing gaps and reflecting lessons learned from prior implementation.

This article examines the key changes and their implications for entities operating in Hungary.

Key changes in the legislative framework

Consolidation of Cybersecurity Legislation

The 2024 Cybersecurity Act, effective from 1 January 2025, consolidates Hungary's cybersecurity legal framework by repealing the 2023 Cybersecurity Act and other fragmented regulations, including Act CXXV of 1995 (Sections 8(7)–(10)) on the National Security Services and Act L of 2013 on Electronic Information Security of State and Municipal Bodies (Information Security Act). This consolidation aims to provide unified rules for entities in both the public and private sectors, addressing the implementation gaps of the 2023 Cybersecurity Act.

As part of the NIS2 implementation efforts, the Hungarian government also released Government Decree 418/2024 (XII. 23.) on the Implementation of the 2024 Cybersecurity Act. This decree outlines the specific obligations of organisations concerning cybersecurity measures, the framework for governmental oversight, and the procedures for compliance. It also delineates the roles of various authorities in monitoring and

ensuring adherence to cybersecurity standards, including the supervision of designated auditors responsible for assessing compliance among affected organisations. Additionally, the decree addresses co-operation between national and international entities in the realm of cybersecurity, aligning with relevant EU directives and regulations. The primary objective of this decree is to ensure a high level of national cybersecurity, protect critical infrastructure, and facilitate effective responses to cyber threats.

Enhanced sectoral scope, main establishment and representative appointment

The 2024 Cybersecurity Act introduced certain changes to the scope of entities previously covered by the 2023 Cybersecurity Act. Public administration bodies at various local levels are now explicitly included, and the new law also applies to the electronic information systems of enterprises under majority state ownership that exceed the thresholds defined for medium-sized enterprises in the Small and Medium-Sized Enterprises Act.

Similarly to the former legislation, the 2024 Cybersecurity Act distinguishes between organisations operating in sectors with high criticality (Annex 2 of the 2024 Cybersecurity Act) and organisations operating in sectors at risk (Annex 3 of the 2024 Cybersecurity Act), introducing minor but significant changes in its scope. While the 2023 Cybersecurity Act extended its scope to all food businesses, including food retailers, the 2024 Cybersecurity Act limited its applicability to food businesses engaged in wholesale distribution, industrial production, and processing of food. Holders of a pharmaceutical wholesale distribution authorisation under Article 79 of Directive 2001/83/EC are no longer covered by the scope of the new legislation, but pharmaceutical wholesalers are. Research organisations

under educational institutions remain excluded from the scope of the 2024 Cybersecurity Act.

The 2023 Cybersecurity Act did not regulate main establishment, territorial scope, or representatives, and its scope did not cover public sector entities. The new law aimed to fill this gap. Under the 2024 Cybersecurity Act, the new law applies to:

- organisations established in Hungary or represented by an established representative in Hungary;
- electronic communications service providers offering services in Hungary; and
- entities such as DNS service providers, top-level domain registries, domain name registration providers, cloud service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines, and social media platforms whose main establishment of business is in Hungary.

According to the 2024 Cybersecurity Act, an organisation's main establishment of business is in Hungary for entities if: (i) decisions related to cybersecurity risk management measures are predominantly made in Hungary; (ii) cybersecurity operations related to the organisation's electronic information systems are conducted in Hungary; or (iii) the organisation's site with the largest number of employees is in Hungary. These new provisions ensure clarity regarding the jurisdiction and establish criteria for entities operating in or offering services within Hungary's regulatory framework.

The 2024 Cybersecurity Act incorporates the provisions of the NIS2 Directive regarding the

appointment of a representative into Hungarian law. Accordingly, an operator of an electronic information system falling under the scope of the 2024 Cybersecurity Act that is not registered in Hungary must appoint a representative operating within Hungary in writing. This representative is responsible for ensuring compliance with the law and bears responsibility under the same rules applicable to the head of the organisation.

Cybersecurity supervision and applicable monetary fines

The 2024 Cybersecurity Act designated different regulators for different sectors according to the types of entities, including the Special Service for National Security (*Nemzetbiztonsági Szakszolgálat*, or NBSZ); the SZTFH and the Hungarian Minister of Defence acts as the cybersecurity authority for the military sector.

The Special Service for National Security (*Nemzetbiztonsági Szakszolgálat*, or NBSZ) is the national cybersecurity authority responsible for supervising the cybersecurity of administrative bodies of the public administration sector (as defined by Annex 1 of the 2024 Cybersecurity Act), enterprises under majority state ownership that exceed the thresholds defined for medium-sized enterprises, and “essential” or “important entities” identified as such by the NBSZ.

The SZTFH continues to supervise entities covered by Annex 2 and Annex 3 of the 2024 Cybersecurity Act which correspond to Annex I and Annex II of the NIS2 Directive. The scope includes entities classified as medium-sized enterprises or those exceeding the thresholds for medium-sized enterprises. Regardless of organisational size, entities that are electronic communications service providers, trust service providers, DNS service providers, top-level domain name registrars, and domain name reg-

istration providers are also covered. The 2024 Cybersecurity Act also grants authority to the SZTFH to issue delegated regulations concerning the following matters:

- cybersecurity supervisory fee payment obligation;
- auditor registration and requirements;
- cybersecurity audit procedures;
- detailed rules for cybersecurity supervision;
- detailed rules for registering economic organisations and individuals authorised to conduct vulnerability assessments; and
- detailed rules for registering organisations authorised to handle cybersecurity incidents.

Government Decree 418/2024 (XII. 23.) on the Implementation of the 2024 Cybersecurity Act specifies the monetary fines that may be imposed on relevant entities. The authority responsible for imposing the fines depends on the supervisory body. The maximum fines stipulated by Government Decree 418/2024 (XII. 23.) for organisations classified as essential entities are up to EUR10 million or 2% of the total global annual turnover for the preceding financial year, whichever is higher. For organisations classified as important entities, it is up to EUR7 million or 1.4% of the total global annual turnover for the preceding financial year, whichever is higher.

Importantly, if the National Authority for Data Protection and Freedom of Information (NAIH) imposes a fine for a violation, the national cybersecurity authority will not impose a fine for the same conduct. However, in justified cases, it may apply other legal consequences. In cases where multiple legal violations occur simultaneously, the maximum fine imposed is the sum of the maximum fines applicable to each individual violation. Payment of the fine does not exempt the offender from criminal or civil liability, nor

does it relieve them of the obligation to rectify the circumstances that led to the imposition of the fine. Furthermore, except for violations that can be immediately remedied, a fine for the same infraction may be re-imposed after two months from the communication of the final decision imposing the previous fine.

Governance and management obligations and personal responsibility

The 2024 Cybersecurity Act also introduced certain changes regarding the governance and management obligations of covered entities. The 2023 Cybersecurity Act imposed obligations on the “upper management”, whereas under the 2024 Cybersecurity Act, cybersecurity management obligations are now imposed on the “head of the organisation”, because the new law assigns accountability to the head of the organisation for cybersecurity compliance and risk management.

The term “head of the organisation” is not defined by the law. Under Hungarian law, this term typically refers to the person responsible for the management and operation of a given organisation, such as a Chief Executive Officer. This role can be fulfilled by an individual or a collective body, depending on the organisation’s structure. This person or body holds the highest authority within the organisation and is accountable for its overall functioning and decision-making processes. The head of the organisation is generally liable for cybersecurity and governance responsibilities in line with the general provisions of civil law and criminal law.

The 2023 Cybersecurity Act did not introduce any qualification requirements for information security officers (ISO). With the 2024 Cybersecurity Act, the appointment of ISOs has become more rigorous. Accordingly, the organisation’s

leader must appoint an ISO for the purposes of risk management, incident handling, and communication, or enter into an agreement with an external individual. The mandatory content of such an agreement is defined by the Government Decree on the Implementation of the 2024 Cybersecurity Act. The role can only be performed by a person who is (i) legally competent; (ii) has a clean criminal record; (iii) holds qualifications, professional certifications, or relevant work experience as defined in a decree issued by the minister responsible for IT. For organisations that are critical or significant from a security perspective, the ISO must possess accredited international qualifications or relevant expertise.

Security and incident reporting obligations

Cybersecurity risk management measures under Article 21 are detailed in the Annexes of MK Decree 7/2024 (VI. 24.) which are based on NIST 800-53 rev. 5. Organisations are required to protect their electronic information systems and the data processed within them proportionally to the associated risks and must classify their relevant systems and data into “basic”, “significant”, or “high” security classes based on the confidentiality, integrity, and availability of the data, as well as the integrity and availability of the systems. Security classification must be reviewed and documented at least every two years or promptly in the event of regulatory or security changes.

Concerned entities must report cybersecurity incidents to the NBSZ as the cybersecurity authority designated as the national Computer Security Incident Response Team (CSIRT) for Hungary. Organisations are also required to report significant cybersecurity threats, near-miss incidents, and incidents, including operational ones, that cause major disruptions or damages, to the CSIRT. Notification timescales and phases are laid down by Section VI of the

Government Decree on the Implementation of the 2024 Cybersecurity Act. The notification deadline is 24 hours after having become aware of the incident, 72 hours for a detailed report, and a final report within one month. The notification shall be made in electronic form as defined by the CSIRT.

Mandatory security audits

The 2024 Cybersecurity Act emphasises regular oversight through biennial cybersecurity audits and mandatory security classifications for state-owned enterprises and organisations operating in sectors with high criticality, and organisations operating in sectors at risk.

The SZTFH does not primarily conduct inspections of the affected organisations – this task will fall to designated auditors. However, the oversight of these auditors remains the responsibility of the SZTFH. The organisation is required to enter into an agreement with an auditor listed in the SZTFH register within 120 days of its registration and conduct the cybersecurity audit for the first time within two years following registration. During the audit, the auditor verifies the classification and the adequacy of protective measures corresponding to the organisation’s assigned security classification. The President of the SZTFH will issue a decree specifying the maximum fee for the audit (excluding VAT), and the procedures for conducting the cybersecurity audit.

Cybersecurity supervision fee payment

Enterprises under majority state ownership that exceed the thresholds defined for medium-sized enterprises. organisations supervised by the SZTFH must pay a cybersecurity supervisory fee as determined by the SZTFH President’s decree, which has not yet been released. The annual cybersecurity supervisory fee is up to 0.015%

of the relevant organisation's net revenue from the previous business year, or if unavailable, the prorated revenue for the current year, capped at HUF10 million (approximately EUR24,200). For entities within the same recognised corporate group or consolidated group under the Civil Code or Accounting Act, the collective annual fee cannot exceed HUF50 million (approximately EUR125,000). The status of operating as a corporate or consolidated group must be verified in line with the SZTFH President's decree. The fee must be paid to SZTFH in the manner and timeframe specified in the decree.

Transitional provisions

The 2024 Cybersecurity Act includes several transitional provisions to facilitate the shift from previous legislation, minimising redundant administrative tasks for organisations already in compliance.

- **Existing Registrations:** Organisations already listed in the registry maintained by the Supervisory Authority for Regulated Activities (SZTFH) are exempt from submitting a new registration. However, these entities must submit a follow-up notification to the SZTFH by 15 February 2025, specifying the EU member states in which they provide their services.

- **First Cybersecurity Audit:** Organisations that commenced operations before 1 January 2025 are required to conduct their first cybersecurity audit by 31 December 2025.
- **Security Classification:** Organisations that have already completed the security classification of their electronic information systems and the data stored, transmitted, or processed are not required to repeat the security classification.

Conclusion

The transition to the 2024 Cybersecurity Act signifies Hungary's commitment to establishing a cohesive and comprehensive cybersecurity framework aligned with EU directives. While the Act introduces enhanced regulatory measures and accountability, it also places significant compliance responsibilities on entities. Organisations must prioritise preparation, leveraging the additional lead time provided for initial audits and classifications. By embracing these changes, entities can strengthen their resilience against cyber threats and contribute to a more secure digital ecosystem in Hungary and the EU at large.

INDIA



Trends and Developments

Contributed by:

Probir Roy Chowdhury and Shivani Bhatnagar
JSA

JSA offers comprehensive data privacy and information security services, leveraging extensive experience in developing and executing multi-jurisdictional compliance strategies. In the event of a cyber-attack or data breach, the first 24 hours are critical. This period demands a sharp focus on forensics and technological response, as well as co-ordination with the board and a range of internal teams, including risk management, IT, legal, compliance, and business continuity. Externally, companies will face strict regulatory reporting requirements, further investigations, and public expectations of

transparency. Having a well-defined response plan, along with proper training to implement it, will build resilience within organisations, helping them avoid common pitfalls and guiding them towards recovery. The JSA team assists in developing the necessary processes to enable a decisive, effective response and offers real-time, practical advice. JSA's extensive network of current and former government and regulatory contacts provides clients with end-to-end support. The team also looks ahead, anticipating any challenges that may arise post-incident.

Authors



Probir Roy Chowdhury is a partner at JSA's TMT team. He is a sought-after industry specialist, with particular expertise in fintech/data protection and cybersecurity.

Probir's niche practice includes product counselling for market-leading technology companies and advising on technology regulation issues, cross-border data flows, and information security. He has extensively advised and assisted clients on various product and service offerings (including payment structure), as well as contractual arrangements with payment aggregators, digital enablement service platforms, and hub-based domestic person-to-person money remittance technology solutions. Probir has been listed as a Next Generation Partner by Chambers and Partners.



Shivani Bhatnagar is a senior data privacy lawyer at JSA, where she specialises in cybersecurity, AI, adtech, social media, and other data-related legal and regulatory matters.

Shivani advises on global data privacy laws, with a particular focus on India's evolving data protection regulations. She also supports clients through product launches, providing strategic advice on innovations involving AI, blockchain, and cloud technologies. In addition, Shivani deals with crisis management and handles cybersecurity incidents, regulatory and governmental inquiries, internal investigations, and litigation related to privacy and security issues.

JSA

18th Floor
SKAV 909
No 9/1
Residency Road
Richmond Circle
Bengaluru 560 025
Karnataka
India

Tel: +91 804 350 3600
Fax: +91 804 350 3617
Email: pro-team@jsalaw.com
Web: www.jsalaw.com



advocates & solicitors

The Indian Cybersecurity Landscape: Rapid Progress and Increased Vulnerabilities

India is at the forefront of a digital revolution, adapting to new technology and improving government services for its people. From pioneering instant payment systems such as [UPI \(Unified Payments Interface\)](#) – which [processes more than 16 billion transactions monthly](#) – to piloting central bank digital currencies, the country has cemented its leadership in digitalising financial ecosystems.

This rapid digitalisation, however, is a double-edged sword. As India accelerates its journey toward becoming a USD1 trillion digital economy by 2030, with digital services projected to contribute [20% of GDP by 2026](#), its expanding cyber frontier has become a magnet for malicious actors. Today, the nation accounts for [13.7% of global cyber-incidents](#).

The Indian government's push to digitalise governance, healthcare, and critical infrastructure has undeniably improved accessibility and efficiency for millions. At the same time, it has also exposed systemic fragilities: a population still

adapting to digital literacy, organisations lagging in cyberhygiene, and sectors such as healthcare and finance – lifelines of the digital economy – emerging as prime targets for ransomware and data extortion. Meanwhile, the rise of AI introduces new complexities, from ethically fraught dilemmas to sophisticated malware capable of evading traditional defences.

Against this backdrop, India's cybersecurity landscape in 2025 is defined by a race between a relentless pace of innovation and an evolving sophistication of threats. While progressive legislation such as the Digital Personal Data Protection Act 2023 (DPDPA) and the updated National Cybersecurity Strategy aim to fortify defences, gaps persist.

Trends in cybersecurity incidents

The cybersecurity environment in India underwent notable changes in 2024, presenting a complex picture of challenges and improvements alike. According to the Data Security Council of India's Cyber Threat Report 2025 (the "Report"), the country experienced significant malware activity while showing enhanced

defensive capabilities. In 2024, India recorded 369.01 million malware detections across 8.44 million endpoints, averaging 702 detections per minute. This represents a reduction from 2023's figures of 400 million detections across 8.5 million endpoints.

More significantly, the number of actual cybersecurity incidents decreased substantially, from approximately 10,500 in 2023 to 7,770 in 2024. Data suggests strengthened cybersecurity measures, as evidenced by an improved incident-to-detection ratio. In 2024, approximately one security incident occurred per 40,400 malware detections, compared to one per 38,000 detections in 2023.

However, the threat landscape has grown more sophisticated, as demonstrated by an increase in behaviour-based malware detections from 12.5% in 2023 to 14.5% in 2024. This indicates that attackers are employing more sophisticated malware and reflects their increasing use of malware that avoids traditional detection by constantly changing its code or hiding in legitimate processes.

Geographically, the threat landscape expanded beyond traditional tech hubs. While states such as Telangana and Tamil Nadu remained primary targets, there was a marked increase in activity in tier-two cities such as Surat and Ahmedabad.

The healthcare sector emerged as the most targeted industry, accounting for 21.82% of all attacks – up from 15% in 2023. This rise is likely driven by the high value of medical data and the essential nature of healthcare systems, which may prompt organisations to be more inclined to pay ransoms. The hospitality (19.6%) and banking sectors (17.4%) also saw significant target-

ing, highlighting the focus on industries handling large volumes of personal and financial data.

India saw a rise in cloud-based detections, accounting for 62% of all detections, which reflects the broader digital transformation across Indian businesses. As more organisations move their operations to the cloud, they are creating new opportunities for attackers to exploit misconfigured or inadequately protected cloud resources.

In terms of malware types, Trojans and infectors remained the most prevalent, constituting 43.25% and 34.10% of detections respectively. These types of malwares often masquerade as legitimate software, tricking users into executing them and providing attackers with backdoor access to systems.

Ransomware attacks continue to pose one of the most acute cybersecurity threats. While the typical approach of stealing and encrypting data remains a primary tactic, there is an increasing trend towards threat actors adopting data extortion tactics whereby data is stolen but not encrypted. This shift reflects a change in the nature of ransomware attacks, moving from traditional encryption-based extortion to more sophisticated data theft and extortion methods.

Ransomware also persistently upholds its position as one of the most pernicious manifestations of cybercrime. A single ransomware security incident emerges for every cluster of 595 detections. That said, the occurrence of a malware incident is considerably less frequent – materialising only once amid a staggering 40,400 detections.

The geopolitical landscape continued to influence cybersecurity threats, with hacktivist

groups and state-sponsored actors targeting critical infrastructure and public utility services. The ongoing conflicts in the Middle East and other regions have also led to increased cyber-activity aimed at undermining India's global standing. Additionally, cyber-activity around key national events (eg, Independence Day and Republic Day) reflects efforts to undermine India's standing on the global stage.

One of the most revealing insights about India's cybersecurity preparedness comes from the Cyber Security Maturity Survey (the "Survey") conducted as part of the Report. The Survey, which involved organisations across India, offers a comprehensive look into critical areas such as cyber-resiliency, preparedness, and priorities. The Survey found that nearly 73% of organisations are unaware if they have ever been attacked and found that 57% lack cyberhygiene practices.

Impact of AI and other emerging technologies

In 2024, AI-driven threats became a significant challenge for Indian organisations owing to their scalability, ability to evade detection, and adaptability against conventional cybersecurity measures. The widespread availability of open-source AI tools and low-cost cloud computing enabled even less-skilled attackers to execute advanced cyber-attacks. Platforms accessible on the dark web simplified the creation of phishing campaigns and [business email compromise \(BEC\) attacks](#), reducing the technical expertise required for such activities.

By way of example, generative AI has been weaponised to craft hyper-personalised phishing emails by scraping publicly available data from social media and corporate websites. There has been a surge in fraud cases where AI-sim-

ulated voices mimicked executives to authorise fraudulent transactions, demonstrating the alarming precision of these tools.

AI-enhanced malware, such as BlackMamba, represents a paradigm shift in cybersecurity threats. Unlike traditional malware, [BlackMamba leverages generative AI](#) to dynamically rewrite its code, evading signature-based detection systems. This adaptability allows attacks to persist undetected, which complicates mitigation efforts for organisations.

Similarly, polymorphic ransomware employs reinforcement learning to alter its behaviour in real-time, targeting critical sectors such as healthcare and finance with increased efficiency. The [healthcare sector](#), already strained by high-value data and operational criticality, witnessed a rise in automated attacks on exposed internet of things (IoT) devices in 2024.

Emerging technologies such as data-centric ransomware signify a strategic shift in attacker priorities. Instead of encrypting data, adversaries now use AI to identify and exfiltrate high-value information, threatening public disclosure unless ransoms are paid. This approach – observed in the [2024 attack on C-Edge Technologies](#), which disrupted 300 rural banks – minimises detection risks while maximising extortion leverage. Concurrently, supply chain compromises through third-party AI vendors and open-source libraries have expanded the attack surface, with malicious code injected via compromised updates or dependencies.

Indian government's efforts

To counter these threats, the Indian government has prioritised regulatory and institutional reforms. The DPDPA mandates stringent safeguards for AI training datasets, requiring explicit

consent for data collection and imposing penalties of up to USD30 million. Complementing this, the [Indian Computer Emergency Response Team \(CERT-In\)'s AI Security Advisory](#) recommends measures to mitigate AI-related threats, including educating users, verifying domains, securing data, and preventing misuse.

International collaboration has also been prioritised, with [India's membership in the Global Partnership on AI \(GPAI\)](#) facilitating cross-border threat intelligence sharing and ethical AI standardisation.

India's position on the global stage: pivotal role of CERT-in

[India has claimed a spot in the Tier-1 category](#) in the latest Global Cybersecurity Index (GCI) 2024, released by the International Telecommunication Union. With a score of 98.49, India is one of 47 countries to be adjudged as a leading nation that has demonstrated commitment to robust cybersecurity practices. Central to this success are the country's progressive legislative frameworks and the operational efficacy of CERT-In.

Among such frameworks, India's legal framework for cybersecurity has also evolved significantly and contributed to this success, anchored by the Information Technology Act 2000 (the "IT Act") and its subsequent amendments. The introduction of the DPDPA further strengthened this framework. By establishing stringent guidelines for data controllers, enforcing organisational and technical safeguards and standards, and imposing penalties for non-compliance, the DPDPA addresses growing concerns around data security in the digitised economy. These legislative measures have been instrumental in aligning India's cybersecurity governance with global standards, earning high marks in the GCI's legal pillar.

India's technical capabilities, particularly through CERT-In, have been pivotal to its Tier-1 status. Established in 2004, CERT-In operates as the national nodal agency for cybersecurity and is tasked with safeguarding India's digital infrastructure, co-ordinating incident responses, and fostering a secure cyber ecosystem. Its mandate spans across threat analysis, vulnerability management, and collaboration with domestic and international stakeholders. CERT-In follows a structured approach to addressing reported incidents, which has significantly enhanced India's capability to manage cybersecurity challenges, as follows.

Incident reporting

As per the [CERT-In Cyber Incident Reporting Guidelines](#), organisations are legally obligated to report certain types of high-severity cybersecurity incidents within six hours. Upon notification, CERT-In may request access to logs, system records, and other forensic data to assess the breach's scope and impact. This process enables targeted mitigation strategies while maintaining a collaborative, non-punitive approach. By prioritising risk mitigation over penalties, CERT-In encourages transparency and proactive reporting among entities.

Proactive organisational engagement

Larger organisations with established cybersecurity practices and significant customer bases in India often proactively report incidents to CERT-In. This is driven by the recognition that timely reporting can help mitigate risks and prevent further damage. CERT-In's responsive and supportive approach encourages organisations to engage with the agency.

Incident management support

CERT-In is known for its proactive and efficient approach to handling reported cybersecurity

incidents. Upon receiving a notification, the agency typically acknowledges the incident promptly and provides a detailed response within 24 hours, thereby ensuring timely action. In certain cases, CERT-In officials often directly reach out to the reporting entity to gather additional information or offer immediate guidance.

Clearly, the agency's support is comprehensive and multifaceted, encompassing technical assistance, remedial measures, and follow-up actions. By way of example, CERT-In provides technical expertise to help organisations contain and mitigate the impact of cyber-incidents. This includes identifying vulnerabilities, recommending patches, and guiding recovery efforts to restore normal operations.

Additionally, CERT-In issues specific recommendations to address incidents and prevent their recurrence. This was demonstrated during the 2017 WannaCry ransomware attack, where the agency played a pivotal role in co-ordinating the response and issuing advisories to affected organisations.

Multi-stakeholder co-ordination

To tackle cybercrimes effectively, CERT-In often works closely with law enforcement agencies to investigate incidents and take down malicious phishing websites. Additionally, CERT-In collaborates with sector-specific regulators, particularly in critical infrastructure sectors such as banking, healthcare, and energy.

Beyond national borders, CERT-In actively engages in international co-operation. It has signed memoranda of understanding (MoUs) with agencies in countries such as Singapore, Japan, and the UK.

Conclusion

India's cybersecurity landscape in 2025 presents a dual narrative of progress and vulnerability. Advancements such as a 26% reduction in cybersecurity incidents and India's Tier-1 ranking in the GCI highlight strides in policy and technical capabilities. Legislative frameworks and the operational efficiency of CERT-In reflect institutional efforts to align with global standards. These measures have strengthened incident response, particularly in critical sectors such as finance and healthcare, where mandatory reporting protocols have been put in place.

However, emerging threats – particularly AI-driven attacks – continue to challenge this progress. The rise of adaptive malware (eg, BlackMamba), AI-generated phishing campaigns, and data-centric ransomware underscores the ability of adversaries to exploit technological advancements. Sectors such as healthcare (targeted in 21.8% of attacks) with limited cybersecurity infrastructure remain disproportionately vulnerable. Geopolitical tensions and state-sponsored attacks further strain cybersecurity defences, as seen in incidents targeting critical infrastructure during national events.

The path forwards hinges on systemic collaboration. While CERT-In's incident management framework and international partnerships demonstrate proactive governance, gaps persist. Bridging these gaps requires scaling capacity-building initiatives, enforcing regulatory mandates such as the DPDPA, and integrating AI-driven threat detection into national strategies. India's cybersecurity future will depend on balancing innovation with equitable resilience to ensure that its digital ambitions are not derailed by evolving risks.



Law and Practice

Contributed by:

Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiaro
ICT Legal Consulting

Contents

1. General Overview of Laws and Regulators p.130

- 1.1 Cybersecurity Regulation Strategy p.130
- 1.2 Cybersecurity Laws p.130
- 1.3 Cybersecurity Regulators p.131

2. Critical Infrastructure Cybersecurity p.133

- 2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.133
- 2.2 Critical Infrastructure Cybersecurity Requirements p.135
- 2.3 Incident Response and Notification Obligations p.137
- 2.4 State Responsibilities and Obligations p.139

3. Financial Sector Operational Resilience Regulation p.140

- 3.1 Scope of Financial Sector Operational Resilience Regulation p.140
- 3.2 ICT Service Provider Contractual Requirements p.141
- 3.3 Key Operational Resilience Obligations p.143
- 3.4 Operational Resilience Enforcement p.145
- 3.5 International Data Transfers p.147
- 3.6 Threat-Led Penetration Testing p.149

4. Cyber-Resilience p.150

- 4.1 Cyber-Resilience Legislation p.150
- 4.2 Key Obligations Under Legislation p.151

5. Security Certification for ICT Products, Services and Processes p.153

- 5.1 Key Cybersecurity Certification Legislation p.153

6. Cybersecurity in Other Regulations p.155

- 6.1 Cybersecurity and Data Protection p.155
- 6.2 Cybersecurity and AI p.156
- 6.3 Cybersecurity in the Healthcare Sector p.156

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

ICT Legal Consulting ICT Legal Consulting (ICTLC) is an international law firm that offers strategic support in legal compliance (privacy, IP and TMT) and assists in drafting and developing governance, organisation, management, security and control models for data-driven organisations. The firm has successfully assembled a close-knit team of more than 80 qualified professionals specialising in the fields of ICT, privacy, data protection, cybersecurity, and IP law.

ICTLC has offices in Italy (Milan, Bologna, and Rome), the Netherlands (Amsterdam), Greece (Athens), France (Paris), Spain (Madrid), Finland (Helsinki), Sweden (Gothenburg), Nigeria (Lagos), Kenya (Nairobi), Saudi Arabia (Riyadh) and Australia (Melbourne). It has also established partnerships with law firms and professionals in 56 other countries, giving clients access to the most qualified professionals who are most suited to their specific needs.

Authors



Paolo Balboni is a founding partner at ICTLC – ICT Legal Consulting. Paolo, a top-tier European ICT, privacy and cybersecurity lawyer, serves as the data protection officer for

multinational companies. He is a Professor of Privacy, Cybersecurity and IT Contract Law at the European Centre on Privacy and Cybersecurity within the Maastricht University Faculty of Law, and a member of the EUMETSAT Data Protection Supervisory Authority and the Europrivacy Board of Experts. Paolo is admitted to the Milan and Amsterdam Bars. He is involved in European Commission studies on new technologies, in addition to participating in the revision of the EU Commission proposal for a General Data Protection Regulation.



Luca Bolognini is a founding partner at ICTLC – ICT Legal Consulting. Luca, a European privacy and data protection lawyer, and has been President of the Italian Institute for Privacy

and Data Valorisation since 2008. He is a member of the IAPP and CIPP/E, and a TÜV Italia Certified Privacy Officer. Luca serves as an independent ethics and privacy adviser for several European research and innovation projects (Horizon 2020) and as an expert coach for the Executive Agency for Small and Medium-sized Enterprises of the European Commission. He is a member of the Experts Board of EU-IoT and co-chair of the Europrivacy Certification Scheme Board of Senior Experts.

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiaro,
ICT Legal Consulting



Francesco Capparelli is chief cybersecurity adviser at ICTLC – ICT Legal Consulting and ICT Cyber Consulting. Francesco is a lawyer, qualified auditor/lead auditor ISO/IEC 27001, ISO

22301, ISO 37001, ISO/IEC 20000-1, ISO 9001, Certified Ethical Hacker, CIPPM and data protection officer. He obtained three master's degrees from LUISS University and Link Campus University in Rome, in Competition Law and Innovation with a specialisation in Privacy and Big Data; in Cybersecurity with a specialisation in Artificial Intelligence and Biometrics; and in Blockchain with a specialisation in Smart Contracts. He is also a certified PRINCE 2 project manager.



Giulia Finocchiaro is a cybersecurity adviser at ICTLC – ICT Legal Consulting and ICT Cyber Consulting. She has a broad legal background and is a qualified auditor/lead auditor

ISO/IEC 27001 and ISO 22301. After graduating in law, she obtained a diploma from the School of Specialisation for the Legal Professions, which further refined her legal skills. She obtained a master's degree in Cybersecurity Culture and Governance from the University of Catania, which deepened her knowledge of the sector. She is also actively involved in research activities, demonstrating her commitment to the advancement of cybersecurity and data protection.

ICTLC – ICT Legal Consulting

Via Borgonuovo 12
20121 Milan
Italy

Tel: +39 028 424 7194
Fax: +39 0270 0512 101
Email: info@ictlc.com
Web: www.ictlc.com



1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy National Cybersecurity Strategy

Italy has developed a structured cybersecurity strategy aimed at strengthening national resilience against cyberthreats, protecting critical infrastructures and ensuring the security of digital services. The strategy aligns with Directive (EU) 2022/2555, known as the NIS2 Directive, and is implemented through Legislative Decree Number 138 of 2024, which transposes the Directive into Italian law.

The Agency for National Cybersecurity, or ACN, is the principal authority overseeing cybersecurity at the national level. Established in 2021, it co-ordinates national and European cybersecurity policies, enhances co-operation between public and private entities, and ensures compliance with regulatory requirements.

The objectives of cybersecurity regulation are as follows:

- enhancing national security by strengthening the resilience of digital and network infrastructures against cyber-attacks, particularly in critical sectors such as energy, telecommunications and finance;
- protecting critical infrastructure by ensuring that essential service providers implement robust security measures in line with the NIS2 Directive and the implementing Regulation (EU) 2024/2690;
- regulating digital resilience through the Digital Operational Resilience Act (DORA), which sets strict requirements for financial sector entities regarding information and communication technology (ICT) risk management;

- ensuring incident reporting and response by mandating timely notification of significant cybersecurity incidents to national authorities and fostering a co-ordinated response to mitigate risks; and
- promoting cybersecurity standards by requiring organisations to adopt internationally recognised security frameworks such as ISO/IEC 27001 and ISO/IEC 27002, which are referenced in Italian cybersecurity regulations.

Cybersecurity regulation in Italy is continuously evolving to address emerging threats and align with EU and international best practices. It is paramount to consider that Italy has implemented the *Perimetro di Sicurezza Cibernetica* (PSNC), which includes all the above-mentioned principles. The legal framework reinforces proactive risk management, fosters digital trust, and ensures the resilience of national infrastructures in the face of increasingly sophisticated cyberthreats.

1.2 Cybersecurity Laws

Italy's cybersecurity legal framework is based on a combination of EU regulations and national laws that govern critical infrastructure protection, digital resilience, data protection, and cybersecurity obligations for public and private entities. The primary legislative instruments include:

- the National Cybersecurity Perimeter Law;
- DORA;
- the NIS2 Directive; and
- the General Data Protection Regulation (GDPR).

The National Cybersecurity Perimeter Law (Legislative Decree No 105/2019):

- establishes a national cybersecurity perimeter to protect critical infrastructures, including

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

- public administration, telecommunications, energy, finance and health sectors;
- requires entities operating in strategic sectors to implement risk management measures, conduct security assessments and report cybersecurity incidents to the Agency for National Cybersecurity (ACN); and
- introduces strict vendor requirements, limiting the use of foreign technology suppliers in critical ICT systems.

DORA (Regulation (EU) 2022/2554):

- applies to financial sector entities, including banks, investment firms, insurance companies and ICT service providers;
- establishes harmonised cybersecurity and risk management requirements, mandating that firms implement robust ICT security measures and ensure resilience against cyberthreats;
- imposes mandatory testing and incident-reporting obligations, requiring financial entities to assess their operational resilience through cybersecurity stress tests; and
- introduces third-party risk-management rules, ensuring financial institutions properly assess and monitor risks arising from outsourced ICT services.

The NIS2 Directive (Directive (EU) 2022/2555 and Legislative Decree No 138/2024):

- expands the scope of cybersecurity obligations to a broader range of critical and essential sectors, including energy, transport, banking, health and digital infrastructure;
- requires enhanced security measures, such as risk management policies, network security controls and business continuity planning;
- strengthens incident-reporting obligations, requiring companies to notify cybersecurity

authorities of significant incidents within 24 hours of detection; and

- introduces stricter enforcement mechanisms, including fines and sanctions for non-compliance.

The GDPR (Regulation (EU) 2016/679):

- establishes a comprehensive framework for data protection and cybersecurity across the EU;
- imposes strict security obligations on organisations processing personal data, including encryption, access controls and data breach notification requirements;
- mandates privacy by design and by default, ensuring cybersecurity measures are integrated into ICT systems from the outset; and
- requires organisations to report personal data breaches to the Italian Data Protection Authority (*Garante per la Protezione dei Dati Personali*) within 72 hours.

Italy's cybersecurity regulatory framework is designed to ensure digital resilience, protect national security and safeguard personal data. The combined effect of NIS2, DORA, the Cybersecurity Perimeter Law and the GDPR establishes strict obligations for organisations across multiple sectors, reinforcing the country's defence against cyberthreats and data breaches.

1.3 Cybersecurity Regulators

Main Cybersecurity Regulators in Italy

Italy's cybersecurity regulatory landscape is structured around several key authorities responsible for cybersecurity governance, critical infrastructure protection, financial sector resilience and data protection. The main regulatory bodies are:

- the ACN;

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiaro,
ICT Legal Consulting

- the National Cybersecurity Incident Response Team (CSIRT Italia);
- the Bank of Italy (*Banca d'Italia*) and financial supervisory authorities; and
- the Italian Data Protection Authority (*Garante per la Protezione dei Dati Personali* – GPD).

ACN

Role and functions:

- established in 2021, the ACN is Italy's central authority for cybersecurity governance, risk management and national defence against cyberthreats;
- implements Legislative Decree No 138/2024, which transposes the NIS2 Directive, and oversees the National Cybersecurity Perimeter Law (Decree No 105/2019);
- develops the National Cybersecurity Strategy and ensures compliance with risk management frameworks and security protocols;
- conducts security audits, vulnerability assessments and cyber-resilience exercises for critical infrastructure operators; and
- collaborates with EU cybersecurity agencies, NATO and international organisations on cybersecurity policies and threat intelligence sharing.

Scope of authority:

- enforces NIS2 and National Cybersecurity Perimeter obligations on public entities, essential service providers and high-risk industries;
- regulates security standards for ICT supply chains, including vendor approval processes for critical infrastructures; and
- oversees cyber incident reporting and response for regulated sectors, ensuring real-time co-ordination during cyber crises.

CSIRT Italia

Role and functions:

- operates as Italy's national Computer Security Incident Response Team (CSIRT) under the ACN's authority;
- provides early warning and response co-ordination for cyber incidents affecting critical infrastructures and public entities;
- develops threat intelligence and cybersecurity advisories, informing organisations of emerging cyberthreats and vulnerabilities; and
- assists in incident containment, mitigation and forensic analysis following major cyberattacks.

Scope of authority:

- covers government agencies, national critical infrastructures and private entities subject to NIS2 regulations; and
- co-ordinates with EU CSIRT Network, ENISA and international cybersecurity agencies for cross-border cyberthreats.

Bank of Italy and Financial Supervisory Authorities

Role and functions:

- enforces cyber-resilience requirements for financial institutions under DORA;
- oversees ICT risk management in banks, insurance companies, investment firms and financial service providers;
- conducts digital resilience testing, ICT audits and third-party risk assessments for financial entities; and
- implements financial sector cybersecurity stress tests and cyber incident reporting frameworks.

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

Scope of authority:

- applies to all regulated financial entities, including banks, insurance companies and payment service providers;
- regulates outsourcing of ICT services, ensuring compliance with third-party cybersecurity standards; and
- works with the European Central Bank (ECB), European Banking Authority (EBA) and European Securities and Markets Authority (ESMA) on financial cybersecurity policies.

GPDP

Role and functions:

- enforces GDPR compliance in Italy;
- investigates personal data breaches, unauthorised access and cybersecurity failures affecting personal information;
- imposes fines and sanctions for non-compliance with data protection and cybersecurity regulations; and
- provides guidance on privacy-enhancing cybersecurity measures, including encryption, secure authentication and access control frameworks.

Scope of authority:

- covers all entities processing personal data, including public institutions, businesses and online service providers;
- mandates data breach reporting within 72 hours, ensuring rapid response to cybersecurity incidents affecting personal data; and
- works with the EU Data Protection Board (EDPB) and other European regulators on cross-border cybersecurity investigations.

Conclusion

Italy's cybersecurity regulatory framework is based on a multi-agency approach, ensuring comprehensive oversight of cybersecurity risks across different sectors:

- the ACN regulates national cybersecurity policies and critical infrastructure protection;
- CSIRT Italia handles incident response and cyberthreat intelligence;
- the Bank of Italy and financial regulators enforce financial sector cybersecurity under DORA; and
- the GPDP ensures cybersecurity compliance for data protection under the GDPR.

Together, these regulatory bodies ensure that Italy's digital infrastructure remains resilient, cyber-risks are effectively mitigated and organisations comply with strict security standards.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

Scope of Application Under the NIS2 Directive

The NIS2 Directive establishes a harmonised cybersecurity framework across the EU, imposing strict security and incident reporting requirements on a broad set of critical and essential entities.

Entities covered:

- expands beyond the original NIS1 Directive (EU 2016/1148) to cover a wider range of sectors, including essential entities (energy, transport, banking, healthcare, public administration and digital infrastructure) and impor-

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

tant entities (postal services, manufacturing, food, waste management and research sectors);

- applies to medium and large enterprises with in these sectors but allows member states to include smaller entities if their cybersecurity risk profile is significant; and
- introduces supply chain obligations, meaning ICT service providers that support critical infrastructure operations are now directly regulated under the Directive.

Key obligations:

- requires implementation of cybersecurity risk management measures, including network security controls, access management and business continuity planning;
- mandates incident reporting within 24 hours of detection for significant cyber events; and
- establishes supervisory and enforcement mechanisms, with severe penalties for non-compliance (up to 2% of an entity's global turnover).

Scope of Application Under the U.S. Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA, 2022)

The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA, 2022), enacted in the United States, establishes mandatory cybersecurity incident-reporting obligations for critical infrastructure operators under the oversight of the Cybersecurity and Infrastructure Security Agency (CISA).

Entities covered:

- covers critical infrastructure sectors designated under Presidential Policy Directive 21 (PPD-21), including communications, financial

services, healthcare, energy, defence, transportation and government facilities;

- applies to any organisation providing essential services to national security, the economy or public safety; and
- unlike NIS2, it does not use size-based criteria, meaning small and medium-sized enterprises (SMEs) can be covered if they support critical infrastructure.

Key obligations:

- requires reporting of cyber incidents within 72 hours and ransomware payments within 24 hours;
- mandates compliance with information-sharing provisions, allowing CISA to disseminate threat intelligence to affected industries; and
- grants legal protections to reporting entities, reducing liability risks associated with disclosing cyber incidents.

Uncertainties in the Interpretation of the Scope

Despite the clear intent to improve cybersecurity resilience, both NIS2 and CIRCIA face interpretational uncertainties that could impact on their practical enforcement.

Defining “Significant” Incidents

NIS2 requires entities to report “significant incidents” but leaves room for interpretation in defining what qualifies as significant. The regulation considers impact on operations, users and the economy, but lacks precise thresholds.

CIRCIA mandates reporting for “substantial” cyber incidents but does not clearly define how severity and material impact should be assessed, leading to potential underreporting or overreporting.

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

Inclusion of SMEs and Supply Chain Entities

NIS2 explicitly covers only medium and large enterprises, but allows member states to extend regulations to smaller entities based on risk. This could lead to fragmentation across EU jurisdictions, where some countries impose stricter obligations than others.

CIRCIA applies to all entities supporting critical infrastructure, regardless of size, but does not clarify the thresholds for third-party ICT providers, leaving uncertainty for vendors and subcontractors.

Cross-Border Enforcement and Jurisdictional Overlaps

NIS2 faces challenges in cross-border enforcement, especially for multinational companies operating in multiple EU member states. National cybersecurity authorities may interpret enforcement differently, leading to inconsistent compliance burdens.

CIRCIA's reporting obligations may conflict with state-level cybersecurity laws, particularly in California and New York, which have separate breach notification requirements. This creates regulatory duplication and compliance complexity.

Interaction with Other Regulations (GDPR, DORA and National Laws)

In the EU, NIS2 overlaps with GDPR and DORA, raising questions about regulatory precedence.

If a cyber incident involves both personal data breaches and operational disruptions, organisations must report separately to the Data Protection Authority and the Cybersecurity Authority, increasing compliance complexity.

In the USA, CIRCIA intersects with sector-specific regulations, such as:

- HIPAA (for healthcare cybersecurity);
- FISMA (for government agencies);
- SEC cybersecurity rules (for public companies); and
- companies subject to multiple regimes may face conflicting reporting timelines and obligations.

Conclusion

While NIS2 and CIRCIA mark significant steps in enhancing critical infrastructure cybersecurity, interpretational uncertainties remain, particularly in defining reportable incidents, scope of covered entities and enforcement across jurisdictions:

- the EU's NIS2 Directive focuses on harmonisation but allows flexibility, leading to potential national divergences in scope and application; and
- the USA's CIRCIA law prioritises rapid incident response but lacks clear criteria for inclusion, creating compliance uncertainties for smaller entities and third-party service providers.

Future regulatory clarifications, sector-specific guidance and international co-operation will be critical to ensuring uniform enforcement and effective cybersecurity protections.

2.2 Critical Infrastructure Cybersecurity Requirements

Italy has adopted a comprehensive regulatory framework to ensure the cybersecurity resilience of critical infrastructure, aligning with EU legislation such as the NIS2 Directive and DORA, as well as national cybersecurity laws. The main

legal instruments governing cybersecurity for critical infrastructure include:

- Legislative Decree No 138/2024 (the “NIS2 Implementation Law”);
- Legislative Decree No 105/2019 (the “National Cybersecurity Perimeter Law”); and
- Regulation (EU) 2022/2554 (DORA) for financial infrastructure.

These laws impose strict cybersecurity obligations on critical infrastructure operators across energy, telecommunications, financial services, healthcare, transportation and public administration.

Key Cybersecurity Requirements

Risk management and security measures are as follows.

- Critical infrastructure operators must implement risk management frameworks to identify, assess and mitigate cyber-risks.
- Companies must apply technical and organisational security measures, including:
 - (a) network and information system security controls;
 - (b) multi-factor authentication and access control policies;
 - (c) regular vulnerability assessments and penetration testing; and
 - (d) data encryption and secure communication protocols.

Cyber Incident Reporting Obligations

Entities covered under the NIS2 Directive must report significant cybersecurity incidents to the Agency for National Cybersecurity (ACN) within 24 hours of detection.

Financial institutions regulated under DORA must report major ICT disruptions or cyber incidents to supervisory authorities within 72 hours.

Organisations must provide a detailed incident analysis, including the impact, response measures and mitigation strategies.

Business Continuity and Resilience Planning

Operators must maintain cyber-resilience plans, ensuring their ability to continue operations during cyber disruptions.

Companies must conduct regular stress tests and resilience exercises to evaluate their preparedness against cyber-attacks.

The use of back-up systems, redundancy mechanisms and disaster recovery protocols is mandatory for ensuring operational continuity.

Supply Chain Security and Third-Party Risk Management

Organisations must assess and monitor cybersecurity risks posed by third-party ICT service providers.

Under DORA, financial entities must implement contractual cybersecurity requirements for ICT suppliers, including incident-reporting clauses and security audit rights.

Critical infrastructure operators are required to verify the security posture of external vendors before integrating their services.

Compliance and Supervision

The ACN conducts regular inspections and audits to verify compliance with cybersecurity laws.

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

Non-compliance with cybersecurity obligations can result in severe penalties, including fines of up to 2% of global turnover.

Authorities have the power to impose remediation measures or restrict ICT operations if security risks are not properly managed.

Conclusion

Italy's cybersecurity regulations establish a robust legal framework to protect critical infrastructure from cyberthreats. These requirements focus on risk management, incident reporting, resilience planning, supply chain security and regulatory supervision. Organisations operating in critical sectors must adhere to strict security standards to ensure national security, economic stability and public safety.

2.3 Incident Response and Notification Obligations

Italy imposes strict cybersecurity incident notification obligations on critical infrastructure owners and operators under the NIS2 Implementation Law, the National Cybersecurity Perimeter Law and DORA. These laws establish mandatory reporting frameworks to ensure rapid response to cyber incidents, minimise disruptions and enhance national cybersecurity resilience.

Notification Requirements Under NIS2 (Legislative Decree No 138/2024)

The NIS2 Directive introduces a harmonised cyber incident reporting framework for critical and essential service providers operating in sectors such as energy, transport, banking, health-care and public administration.

Entities covered:

- essential and important entities defined under NIS2, including critical infrastructure opera-

tors, ICT service providers and public sector entities; and

- third-party ICT service providers that support critical infrastructure operations.

Incident reporting timeline:

- within 24 hours – operators must submit an early warning notification to ACN if they detect a potentially significant cybersecurity incident;
- within 72 hours – a formal incident report must be submitted, including details on the attack vector, impact assessment and immediate mitigation measures; and
- within one month – a final report must be provided, outlining post-incident forensic analysis and lessons learned.

Criteria for Reporting

An incident must be reported if it:

- significantly disrupts the availability, integrity or confidentiality of essential services;
- causes substantial economic or operational damage to the affected entity; and
- has cross-border implications, affecting other EU member states.

Penalties for Non-Compliance

Failure to report cyber incidents may result in fines of up to 2% of an entity's global turnover.

The ACN can impose corrective measures, audits or operational restrictions if an organisation fails to comply.

Notification Requirements Under the National Cybersecurity Perimeter Law (Legislative Decree No 105/2019)

This law applies to operators of critical infrastructure and strategic national entities, such as

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

those in defence, telecommunications, energy and public administration.

Incident reporting timeline:

- immediate notification – entities must immediately report any suspected cybersecurity breach affecting national security to the ACN and the National Cybersecurity Incident Response Team (CSIRT Italia);
- 48-hour follow-up report – a more detailed report must be provided, specifying affected systems, attack vectors and initial containment measures; and
- final remediation report – organisations must submit a comprehensive incident analysis, including recovery steps taken.

Key obligations:

- operators must establish real-time monitoring and detection mechanisms to identify cybersecurity threats; and
- they must co-operate with government agencies during national cybersecurity emergencies.

Enforcement and penalties:

- non-compliance with notification obligations may result in severe financial penalties and operational restrictions; and
- the ACN has the authority to audit and enforce cybersecurity resilience measures in critical sectors.

Notification Requirements Under DORA for Financial Entities

DORA imposes specific cybersecurity reporting requirements on banks, insurance companies, investment firms and financial service providers.

Incident reporting timeline:

- within four hours – financial institutions must notify their national supervisory authority if an incident is deemed severe;
- within 24 hours – a preliminary impact assessment must be submitted, detailing the scale of the disruption and affected systems; and
- within 72 hours – a detailed incident report must be provided, including technical analysis, forensic findings and recovery strategies.

Criteria for Reporting

Incidents must be reported if they:

- disrupt financial transactions, banking operations or stock market activities;
- affect payment processing, fund transfers or critical ICT infrastructure; and
- have cross-border implications within the EU financial sector.

Regulatory Oversight

The Bank of Italy, Consob and IVASS oversee DORA compliance in Italy.

Financial institutions failing to report incidents face regulatory sanctions and potential suspension of operations.

Conclusion

Italy's cybersecurity notification framework is one of the most stringent in the EU, requiring rapid incident reporting, real-time threat monitoring and co-ordinated response mechanisms.

- NIS2 mandates a structured incident-reporting process for critical infrastructure operators, with severe penalties for non-compliance;

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

- the National Cybersecurity Perimeter Law imposes additional security obligations on entities deemed essential to national security and defence; and
- DORA establishes financial sector-specific reporting requirements to ensure cyber-resilience in banking, insurance and financial markets.

These laws ensure that Italy's critical infrastructure remains resilient, cyberthreats are swiftly addressed and government agencies can co-ordinate effective cyber crisis responses.

2.4 State Responsibilities and Obligations

Italy has established a national cybersecurity framework that assigns clear responsibilities to state authorities for resilience building and cyberthreat identification. These responsibilities are defined under the NIS2 Implementation Law, the National Cybersecurity Perimeter Law and DORA.

National Cyber-Resilience Responsibilities

The Italian state is responsible for strengthening the cybersecurity resilience of critical infrastructure, essential service providers and public sector entities. These responsibilities include the following.

Developing and enforcing cybersecurity policies

The ACN is tasked with defining and implementing the National Cybersecurity Strategy, aligning with EU Regulations and international best practices.

The government establishes sector-specific cybersecurity regulations, ensuring that energy, telecommunications, healthcare, finance and

public administration sectors comply with risk management requirements.

Supervising critical infrastructure cybersecurity compliance

The ACN conducts regular cybersecurity audits and risk assessments for national critical infrastructure operators.

Operators of essential services must submit cyber-risk management plans to demonstrate resilience preparedness.

The ACN can impose corrective measures and penalties if an entity fails to implement required cybersecurity measures.

Establishing cyber incident response capabilities

CSIRT Italia (the National Cybersecurity Incident Response Team) co-ordinates real-time threat response and mitigation for national security threats.

The State facilitates public-private collaboration on cybersecurity best practices, ensuring that private sector entities share threat intelligence with national authorities.

Italy participates in EU-wide cybersecurity initiatives, including the EU Cyber Crisis Liaison Organisation Network (EU-CyCLONe) for rapid cyber crisis management.

National Cyberthreat Identification and Intelligence-Sharing Responsibilities

The Italian government plays a proactive role in identifying, analysing and mitigating cyberthreats at the national level.

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

Cyberthreat monitoring and detection

The ACN and CSIRT Italia continuously monitor cyberthreats, vulnerabilities and attack vectors targeting critical infrastructure.

The State mandates that essential service providers implement advanced threat-detection systems, including intrusion detection, behavioural analytics and automated monitoring tools.

The National Cyber Threat Intelligence Platform collects, analyses and distributes real-time cyberthreat intelligence to government agencies and private entities.

Cybersecurity incident reporting and analysis

Entities covered under NIS2 and the National Cybersecurity Perimeter Law must report significant cybersecurity incidents to the ACN within 24 hours.

The State analyses cyber incident reports to assess risk trends, identify attack patterns and develop national defence strategies.

Italy collaborates with EU cybersecurity agencies (ENISA, Europol and NATO cyber defence units) to exchange threat intelligence and coordinate international cyber response actions.

National defence against cyberthreats

The government strengthens national cyber defence capabilities by investing in cybersecurity research, innovation and workforce development.

Italy enforces strict cybersecurity standards for ICT suppliers, ensuring that critical infrastructure operators use secure, vetted technologies.

The Ministry of Defence and intelligence agencies monitor cyberthreats linked to foreign

actors, cyber-espionage and State-sponsored attacks.

Conclusion

Italy's State responsibilities on resilience and threat identification ensure a structured and proactive approach to national cybersecurity:

- the government enforces cybersecurity laws, supervises compliance and ensures that critical infrastructure remains resilient against cyberthreats;
- national cybersecurity agencies (the ACN and CSIRT Italia) identify, monitor and respond to cyberthreats, ensuring real-time protection of essential services; and
- the State collaborates with EU and international partners to strengthen cyber intelligence, prevent large-scale cyber incidents and secure the digital ecosystem.

Through policy enforcement, risk monitoring and cyber intelligence operations, Italy upholds a robust cybersecurity framework that safeguards national security, economic stability and public trust.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

Italy's financial sector's operational resilience is regulated primarily under DORA, which establishes a harmonised cybersecurity framework for financial entities across the EU. DORA applies directly in Italy without requiring national transposition, ensuring uniform ICT risk management and cyber-resilience measures for financial institutions.

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiaro,
ICT Legal Consulting

Material Scope of Application

DORA applies to a broad range of financial entities and their third-party ICT service providers, ensuring that digital resilience measures extend throughout the financial supply chain.

Financial entities covered:

- banks and credit institutions;
- investment firms and asset managers;
- insurance and reinsurance companies;
- payment institutions and e-money firms;
- crypto-asset service providers (CASPs) under MiCA; and
- central securities depositories and financial market infrastructures.

Third-party ICT providers covered:

- cloud service providers, data centres and cybersecurity firms that support financial operations; and
- managed service providers (MSPs) offering IT, software or infrastructure services to financial institutions.

Key regulatory requirements:

- mandatory ICT risk management framework, including business continuity planning and cyber incident response;
- obligatory cyber incident reporting within 72 hours to national financial regulators;
- regular penetration testing and digital operational resilience testing to ensure financial stability; and
- oversight of third-party ICT service providers, requiring contractual risk management measures.

Territorial Scope of Application

DORA applies to all financial entities operating within the EU, including:

- entities headquartered in Italy – all financial institutions and ICT service providers based in Italy fall directly under DORA's jurisdiction;
- EU branches of foreign financial institutions – non-EU firms operating in Italy through subsidiaries must comply with DORA's ICT risk management and reporting obligations; and
- third-country ICT providers servicing EU financial firms – non-EU technology firms that offer ICT services to European financial institutions are subject to DORA's Oversight Framework for Critical ICT Providers, requiring them to adhere to EU cybersecurity standards.

The Bank of Italy, Consob and IVASS are responsible for DORA's enforcement in Italy, ensuring that financial institutions meet digital resilience obligations and remain operationally secure against cyberthreats.

3.2 ICT Service Provider Contractual Requirements

Under DORA, Italy enforces strict contractual obligations for ICT service providers that support financial sector operations. These requirements aim to ensure resilience, security and accountability in the supply chain of banks, investment firms, insurance companies and other financial entities.

Definition of ICT Service Providers in Italy

DORA defines ICT service providers as third-party entities offering digital, information technology or cybersecurity services to financial institutions. This includes:

- cloud service providers (IaaS, PaaS, SaaS);

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

- data centres and hosting providers;
- cybersecurity firms (managed security services, threat intelligence, incident response);
- software vendors and fintech providers;
- telecommunications providers supporting financial transactions; and
- artificial intelligence and automation service providers used in financial risk management.

If an ICT provider delivers essential digital services to financial entities, it falls under DORA's oversight framework, requiring compliance with contractual and risk management obligations.

Contractual Requirements for ICT Service Providers Under DORA

Financial institutions in Italy must ensure that contracts with ICT service providers include specific provisions on risk management, security and resilience.

Mandatory Contractual Clauses

Security and risk management standards:

- ICT providers must implement strong cybersecurity measures, including encryption, access control and data protection mechanisms; and
- compliance with ISO/IEC 27001, NIST frameworks and other EU cybersecurity standards is required.

Business continuity and incident response obligations:

- contracts must include service-level agreements (SLAs) for disaster recovery, back-up availability and cybersecurity incident handling; and
- ICT providers must conduct regular resilience testing and provide results to financial regulators.

Incident reporting and notification requirements:

- ICT providers must report cyber incidents and disruptions to financial institutions within 24 hours; and
- financial institutions must then notify the Bank of Italy, IVASS or Consob under DORA's 72-hour reporting obligation.

Audit rights and compliance monitoring:

- financial institutions must have the right to audit ICT providers to assess compliance with operational resilience requirements; and
- regulatory authorities may conduct independent supervisory assessments of critical ICT providers.

Exit and termination strategy:

- contracts must outline clear termination clauses and transition plans to prevent operational disruptions if the ICT provider fails to meet security obligations.

Classification of Critical ICT Services Under DORA

DORA mandates additional oversight for “critical ICT service providers”, which are entities indispensable for the stability of financial markets.

Critical ICT services include:

- cloud computing services used for banking transactions, payment processing and data storage;
- cybersecurity and managed security services (MSSPs) protecting financial networks from cyberthreats;
- AI-driven fraud detection and risk management platforms used in credit scoring and market analysis; and

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiaro,
ICT Legal Consulting

- third-party digital infrastructure providers essential for financial services (eg, cross-border payment networks, digital identity verification systems).

These critical ICT providers are subject to direct regulatory oversight from the European Supervisory Authorities (ESAs), including:

- the European Banking Authority (EBA);
- the European Insurance and Occupational Pensions Authority (EIOPA); and
- the European Securities and Markets Authority (ESMA).

Will Every Cloud Service Provider Be Classified as Critical?

A cloud service provider will not necessarily be classified as critical. DORA applies additional scrutiny only to cloud providers whose services are fundamental to financial stability:

- large cloud service providers (AWS, Microsoft Azure, Google Cloud) that host banking operations will likely be classified as critical;
- small cloud vendors or niche SaaS providers that do not support essential financial operations may not fall under direct regulatory oversight; and
- ICT providers servicing multiple financial institutions are more likely to be designated as critical by the ESAs.

However, even non-critical cloud providers must comply with DORA's contractual obligations, ensuring cybersecurity, resilience and transparency in financial ICT supply chains.

Conclusion

DORA imposes strict contractual requirements on ICT service providers, ensuring cybersecurity resilience, incident reporting and regulatory

compliance for financial sector digital infrastructure:

- ICT service providers are broadly defined, covering cloud services, cybersecurity, fintech and digital infrastructure providers;
- critical ICT providers (eg, cloud computing firms supporting financial transactions) face enhanced regulatory oversight; and
- not all cloud service providers are automatically classified as critical, but those supporting essential financial functions will be directly supervised by EU regulators.

3.3 Key Operational Resilience Obligations

DORA establishes a uniform legal framework for digital operational resilience in the EU financial sector, applying directly to Italy. The Regulation ensures that financial institutions and their ICT service providers can withstand, respond to and recover from cyberthreats and ICT disruptions.

Objectives of DORA

The primary goals of DORA are to:

- strengthen ICT risk management across the financial sector, ensuring business continuity and financial stability;
- standardise incident response and reporting, allowing for timely detection, containment and notification of cyberthreats;
- ensure regulatory oversight of critical ICT service providers, reducing third-party risks in financial operations;
- enhance resilience testing by mandating cyber stress tests and penetration testing for financial firms; and
- promote threat intelligence-sharing, improving sector-wide cyberthreat detection and mitigation.

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

Key Obligations Under DORA

DORA applies to banks, insurance companies, investment firms, crypto-asset service providers and ICT vendors supporting financial institutions. Its requirements include the following.

ICT risk management:

- financial entities must adopt a risk management framework covering ICT security policies, network protection and access controls;
- continuous monitoring of ICT systems to detect vulnerabilities and threats; and
- implementation of business continuity and disaster recovery strategies.

ICT third-party risk management:

- financial firms must assess third-party ICT risks, ensuring that suppliers meet strict cybersecurity standards;
- contracts with ICT providers must include security, incident reporting and resilience-testing obligations; and
- regulatory oversight of critical ICT providers offering cloud services, managed security and data-processing.

Digital resilience testing:

- regular cyber-resilience testing, including penetration testing, vulnerability scans and risk assessments; and
- threat-led penetration testing (TLPT) required for systemically important financial entities.

Governance and compliance:

- senior management is responsible for ICT risk oversight and regulatory compliance;

- mandatory training and awareness programmes for employees handling financial IT systems; and
- financial regulators can audit compliance and impose penalties for non-compliance.

Incident and Reporting Obligations Under DORA

DORA introduces strict cybersecurity incident reporting requirements to prevent systemic financial risks.

Incident classification:

- major ICT-related incidents include cyber-attacks, ransomware, system failures and data breaches affecting financial services; and
- incidents are categorised based on impact on operations, data security and financial stability.

The reporting timeline and process is as follows.

- Within four hours – financial institutions must notify their national financial regulator (eg, Bank of Italy, Consob, IVASS) if a major cyber incident is detected.
- Within 24 hours – a preliminary incident report must be submitted, detailing affected systems, potential risks and immediate response actions.
- Within 72 hours – a detailed incident report must provide:
 - (a) root cause analysis;
 - (b) impact assessment;
 - (c) steps taken to contain the attack; and
 - (d) future prevention measures.
- Final post-mortem report – required if the incident had severe financial or systemic implications, ensuring regulatory follow-up and that industry-wide lessons were learned.

Cross-border co-ordination:

- if an ICT incident has cross-border impact, financial firms must notify the ESAs; and
- regulators collaborate with CSIRT Italia and ENISA to manage large-scale cyberthreats.

Conclusion

DORA sets out comprehensive digital resilience standards for Italy's financial sector, ensuring strict cybersecurity measures, third-party risk controls and mandatory cyber incident reporting:

- financial institutions must implement robust ICT risk management policies and resilience testing;
- ICT service providers supporting financial firms must comply with cybersecurity and incident-reporting obligations; and
- strict incident-reporting requirements ensure rapid regulatory response to cyberthreats, preventing financial instability.

These measures enhance cyber-resilience, protect financial markets and ensure regulatory oversight in an increasingly digital financial ecosystem.

3.4 Operational Resilience Enforcement

Under DORA, regulatory authorities in Italy and the EU enforce strict operational resilience obligations on critical ICT service providers that support the financial sector. These providers – such as cloud computing firms, cybersecurity vendors and data-processing centres – are subject to direct regulatory oversight due to their essential role in financial stability.

Regulatory Authorities Responsible for Enforcement

The enforcement of operational resilience obligations is managed by both national and EU-level regulators, including:

- the Bank of Italy (*Banca d'Italia*) – supervises banking and payment service ICT risk;
- IVASS (the Italian Insurance Supervisory Authority) – regulates ICT resilience in the insurance sector;
- Consob (the Italian Securities Commission) – oversees cybersecurity in investment firms and financial markets;
- European Supervisory Authorities (ESAs) – the European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA) and European Securities and Markets Authority (ESMA) conduct cross-border supervision; and
- the European Central Bank (ECB) – directly supervises significant banks under the Single Supervisory Mechanism (SSM).

For critical ICT providers, DORA establishes a direct regulatory oversight framework, allowing EU financial authorities to intervene in ICT service delivery, mandate corrective actions and impose sanctions.

Compliance Obligations for Critical ICT Service Providers

Critical ICT service providers must comply with specific operational resilience obligations, including:

- ICT risk management – providers must implement strict security controls, continuous monitoring and incident-detection mechanisms;
- cyber-resilience testing – regular penetration testing and risk assessments are mandatory, with financial regulators overseeing results;

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

- incident response and reporting – providers must notify financial institutions of cyber incidents within 24 hours, enabling banks and insurers to report to regulators within 72 hours;
- business continuity and recovery plans – providers must maintain back-up systems, failover strategies and rapid disaster-recovery capabilities; and
- regulatory audit rights – national and EU financial regulators have full authority to conduct audits, on-site inspections and security evaluations of critical ICT service providers.

Enforcement Measures and Sanctions

Regulatory bodies enforce compliance through audits, inspections and corrective actions. If a critical ICT provider fails to meet operational resilience standards, the following enforcement measures apply.

Supervisory audits and on-site inspections

Regulatory authorities audit ICT providers to verify compliance with DORA and cybersecurity best practices.

On-site inspections and forensic reviews are conducted if vulnerabilities or past incidents indicate a high cyber risk.

Corrective measures and compliance orders

If deficiencies are found, regulators can issue binding corrective measures, including:

- security upgrades and process improvements;
- additional penetration-testing requirements; and
- stronger supply chain risk assessments.

Financial penalties for non-compliance

ICT service providers failing to meet regulatory obligations may face severe financial penalties:

- up to 2% of global turnover for non-compliance with cybersecurity and risk management standards; and
- additional daily fines until corrective actions are fully implemented.

Termination of ICT service contracts

If a critical ICT provider poses an unacceptable risk to financial stability, regulators can order financial institutions to terminate service contracts with the non-compliant provider.

The ESAs maintain a register of high-risk ICT service providers, restricting their access to EU financial markets.

Regulatory intervention in ICT service operations

In extreme cases, regulators may impose operational restrictions, requiring ICT providers to suspend or restructure critical services that threaten financial stability.

National authorities can mandate emergency cybersecurity measures if a major cyber event impacts on financial institutions.

Cross-Border Enforcement and Co-ordination

Because many critical ICT service providers operate across multiple jurisdictions, enforcement requires EU-wide co-ordination:

- joint supervisory teams (JSTs) – national regulators collaborate with the ECB and ESAs to conduct cross-border compliance reviews of ICT providers servicing multiple EU financial institutions;

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

- EU cyber crisis response framework – regulators co-ordinate responses for large-scale cyber incidents affecting multiple financial firms and ICT providers; and
- information-sharing mandates – ICT service providers must participate in threat intelligence-sharing programmes with financial regulators to enhance industry-wide cyber-resilience.

Conclusion

Enforcement of operational resilience obligations for critical ICT providers under DORA is strict and proactive, ensuring financial market stability and cybersecurity resilience:

- regulatory authorities in Italy and the EU directly oversee critical ICT providers, conducting audits, compliance checks and on-site inspections;
- failure to meet resilience standards results in heavy penalties, service restrictions and contract termination orders; and
- cross-border collaboration ensures that multinational ICT providers comply with harmonised EU financial cybersecurity regulations.

Through these measures, Italy and the EU maintain a secure, resilient and stable financial digital infrastructure, protecting against cyberthreats and ICT disruptions.

3.5 International Data Transfers

Italy's legal framework for cybersecurity and financial resilience includes multiple provisions that directly or indirectly regulate international data transfers. These rules stem from EU regulations such as the GDPR, DORA and NIS2, as well as national cybersecurity laws.

The impact on international data transfers arises through:

- data protection regulations imposing cross-border data transfer restrictions;
- cybersecurity laws requiring localisation or risk assessments for data transfers; and
- operational resilience regulations affecting third-party ICT providers outside the EU.

Direct Provisions Impacting on International Data Transfers GDPR:

- Transfers of personal data outside the EU are strictly regulated under Chapter V of the GDPR.
- Transfers to non-EU countries are permitted only if:
 - (a) the destination country has an EU adequacy decision (eg, Japan, UK, Canada);
 - (b) the transfer is governed by Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs); and
 - (c) derogations apply, such as explicit user consent or contractual necessity.
- Impact on cybersecurity – if an ICT provider stores financial or critical infrastructure data outside the EU, data protection authorities may restrict the transfer.

DORA:

- cross-border ICT risk assessment – financial entities must ensure that third-party ICT service providers processing financial data outside the EU comply with EU cybersecurity standards;
- critical ICT providers may be subject to EU regulatory oversight even if headquartered abroad; and
- enforcement of localisation requirements – if an ICT provider cannot ensure compliance with EU security requirements, financial institutions must terminate contracts.

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

NIS2:

- essential and important entities in critical sectors (eg, energy, telecoms, healthcare, finance) must conduct risk assessments before transferring security-related data outside the EU;
- cross-border cybersecurity incident reporting – entities must report cyber incidents involving non-EU data processing to the ACN; and
- national security exception – if an ICT service provider transfers critical infrastructure data to high-risk jurisdictions, Italian authorities can restrict or block such transfers.

The National Cybersecurity Perimeter Law:

- State and critical infrastructure operators must store and process security-sensitive data within the EU or trusted jurisdictions;
- foreign ICT providers handling Italian government or critical infrastructure data must comply with supply chain security assessments; and
- transfers to non-EU vendors (eg, cloud services) require government approval if involving national security data.

Indirect Provisions Affecting International Data Transfers

Cloud service and ICT provider oversight:

- cloud service providers hosting financial or critical infrastructure data outside the EU are subject to heightened regulatory scrutiny under DORA and NIS2;
- if a cloud provider fails EU compliance tests, financial institutions must discontinue services; and
- DORA's Oversight Framework for Critical ICT Providers applies extraterritorially, meaning

non-EU cloud vendors must comply with EU security rules.

Supply chain cybersecurity and data flow restrictions:

- financial institutions and critical infrastructure operators must vet third-party suppliers that process security-related data abroad;
- regulators may ban or restrict contracts with ICT vendors if cross-border data flows present an unacceptable security risk; and
- NIS2 and the National Cybersecurity Perimeter Law require security audits for non-EU third-party service providers.

Cyber incident notification and international data flows:

- companies reporting a cybersecurity incident under NIS2 must disclose if the breach involves data stored or processed outside the EU;
- financial entities under DORA must report ICT incidents affecting non-EU cloud or service providers to national regulators and EU authorities; and
- failure to properly assess the risks of non-EU data transfers can result in fines, compliance orders or contract termination requirements.

Conclusion

Italy's regulatory framework restricts and regulates international data transfers through the GDPR, DORA, NIS2 and national cybersecurity laws:

- the GDPR strictly limits personal data transfers to non-EU jurisdictions, allowing them only under specific safeguards;
- DORA and NIS2 impose cybersecurity and operational resilience restrictions on ICT

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

- providers handling financial and critical infrastructure data outside the EU; and
- the National Cybersecurity Perimeter Law prevents security-sensitive data from being transferred to high-risk jurisdictions.

These legal provisions ensure that international data transfers do not expose Italy's financial and critical sectors to cyberthreats, unauthorised access or geopolitical risks.

3.6 Threat-Led Penetration Testing

In Italy, threat-led penetration testing (TLPT) is mandated under DORA, which directly applies to banks, investment firms, insurance companies and other financial sector entities. The Bank of Italy, Consob and IVASS oversee TLPT compliance for financial institutions.

Scope of TLPT Requirements

TLPT is a high-level cybersecurity testing framework designed to simulate real-world cyberattacks on financial institutions and their critical ICT infrastructure:

- it applies to systemically important financial institutions, including major banks, payment service providers, insurance firms and trading platforms;
- it focuses on high-risk ICT systems supporting essential financial services; and
- ICT third-party providers (eg, cloud computing firms and managed security service providers) may also be subject to TLPT if classified as critical.

Key TLPT Obligations Under DORA

Risk-based TLPT execution:

- financial institutions must conduct TLPT at least every three years on their most critical ICT systems;

- the tests must be tailored to the entity's specific threat landscape, mimicking advanced persistent threats (APTs) and real-world cyber-attack scenarios; and
- TLPT must be performed by accredited and independent ethical hacking teams.

Regulatory oversight and reporting:

- financial firms must submit TLPT results to national regulators (Bank of Italy, IVASS or Consob);
- if vulnerabilities are discovered, firms must implement remediation measures and report follow-up actions; and
- regulators can mandate additional TLPT cycles if major cybersecurity weaknesses are detected.

Cross-border testing and EU co-ordination:

- financial institutions operating across multiple EU jurisdictions may be required to co-ordinate TLPT with the ESAs (EBA, ESMA, EIOPA); and
- TLPT methodologies must align with TIBER-EU (Threat Intelligence-Based Ethical Red Teaming), the EU-wide cybersecurity testing framework.

Enforcement and Non-Compliance Penalties

Failure to conduct TLPT or address identified vulnerabilities can lead to regulatory sanctions, including fines and operational restrictions.

Non-compliance with TLPT obligations may result in penalties up to 2% of global turnover under DORA.

Regulators may impose mandatory audits, security patches or temporary suspension of ICT services if critical risks are found.

Conclusion

Italy enforces strict TLPT requirements for major financial institutions and their critical ICT providers, ensuring proactive cybersecurity resilience:

- mandatory TLPT every three years for high-risk ICT systems;
- tests must simulate real-world cyber-attacks, aligning with TIBER-EU methodologies; and
- financial regulators oversee TLPT compliance, with penalties for non-compliance.

These measures strengthen digital operational resilience, protecting Italy's financial sector from advanced cyberthreats and systemic disruptions.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

Italy has established a comprehensive cybersecurity and cyber-resilience regulatory framework, aligning with EU Directives and Regulations. The country enforces strict cyber-resilience obligations for critical infrastructure, financial institutions, public administration and private entities handling sensitive data.

The legislative framework is built on:

- 1 EU Regulations and Directives, including DORA, NIS2 and the GDPR, which apply directly or require national transposition; and
- 2 national cybersecurity laws, such as the National Cybersecurity Perimeter Law (Legislative Decree No 105/2019) and the NIS2 Implementation Law (Legislative Decree No 138/2024).

Core Cyber-Resilience Laws in Italy

The GDPR:

- enforces strict cybersecurity and data protection requirements for organisations handling personal data;
- requires entities to implement technical and organisational security measures, such as encryption, access control and breach notification procedures; and
- imposes severe penalties for security failures, including fines of up to 4% of global turnover.

NIS2:

- strengthens cyber-resilience obligations for essential and important entities, including energy, transport, healthcare, financial services and digital infrastructure;
- mandates risk management frameworks, incident reporting within 24 hours and resilience testing; and
- expands regulatory enforcement and introduces fines for non-compliance of up to EUR10 million or 2% of global turnover.

DORA:

- applies directly to banks, insurance companies, investment firms and crypto-asset providers;
- mandates ICT risk management policies, cyber incident reporting within 72 hours, and TLPT (Threat-Led Penetration Testing) every three years; and
- introduces regulatory oversight for third-party ICT providers, ensuring financial entities only use compliant cloud, data-processing and cybersecurity services.

The National Cybersecurity Perimeter Law:

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

- establishes security measures for critical infrastructure and public sector IT systems;
- requires government entities and strategic industries (defence, telecommunications, finance, energy) to store sensitive data within the EU and to use trusted ICT providers; and
- enforces mandatory risk assessments and cybersecurity incident response plans.

Cybercrime and national security regulations:

- the Italian Penal Code Articles 615-ter to 640-ter criminalise unauthorised system access, data breaches, and cyberfraud;
- Decree Law No 82/2021 created the ACN, centralising cybersecurity enforcement; and
- the National Cybersecurity Strategy 2022–2026 outlines investment priorities and strategic cybersecurity initiatives.

Enforcement and Supervision of Cyber-Resilience

The ACN enforces NIS2, supervises critical infrastructure security, and co-ordinates cyber crisis response.

The Bank of Italy, IVASS and Consob regulate financial sector cyber-resilience under DORA, ensuring compliance with ICT risk management and testing requirements.

The Italian Data Protection Authority (*Garante per la Protezione dei Dati Personali* – GDPRP) ensures GDPR compliance, personal data security and breach-reporting enforcement.

Future Legislative Developments in Cyber-Resilience

National AI and cybersecurity regulations

The EU AI Act and upcoming EU cybersecurity certification schemes will impose new compli-

ance obligations for AI-driven cybersecurity solutions and critical infrastructure technologies.

Strengthened supply chain security rules

Italy is expected to introduce additional controls on ICT vendors and foreign technology providers, especially in critical sectors such as telecommunications and defence.

Expanded cybercrime enforcement

New measures will increase penalties for cyberattacks targeting government systems and essential services.

Conclusion

Italy's cyber-resilience legal framework is one of the most robust in the EU, incorporating the GDPR, NIS2, DORA and national cybersecurity laws;

- regulations apply to a broad range of sectors, ensuring cyber-resilience in critical infrastructure, financial services and data protection;
- national and EU regulators enforce cybersecurity standards, with significant penalties for non-compliance; and
- future legislative developments will strengthen supply chain security, AI governance and cybercrime enforcement.

These measures ensure that Italy's digital infrastructure remains resilient against cyberthreats, safeguarding economic stability and national security.

4.2 Key Obligations Under Legislation

Italy enforces strict cyber-resilience obligations across critical infrastructure, financial institutions and data-driven enterprises under EU Regulations (DORA, NIS2, GDPR) and national cybersecurity laws. These obligations ensure ICT risk management, incident reporting, business

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

continuity and regulatory oversight to mitigate cyberthreats and enhance digital resilience.

Cyber-Resilience Obligations Under Existing Legislation

GDPR:

- technical and organisational security measures – organisations handling personal data must implement access controls, encryption and data breach-prevention systems;
- data breach notification – personal data breaches must be reported to GPDP within 72 hours; and
- risk-based security assessment – companies must conduct Data Protection Impact Assessments (DPIAs) for high-risk data-processing activities.

NIS2:

- mandatory cybersecurity measures – essential and important entities must implement risk management frameworks, network security protocols and security monitoring;
- cyber incident reporting – entities must notify the ACN within 24 hours of detecting a significant cybersecurity incident;
- business continuity and recovery planning – organisations must develop incident response and disaster recovery plans, conducting regular resilience testing; and
- third-party risk management – companies must assess ICT suppliers and outsourcing risks, ensuring vendor compliance with security standards.

DORA:

- ICT risk management for financial institutions – banks, insurers, investment firms and

crypto-asset service providers must implement strict digital resilience policies;

- cyberthreat monitoring and testing – financial entities must conduct penetration testing, vulnerability assessments and red teaming exercises;
- third-party ICT oversight – ICT vendors supporting financial institutions must comply with DORA's contractual and security obligations, including cyber incident reporting; and
- threat-led penetration testing (TLPT) – systemically important financial institutions must conduct real-world cyber-attack simulations every three years.

The National Cybersecurity Perimeter Law:

- data localisation requirements – strategic entities must store sensitive data within the EU or in trusted jurisdictions;
- cybersecurity risk assessments – organisations must conduct regular cyber-risk audits and compliance assessments; and
- supply chain security controls – companies must ensure that ICT providers meet national security and cybersecurity standards before engaging in service agreements.

Cyber-Resilience Obligations Under Draft Legislation and Future Regulations

EU AI Act (Draft):

- AI cybersecurity and risk management – AI-driven cybersecurity tools must meet strict risk classification, transparency and security measures; and
- cybersecurity auditing and testing for high-risk AI systems – AI models used in critical infrastructure or financial operations will require external validation and regulatory oversight.

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

Cyber-Resilience Act (Draft – Proposed by the European Commission):

- cybersecurity certification for ICT products – manufacturers of hardware, software and cloud services must obtain EU-wide cybersecurity certification;
- mandatory security updates and patch management – companies must provide continuous security updates to address vulnerabilities; and
- penalties for non-compliance – firms failing to meet cyber-resilience requirements may face severe regulatory sanctions.

Strengthened supply chain cybersecurity rules (upcoming national reforms):

- increased scrutiny of foreign ICT vendors – Italy plans to impose additional restrictions on non-EU cloud and telecommunications providers; and
- expanded cybersecurity requirements for SMEs – more SMEs may be included under mandatory NIS2 compliance.

Key enforcement mechanisms and penalties are as follows.

- Regulatory audits and compliance inspections – the ACN, Bank of Italy, IVASS and Consob enforce cyber-resilience measures through periodic audits.
- Financial penalties:
 - (a) up to EUR10 million or 2% of global turnover for NIS2 non-compliance;
 - (b) up to 4% of global turnover for GDPR violations; and
 - (c) operational restrictions or contract termination orders under DORA for non-compliant ICT providers.

- Incident response enforcement – regulatory authorities can impose remediation measures if cyber incidents expose vulnerabilities in financial or critical infrastructure systems.

Conclusion

Italy's cyber-resilience obligations are among the most stringent in the EU, covering critical infrastructure, financial institutions and digital service providers:

- existing laws (NIS2, DORA, GDPR) mandate cybersecurity risk management, threat monitoring and supply chain security;
- future regulations (the Cyber-Resilience Act, the AI Act) will expand cybersecurity requirements to cover AI and ICT products; and
- regulatory enforcement ensures compliance, with severe penalties for security failures.

These measures fortify national cybersecurity resilience, protect critical services from cyberthreats and ensure compliance with evolving EU Regulations.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

Italy's cybersecurity and cyber-resilience legal framework is shaped by EU Regulations, national laws and sector-specific rules that govern data protection, critical infrastructure security, financial sector resilience and cybercrime prevention.

The GDPR:

- applies to all organisations processing personal data in Italy;

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiaro,
ICT Legal Consulting

- imposes strict security obligations, including encryption, access controls and breach reporting;
- requires notification of personal data breaches within 72 hours; and
- is enforced by the GDPR.

NIS2:

- expands cybersecurity obligations for essential and important entities in critical infrastructure sectors;
- mandates risk management frameworks, security monitoring and cyber incident reporting within 24 hours;
- establishes severe penalties for non-compliance (up to EUR10 million or 2% of global turnover); and
- is enforced by the Agency for National Cybersecurity (ACN).

DORA:

- applies to banks, investment firms, insurers, crypto-asset providers and third-party ICT service providers;
- requires ICT risk management, penetration testing (TLPT) and cyber incident reporting within 72 hours;
- introduces regulatory oversight for cloud providers and ICT vendors supporting financial firms; and
- is enforced by the Bank of Italy, Consob and IVASS.

The National Cybersecurity Perimeter Law:

- establishes cybersecurity obligations for government entities and national critical infrastructure operators;
- requires data localisation and supply chain security assessments for ICT providers;

- imposes mandatory risk assessments and cybersecurity compliance audits; and
- is enforced by the ACN and National Cybersecurity Incident Response Team (CSIRT Italia).

Cybercrime and digital security laws:

- the Italian Penal Code (Articles 615-ter to 640-ter) criminalises unauthorised access, data breaches and cyberfraud;
- Decree Law No 82/2021 created the ACN to centralise cybersecurity governance; and
- Legislative Decree No 231/2001 introduces corporate liability for cybersecurity failures.

Upcoming and draft legislation:

- the Cyber-Resilience Act (EU Draft) will impose mandatory security updates and cybersecurity certification for ICT products;
- the AI Act (EU Draft) will regulate AI-driven cybersecurity tools and risk management systems; and
- the National Supply Chain Security Rules (Upcoming Reforms) are expected to restrict high-risk foreign ICT providers in critical sectors.

Conclusion

Italy enforces a multi-layered cybersecurity legal framework, ensuring:

- strong data protection (GDPR);
- critical infrastructure resilience (NIS2, the National Cybersecurity Perimeter Law);
- financial sector cybersecurity (DORA); and
- cybercrime prevention and ICT vendor oversight.

Future laws will further enhance cyber-resilience, AI security and supply chain protection, reinforcing

ing Italy's national and EU-wide cybersecurity defences.

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

Italy enforces strict cybersecurity obligations under the GDPR and national data protection laws. These rules require organisations processing personal data to implement technical and organisational security measures to prevent data breaches, unauthorised access and cyberthreats.

Key Cybersecurity Obligations Under the GDPR

Risk-based security measures (Article 32, GDPR)

Organisations must implement appropriate technical and organisational security measures based on data sensitivity and processing risks.

Required measures include:

- data encryption and pseudonymisation to protect personal information;
- access controls and multi-factor authentication (MFA) to limit unauthorised access; and
- regular cybersecurity audits and vulnerability assessments.

Data breach notification (Articles 33 & 34, GDPR)

Organisations must report personal data breaches to the GPDP within 72 hours.

If the breach poses a high risk to individuals, the organisation must also notify affected data subjects without delay.

Security of processing (Article 25, GDPR – Privacy by Design and by Default)

Organisations must integrate cybersecurity protections from the outset of data-processing activities.

Systems must be configured to minimise data collection, restrict access and ensure secure storage.

Third-party risk management

Companies using cloud services, external data processors or ICT vendors must ensure contractual compliance with GDPR security requirements.

Data-processing agreements (DPAs) must include security guarantees, incident-reporting procedures and compliance obligations.

Enforcement and Penalties for Non-Compliance

Severe GDPR fines apply for cybersecurity failures:

- up to EUR20 million or 4% of global turnover for major violations; and
- additional penalties for failing to report data breaches or lack of adequate security measures.

The GPDP conducts security audits, issues compliance orders and enforces corrective measures.

Conclusion

Italy's data protection cybersecurity obligations require organisations to implement strong security controls, monitor risks and report breaches. Failure to comply can result in significant financial penalties and regulatory actions, reinforcing

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

the importance of robust cybersecurity practices in data-processing activities.

6.2 Cybersecurity and AI

Italy follows EU-wide regulations on AI security and cybersecurity obligations, with upcoming AI-specific laws under the Artificial Intelligence Act (AI Act – EU Draft). Currently, AI systems must comply with GDPR, NIS2, and cybersecurity best practices, ensuring data protection, algorithmic security, and resilience against cyberthreats.

AI Security and Risk Management Obligations

General cybersecurity requirements (the GDPR and NIS2):

- AI systems handling personal data must integrate privacy-by-design principles, ensuring secure data storage, access controls and encryption;
- organisations using AI in critical infrastructure (eg, finance, healthcare, defence) must implement cybersecurity risk assessments; and
- regular penetration testing and AI model security audits are required to prevent data poisoning, adversarial attacks and unauthorised access.

Upcoming AI Act cybersecurity obligations (EU Draft):

- high-risk AI systems (used in finance, biometric identification, law enforcement, etc) must meet strict cybersecurity standards;
- mandatory AI security testing, logging and real-time monitoring to detect cyberthreats and unauthorised modifications; and
- AI developers must conduct adversarial testing to prevent exploitation of machine-learning vulnerabilities.

AI Supply Chain and Third-Party Security Obligations

Cloud AI services and external AI vendors must meet cybersecurity certification standards before integration.

Financial and critical sectors using AI for fraud detection or automated decision-making must comply with DORA and NIS2 security controls.

AI Cybersecurity Enforcement and Compliance

The GDPR enforces AI security compliance under the GDPR.

The ACN will oversee AI-related cyber-risks under NIS2.

Violations of AI cybersecurity standards could lead to penalties similar to GDPR fines (up to 4% of global turnover).

Conclusion

Italy's AI cybersecurity obligations focus on risk management, data security and adversarial resilience. Future EU AI Act regulations will further tighten cybersecurity requirements for high-risk AI systems, ensuring robust security frameworks and regulatory enforcement.

6.3 Cybersecurity in the Healthcare Sector

Italy enforces strict cybersecurity obligations for the healthcare sector under GDPR, NIS2, and national health data protection laws. These regulations ensure secure processing, storage, and transmission of sensitive health data, protecting medical institutions from cyberthreats, data breaches, and unauthorised access.

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

Key Cybersecurity Obligations Under Healthcare Regulations

GDPR:

- healthcare providers and medical institutions must implement technical and organisational security measures to protect sensitive personal health data (special category data under the GDPR);
- mandatory encryption, access control and anonymisation for patient records; and
- breach notification within 72 hours to the GPDP if a medical data breach occurs.

NIS2:

- hospitals, laboratories and digital healthcare services are classified as “essential entities” and must implement robust cybersecurity risk management;
- 24-hour incident reporting requirement to ACN for cyber-attacks affecting healthcare operations; and
- regular cybersecurity audits, resilience testing and supply chain security assessments are mandatory.

Electronic Health Record (EHR) and telemedicine regulations:

- digital medical records and e-prescription systems must comply with secure data storage and transmission standards; and
- healthcare IoT devices and telemedicine platforms must include built-in cybersecurity protections to prevent remote hacking and patient data breaches.

Cybersecurity Compliance and Enforcement

The Italian Ministry of Health and GPDP oversee compliance with health data security regulations.

Non-compliance with healthcare cybersecurity laws can result in fines of up to EUR20 million or 4% of global turnover under the GDPR.

The ACN enforces cybersecurity resilience for hospitals and digital health providers under NIS2.

Conclusion

Italy’s healthcare cybersecurity laws impose strict data protection, network security and incident-reporting requirements. Hospitals, medical institutions and digital health services must comply with the GDPR and NIS2 to ensure patient data confidentiality, system resilience and regulatory compliance.

Trends and Developments

Contributed by:

Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiaro

ICT Legal Consulting

ICT Legal Consulting ICT Legal Consulting (ICTLC) is an international law firm that offers strategic support in legal compliance (privacy, IP and TMT) and assists in drafting and developing governance, organisation, management, security and control models for data-driven organisations. The firm has successfully assembled a close-knit team of more than 80 qualified professionals specialising in the fields of ICT, privacy, data protection, cybersecurity, and IP law.

ICTLC has offices in Italy (Milan, Bologna, and Rome), the Netherlands (Amsterdam), Greece (Athens), France (Paris), Spain (Madrid), Finland (Helsinki), Sweden (Gothenburg), Nigeria (Lagos), Kenya (Nairobi), Saudi Arabia (Riyadh) and Australia (Melbourne). It has also established partnerships with law firms and professionals in 56 other countries, giving clients access to the most qualified professionals who are most suited to their specific needs.

Authors



Paolo Balboni is a founding partner at ICTLC – ICT Legal Consulting. Paolo, a top-tier European ICT, privacy and cybersecurity lawyer, serves as the data protection officer for

multinational companies. He is a Professor of Privacy, Cybersecurity and IT Contract Law at the European Centre on Privacy and Cybersecurity within the Maastricht University Faculty of Law, and a member of the EUMETSAT Data Protection Supervisory Authority and the Europrivacy Board of Experts. Paolo is admitted to the Milan and Amsterdam Bars. He is involved in European Commission studies on new technologies, in addition to participating in the revision of the EU Commission proposal for a General Data Protection Regulation.



Luca Bolognini is a founding partner at ICTLC – ICT Legal Consulting. Luca, a European privacy and data protection lawyer, and has been President of the Italian Institute for Privacy

and Data Valorisation since 2008. He is a member of the IAPP and CIPP/E, and a TÜV Italia Certified Privacy Officer. Luca serves as an independent ethics and privacy adviser for several European research and innovation projects (Horizon 2020) and as an expert coach for the Executive Agency for Small and Medium-sized Enterprises of the European Commission. He is a member of the Experts Board of EU-IoT and co-chair of the Europrivacy Certification Scheme Board of Senior Experts.

ITALY TRENDS AND DEVELOPMENTS

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiaro,
ICT Legal Consulting



Francesco Capparelli is chief cybersecurity adviser at ICTLC – ICT Legal Consulting and ICT Cyber Consulting. Francesco is a lawyer, qualified auditor/lead auditor ISO/IEC 27001, ISO

22301, ISO 37001, ISO/IEC 20000-1, ISO 9001, Certified Ethical Hacker, CIPPM and data protection officer. He obtained three master's degrees from LUISS University and Link Campus University in Rome, in Competition Law and Innovation with a specialisation in Privacy and Big Data; in Cybersecurity with a specialisation in Artificial Intelligence and Biometrics; and in Blockchain with a specialisation in Smart Contracts. He is also a certified PRINCE 2 project manager.



Giulia Finocchiaro is a cybersecurity adviser at ICTLC – ICT Legal Consulting and ICT Cyber Consulting. She has a broad legal background and is a qualified auditor/lead auditor

ISO/IEC 27001 and ISO 22301. After graduating in law, she obtained a diploma from the School of Specialisation for the Legal Professions, which further refined her legal skills. She obtained a master's degree in Cybersecurity Culture and Governance from the University of Catania, which deepened her knowledge of the sector. She is also actively involved in research activities, demonstrating her commitment to the advancement of cybersecurity and data protection.

ICTLC – ICT Legal Consulting

Via Borgonuovo 12
20121 Milan
Italy

Tel: +39 028 424 7194
Fax: +39 0270 0512 101
Email: info@ictlc.com
Web: www.ictlc.com



Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

Cybersecurity and digital resilience are critical priorities in Italy, shaped by new EU Regulations, evolving cyberthreats and increasing digital transformation across industries. Businesses operating in Italy must adapt to a rapidly changing regulatory and risk landscape, ensuring compliance with stringent cybersecurity obligations while mitigating emerging cyber-risks.

Regulatory Evolution: Strengthening Cybersecurity Laws

Implementation of NIS2 and national cybersecurity reforms

Italy has adopted Legislative Decree No 138/2024, implementing the NIS2 Directive (Directive (EU) 2022/2555) and significantly expanding cybersecurity compliance obligations for essential and important entities. Key regulatory shifts include:

- broader industry coverage – NIS2 applies to energy, healthcare, banking, digital infrastructure and transport, imposing mandatory risk management and incident-reporting obligations;
- tighter incident reporting rules – businesses must report cyber incidents within 24 hours to the Agency for National Cybersecurity (ACN), reinforcing real-time cyberthreat monitoring; and
- stronger supply chain security – companies must assess and monitor third-party ICT providers, ensuring compliance with cybersecurity standards.

Italy's National Cybersecurity Perimeter Law (Legislative Decree No 105/2019) also enforces data localisation requirements, requiring critical infrastructure operators to store and process security-sensitive data within the EU or in trusted jurisdictions.

DORA and financial sector digital resilience

The Digital Operational Resilience Act (DORA – Regulation (EU) 2022/2554) directly applies to Italy's financial sector, introducing strict cyber-resilience and ICT risk management standards:

- banks, insurers and investment firms must implement continuous security monitoring, penetration testing and cyber incident response plans;
- financial entities must report major cyber incidents within 72 hours, ensuring regulatory oversight and co-ordinated incident response; and
- third-party ICT providers (cloud services, cybersecurity vendors) supporting financial institutions must comply with contractual security obligations, ensuring full regulatory supervision.

These regulations signal a shift from reactive cybersecurity measures to proactive resilience strategies, requiring financial institutions and ICT vendors to enhance cyber defences.

Emerging Cyberthreats and Risk Landscape *Rise in ransomware and cyber-extortion attacks*

Italy has seen a surge in ransomware incidents, targeting public institutions, healthcare providers and large corporations. Cybercriminals exploit vulnerabilities in outdated IT systems and third-party supply chains, demanding ransom payments in cryptocurrency to avoid data leaks.

Businesses must implement advanced endpoint protection, secure back-up solutions and real-time threat intelligence-monitoring to mitigate ransomware risks.

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

Supply chain attacks and third-party risk

Cybercriminals increasingly target ICT vendors, cloud service providers and managed security services to infiltrate large enterprises and government networks:

- NIS2 and DORA mandate third-party risk assessments, requiring businesses to conduct due diligence on ICT suppliers; and
- companies must ensure that contractual agreements with vendors include cybersecurity standards, incident-response obligations and compliance audits.

AI-powered cyberthreats

The adoption of artificial intelligence (AI) and automation in cybersecurity presents both opportunities and risks. While AI enhances threat detection and anomaly identification, cybercriminals are leveraging AI-driven attacks, including deepfake fraud and automated phishing campaigns.

With the EU AI Act in development, companies deploying AI-based security tools must comply with transparency, accountability and risk mitigation requirements.

Compliance Challenges and Business Adaptation

Increased regulatory complexity

The overlap of cybersecurity laws (the GDPR, NIS2, DORA and national regulations) creates compliance challenges for businesses, particularly multinational corporations operating in Italy.

To navigate regulatory complexities, organisations must:

- adopt integrated cybersecurity frameworks, aligning with EU and national requirements;

- develop multi-jurisdictional incident-response policies, ensuring compliance with sector-specific reporting rules; and
- enhance cross-functional collaboration between legal, IT security and risk management teams to meet evolving obligations.

Operational and financial burden on SMEs

While large corporations can invest in cybersecurity infrastructure and compliance programmes, small and medium-sized enterprises (SMEs) face financial and technical challenges in meeting regulatory standards:

- SMEs must leverage government incentives and public-private cybersecurity partnerships to access affordable security solutions; and
- regulatory bodies are introducing simplified compliance frameworks for SMEs to balance security with operational feasibility.

Future Outlook: Strengthening Cyber-Resilience in Italy

Cybersecurity investment and public-private collaboration

Italy is expanding investment in cybersecurity innovation, fostering collaboration between government agencies, private enterprises and academia to strengthen national cyber defence capabilities:

- the National Cybersecurity Strategy (2022–2026) promotes investments in cybersecurity R&D, skills development and cyber intelligence sharing; and
- public-private partnerships are enhancing real-time threat intelligence exchange, improving national resilience against State-sponsored attacks and cyber espionage.

Contributed by: Paolo Balboni, Luca Bolognini, Francesco Capparelli and Giulia Finocchiario,
ICT Legal Consulting

Focus on AI and quantum-resistant cybersecurity

AI-powered cybersecurity solutions will play a key role in automating threat detection, response and risk analysis.

Quantum-resistant cryptography is emerging as a critical area of research, ensuring long-term protection against quantum computing threats.

Harmonisation of cybersecurity standards across the EU

The EU Cyber-Resilience Act (expected in 2025) will introduce mandatory cybersecurity certification for ICT products, further harmonising cyber-risk management across sectors.

Italy will need to adapt national regulations to align with new EU cybersecurity frameworks, ensuring interoperability and compliance efficiency.

Conclusion

Italy's cybersecurity landscape is rapidly evolving, driven by regulatory reforms, emerging cyberthreats and technological advancements. Businesses must proactively enhance cyber-resilience, adopting risk-based security strategies, compliance automation and advanced threat intelligence to navigate the growing complexity of cybersecurity obligations.

As digital transformation accelerates, organisations that prioritise cybersecurity investments, strengthen regulatory compliance and adopt cutting-edge security technologies will gain a competitive advantage in the Italian market.

JAPAN

Law and Practice

Contributed by:

Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii
Mori Hamada & Matsumoto



Contents

1. General Overview of Laws and Regulators p.166

- 1.1 Cybersecurity Regulation Strategy p.166
- 1.2 Cybersecurity Laws p.166
- 1.3 Cybersecurity Regulators p.168

2. Critical Infrastructure Cybersecurity p.168

- 2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.168
- 2.2 Critical Infrastructure Cybersecurity Requirements p.169
- 2.3 Incident Response and Notification Obligations p.169
- 2.4 State Responsibilities and Obligations p.171

3. Financial Sector Operational Resilience Regulation p.171

- 3.1 Scope of Financial Sector Operational Resilience Regulation p.171
- 3.2 ICT Service Provider Contractual Requirements p.171
- 3.3 Key Operational Resilience Obligations p.172
- 3.4 Operational Resilience Enforcement p.172
- 3.5 International Data Transfers p.172
- 3.6 Threat-Led Penetration Testing p.173

4. Cyber-Resilience p.173

- 4.1 Cyber-Resilience Legislation p.173
- 4.2 Key Obligations Under Legislation p.173

5. Security Certification for ICT Products, Services and Processes p.173

- 5.1 Key Cybersecurity Certification Legislation p.173

6. Cybersecurity in Other Regulations p.173

- 6.1 Cybersecurity and Data Protection p.173
- 6.2 Cybersecurity and AI p.173
- 6.3 Cybersecurity in the Healthcare Sector p.173

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,
Mori Hamada & Matsumoto

Mori Hamada & Matsumoto is a full-service law firm that has served clients with distinction since its establishment in December 2002. Mori Hamada & Matsumoto is made up of experienced lawyers with considerable expertise in the constantly evolving and increasingly complex areas of information technology, life sciences and intellectual property, providing a variety of legal services in response to the diverse

legal needs of its clients. These legal services include advising on regulatory requirements, setting up business, corporate housekeeping, contract negotiations and dispute resolution. In terms of data protection, the firm has noted expertise in leveraging user information while protecting clients' businesses. Mori Hamada & Matsumoto's data protection team comprises approximately 130 lawyers.

Authors



Yoshifumi Onodera is a partner at Mori Hamada & Matsumoto. Highly experienced in all kinds of data-related matters involving communication, media, competition, consumer and/or

information laws, he is particularly adept at delivering advice to both foreign and domestic clients on complex business structures spanning vast content and communication-related industries, including internet-related services, social networking services, games, music, movies and telecommunications. His expertise also extends to IP-related transactions, concerning licensing and dispute resolution aspects in the subsidiary fields of infringement litigation, invalidity trials, appellate litigation and arbitration, and licensing in relation to intellectual property, including patents, trademarks and copyright.



Hiroyuki Tanaka is a partner at Mori Hamada & Matsumoto, admitted to practise in Japan (Daini Tokyo Bar Association) and New York. Hiroyuki's practice areas are data

protection, IT and IP, and he has substantial experience advising foreign clients on Japanese data protection law. He is also familiar with global data protection regulations, including the GDPR and CCPA, and helps Japanese clients with global data protection compliance by working closely with local counsel. His practice area includes legal issues relating to AI (especially generative AI) and the protection of cybernetic avatars. He is an adjunct project professor at Keio University Graduate School of Law (2023-present).

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,
Mori Hamada & Matsumoto



Naoto Shimamura is a senior associate at Mori Hamada & Matsumoto, licensed in Japan (Daini Tokyo Bar Association), California and New York, and a lecturer at Ochanomizu

University and Japan Women's University. He uses his in-depth knowledge of computers and the internet to engage in technology-related cases, including those involving e-commerce, consumer protection, licensing, privacy, data protection, cybersecurity, defamation on the internet, intellectual property and dispute resolution. Naoto is also qualified as a Certified Information Privacy Professional/Europe (CIPP/E), a Certified Information Privacy Professional/United States (CIPP/US), and a Registered Information Security Specialist, which is recognised as the highest level of security engineering qualification in Japan.



Rio Ichii is a junior associate at Mori Hamada & Matsumoto, licensed in Japan (Daiichi Tokyo Bar Association). She has a broad portfolio and a wealth of experience across a number of practice areas, including IT, intellectual property, healthcare and trade law. She has also written many articles on these topics.

Mori Hamada & Matsumoto

16th Floor, Marunouchi Park Building
2-6-1 Marunouchi
Chiyoda-ku
100-8222
Tokyo
Japan

Tel: +81 362 128 330
Fax: +81 362 128 230
Email: info@morihamada.com
Web: www.morihamada.com

MORI HAMADA & MATSUMOTO

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,
Mori Hamada & Matsumoto

1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

The Basic Act on Cybersecurity is Japan's fundamental law on cybersecurity, and the Act on the Protection of Personal Information (APPI) is the country's principal data protection law.

Pursuant to the APPI, a personal data breach is subject to mandatory reporting and notification requirements – see **2.3 Incident Response and Notification Obligations**.

However, there is no general regulation imposing a mandatory reporting obligation for a cybersecurity incident that does not involve a personal data breach.

The Unfair Competition Prevention Act prohibits the infringement of trade secrets, and the Act on Prohibition on Unauthorised Computer Access outlaws unauthorised computer access. The Penal Code also includes penalties for some cybersecurity crimes. The Telecommunications Business Act requires telecommunications carriers to ensure the secrecy of communications.

Japan does not have specific regulations for secure software development.

For more details on the laws cited above and other relevant laws, see **1.2 Cybersecurity Laws**.

1.2 Cybersecurity Laws

The Basic Act on Cybersecurity regulates the responsibility of the national government and local governments for cybersecurity (Articles 4 and 5). It also stipulates the obligation of critical information infrastructure operators, cyberspace-related business providers, and research

institutions such as universities (Articles 6, 7 and 8) to exert efforts to ensure cybersecurity.

The APPI, Japan's principal data protection law, provides the basic principles for the government's regulatory policies and authority, as well as requirements for handling operators.

Another important law is the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures (the "My Number Act"), which stipulates special rules for "my number" – a 12-digit individual number assigned to each resident of Japan.

The *kyorei*, or ordinances, enacted by local governments contain public sector obligations.

The Unfair Competition Prevention Act prohibits the infringement of trade secrets and provides for cause of actions in civil cases, such as compensation for damages and injunctive relief, as well as criminal sanctions. Information that is not protected as a trade secret may instead be protected as "data for limited provision". An unauthorised acquisition or utilisation of data for limited provision may be deemed to be unfair competition, which is subject to compensation for damages and injunctive relief but not criminal sanctions.

The Act on the Prohibition on Unauthorised Computer Access outlaws:

- the use of another person's identification code (eg, a password) to access remote computers via a telecommunications network;
- inputting information (excluding an identification code) or a command to evade access restrictions on remote computers via a telecommunications network;

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,
Mori Hamada & Matsumoto

- obtaining, supplying or storing someone else's identification code without legitimate reason (Articles 3, 4, 5 and 6); and
- phishing or creating a false impression of being the network administrator concerned and requesting identification codes (Article 7).

The Penal Code prohibits:

- the creation of false electromagnetic records that are related to rights, duties or the certification of facts (Article 161–2);
- fraud by using computers (Article 246–2);
- the destruction of electromagnetic records in use by a public office or concerning private rights or duties (Articles 258 and 259);
- the obstruction of a business by damaging its computers or electromagnetic records or causing them to operate counter to their original purpose (Article 234–2); and
- the creation, provision, acquisition or storage of a computer virus (Articles 168–2 and 168–3).

The Telecommunications Business Act requires telecommunications carriers to ensure the secrecy of communications (Article 41.6 (iii)) and to report serious breaches to the Ministry of Internal Affairs and Communications (MIC).

The Installment Sales Act requires businesses who handle credit card numbers to take necessary and appropriate measures to prevent the leakage, loss of, or damage to those credit card numbers (Article 35–16).

The Payment Services Act requires prepaid payment instrument issuers, funds transfer service providers, and virtual currency exchange service providers to take necessary and appropriate measures to prevent the leakage, loss of,

or damage to information pertaining to their respective businesses (Articles 21, 49 and 63–8).

Sector-specific regulators impose additional information security obligations on some industries including the financial and healthcare industries. For the financial sector, the Financial Services Agency (FSA) issued the Comprehensive Guidelines for the Supervision of Major Banks, which provide for cybersecurity obligations of financial institutions. For details on cybersecurity guidelines in finance, see **3. Financial Sector Operational Resilience Regulation**. As for the healthcare industry, an enforcement order on the Medical Care Act requires hospitals, clinics and birthing centres to take appropriate steps to ensure cybersecurity (Article 14.2) and an enforcement order of the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices also requests pharmacies to do the same (Article 11.2). Further, various ministries have issued other relevant guidelines:

- the Ministry of Health, Labour and Welfare (MHLW) issued the “Guidelines on Safety Management of Medical Information Systems” (last amended in May 2023);
- the Ministry of Economy, Trade and Industry (METI) and MIC jointly issued the “Safety Management Guidelines for Providers of Information Systems and Services Handling Medical Information” (last amended in July 2023);
- the MIC published comprehensive measures for the security of the internet of things (IoT) (July 2016); and
- the MIC published guidelines on the application of the Telecommunications Business Act to reports of serious accidents (volume 7, December 2023).

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,
Mori Hamada & Matsumoto

1.3 Cybersecurity Regulators

The regulator tasked with enforcing and implementing the APPI is the Personal Information Protection Commission (PPC), which has the following powers under the APPI:

- to require private business operators who handle personal information (handling operators) to report or submit materials regarding its handling of personal information (Article 146), which the APPI defines as information about living individuals that can identify specific individuals or contains what is referred to in the APPI as an “individual identification code” (Article 2.1);
- to enter a handling operator’s offices or other places to investigate, make enquiries and check records or other documents (Article 146);
- to provide guidance or advice to a handling operator (Article 147);
- to recommend that a handling operator cease any act constituting a violation of the APPI and take other necessary measures to correct the violation (Article 148.1);
- to order a handling operator to take necessary measures to implement the PPC’s recommendation mentioned above and to rectify certain violations of the APPI (Articles 148.2 and 148.3); and
- when the PPC issues an order pursuant to Articles 148.2 and 148.3, and a handling operator violates the order, the PPC may publicly announce the violation (Article 148.4).

The National Police Agency and the Public Prosecutors Office are responsible for the criminal investigation and prosecution of cybercrimes.

As for non-regulatory government authorities that are also directly involved with cybersecurity, the Information Technology Promotion Agency

of Japan (IPA) and the National Center for Incident Readiness and Strategy for Cybersecurity (NISC) are notable. The IPA regularly publishes important guidelines and provides information on cybersecurity. The more important guidelines include the Cybersecurity Management Guidelines, guidelines for small and mid-sized companies on information security, and guidelines on preventing insider data breaches. The IPA also runs the J-CSIP, or the Initiative for Cybersecurity Information Sharing Partnership of Japan, which shares cybersecurity information of critical information infrastructure operators (ie, operators of businesses that provide infrastructure that is the foundation of people’s living conditions and economic activities, the functional failure or deterioration of which could have a highly significant impact on people). NISC is responsible for national-level cybersecurity under the Basic Act on Cybersecurity and regularly publishes updates to Japan’s Cybersecurity Strategy. For more on other regulators, refer to the previous sections in **1. General Overview of Laws and Regulators**.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

The Cybersecurity Policy for Critical Infrastructure Protection defines the following 15 sectors as critical information infrastructure:

- airports;
- aviation;
- chemical industry;
- credit cards;
- electric power supply;
- financial services;
- gas supply;

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,
Mori Hamada & Matsumoto

- information and communication;
- government and administration;
- logistics and shipping;
- medical;
- petroleum industry;
- ports and harbours;
- railways; and
- water supply.

The aforementioned Cybersecurity Policy also encourages critical information infrastructure operators to periodically assess their progress in implementing security measures and policies.

2.2 Critical Infrastructure Cybersecurity Requirements

Under the APPI, a handling operator not limited to critical infrastructure must take necessary and appropriate action for security control over the personal data that it handles, including preventing the leakage, loss or damage of or to personal data (Article 23).

The PPC is the regulator primarily responsible for the APPI and the My Number Act; it has published guidelines for the handling of personal information (the “PPC Guidelines”).

The PPC Guidelines provide examples of these handling measures, such as establishing and implementing basic policies, internal rules, and organisational, personal and technical security measures, as well as understanding of the external environment. “Understanding of the external environment” is a security measure, newly introduced by the amendments to the Guidelines, which requires a handling operator who processes personal data in a foreign country to understand the foreign country’s legal system for personal information protection and, taking into consideration that legal system, to take necessary and appropriate measures to ensure the

security of personal data. Effective from 1 April 2024, the PPC Guidelines also require a handling operator to take security control over personal information that is collected and expected to be treated as personal data so that a cyber-attacker may not intercept such information on behalf of the operator.

According to the APPI, when a handling operator allows its employees to handle personal data, it must exercise necessary and appropriate supervision over the employees to ensure security control over the personal data (Article 24). The APPI also requires a handling operator to ensure that the entity to whom it has entrusted the handling of personal data (eg, a third-party vendor) takes appropriate measures to ensure security control over the personal data (Article 25).

Under the Economic Security Promotion Act, important critical infrastructure businesses are individually designated by the competent ministry as Specified Essential Infrastructure Service Providers. They are required to take measures to reduce or eliminate risk factors among parties involved in the supply chain. Some of the requirements include establishing measures to:

- prevent unauthorised changes to specified critical facilities;
- prevent service interruptions;
- confirm any legal or contractual violations by parties involved in the supply chain; and
- prevent unintended changes by subcontractors.

2.3 Incident Response and Notification Obligations

The Cybersecurity Policy for Critical Infrastructure Protection provides for the reporting obligations of critical information infrastructure operators in the following instances:

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,
Mori Hamada & Matsumoto

- if there is a legal reporting requirement by law or regulation;
- if the operator has determined that an incident has had a serious impact on the lives of people or the operator's services and that information must be shared; and
- in other cases where the operator has determined that information must be shared.

Definition of Data Security Incident, Breach or Cybersecurity Event

The APPI stipulates mandatory obligations to report data breach incidents to the PPC and to notify affected data subjects in cases where their rights and interests are likely to be infringed (Article 26). The PPC Ordinance defines a data security incident or breach as the occurrence or possible occurrence of the leakage or loss of, or damage to personal data. The details of the requirements are discussed below.

There is also a special rule for “my numbers” under the My Number Act. There is no general regulation to impose a mandatory reporting obligation for a cybersecurity incident that does not involve a personal data breach. However, there are various regulations generally mandating certain types of service providers to report an incident affecting their service to the authorities. This reporting obligation also covers cases where service failure happens as a result of a cyber-attack.

For example, under the Telecommunications Business Act, if an accident occurs and causes a suspension or deterioration of the quality of services for more than the prescribed number of hours and affects a certain number of users specified by the relevant ordinance, the telecommunications business operator must report the accident to the MIC. Furthermore, the MIC has the authority to issue orders to improve the busi-

ness practices of licensed telecommunications service providers. Another example is financial institutions; many laws regulating financial sectors oblige them to report material service failure to its authorities.

Data Elements Covered

Breach of data security is applicable to personal data. The APPI defines personal data as personal information that is contained in a personal information database (Article 16.3), which is a collection of information (which includes personal information) that is systematically organised to enable a computer or some other means to search for particular personal information. However, this term excludes a collection of information that a Cabinet Order indicates as having little possibility of harming an individual's rights and interests considering how that collection uses personal information (Article 16.4). Examples of collections of information that are excluded from this definition include a commercially available telephone directory or a car navigation system.

The PPC Ordinance prescribes that a mandatory data breach report is required if a data breach includes personal data (excluding advanced encryption or other measures that are necessary to protect the rights and interests of the individual):

- containing “special care-required personal information”;
- that is likely to cause property damage if used inappropriately;
- that is likely to have been committed for an improper purpose (effective from 1 April 2024, personal information that is already collected or will be collected and expected to be treated as personal data is also included in this requirement); or
- of more than 1,000 individuals.

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,
Mori Hamada & Matsumoto

Special care-required personal information is defined as personal information comprising a data principal's race, creed, social status, medical history, criminal record, the fact of having been a victim of a crime, or other descriptions that may be prescribed by a cabinet order as requiring special care in handling so as not to cause unfair discrimination, prejudice or other disadvantages to the data subject (Article 2.3).

2.4 State Responsibilities and Obligations

Governmental authorities that have specific jurisdiction over some of the 15 critical information infrastructure sectors have issued specific guidelines, described below, concerning cybersecurity.

For the healthcare industry, see **6.3 Cybersecurity in the Healthcare Sector**. For the financial industry, see **3. Financial Sector Operational Resilience Regulation**.

The Ministry of Land, Infrastructure, Transport and Tourism (MLIT) issued:

- the Safety Guidelines for Ensuring Information Security for Air Transport Operators for aviation services;
- the Safety Guidelines for Securing Information Security in the Airport Sector for airport services;
- the Safety Guidelines for Ensuring Information Security for Railway Operators for railway services; and
- the Safety Guidelines for Ensuring Information Security for the Logistics Sector for logistics services.

The MLIT also issues information security countermeasure checklists for railway service, bus

service, bus terminals, taxis, hotels, ferries, and airports and airport buildings.

The MHLW issued the Information Security Guidelines for the Water Sector for water services.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

The FSA issued the Comprehensive Guidelines for the Supervision of Major Banks, etc. (the "Comprehensive Guidelines for SMB"), which mention cybersecurity obligations, referring to the Guidelines for Cyber Security in Finance Sector (the "Guidelines for CSFS"). The Comprehensive Guidelines for SMB further include measures regarding operational resilience. Operational resilience refers to the ability of financial institutions to continue to maintain the minimum level of their critical operations even in the event of a system failure, terrorist attack, cyber-attack, infectious disease, natural disaster or other event. The Comprehensive Guidelines for SMB specify the actions to be taken by the board of directors and the regulations of the authorities to achieve operational resilience.

3.2 ICT Service Provider Contractual Requirements

Not limited to the financial sector, when a handling operator entrusts personal data, it must exercise the necessary and appropriate supervision over the entrusted person to ensure security control over the entrusted personal data (Article 25 of the APPI). Handling operators shall supervise the entrustees to ensure that the same levels of security control are taken as those imposed on the operators under the APPI.

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,
Mori Hamada & Matsumoto

If a handling operator uses cloud services, it may not be considered as entrustment and thus, the aforesaid obligation under Article 25 of the APPI does not apply. Instead, businesses that use cloud services must still take appropriate security control over the personal data stored in cloud services as part of their own duties.

3.3 Key Operational Resilience Obligations

The Comprehensive Guidelines for SMB require businesses to report to the authorities when they become aware of a computer system failure or cybersecurity incident, when they are recovering from such incidents, and when they have identified the cause of an incident. Where the business detects that cyber-attack will or is highly likely to have an impact on customers or business, a report is required even if the system failure or incident does not occur. For details of the Comprehensive Guidelines, see 3.1 **Scope of Financial Sector Operation Resilience Regulation**.

3.4 Operational Resilience Enforcement

The FSA may impose administrative disposition on financial businesses that may violate or may have violated laws and regulations. Such disposition includes on-site inspections and orders to improve business operations.

3.5 International Data Transfers

For offshoring, there are special restrictions on the transfer of personal data to a foreign country. In principle, the APPI requires the transferor to obtain the prior consent of individuals whose personal data will be transferred to a third party located in a foreign country (Article 28). In other words, overseas transfer restrictions will apply if a foreign company transfers user data to another company outside Japan. Conversely, if a foreign company transfers user data to a company in

Japan, these overseas transfer restrictions will not apply. The overseas transfer restrictions apply even in the cases of outsourcing that are exceptions to local third-party data transfer restrictions.

The data subjects' consent to overseas data transfers is not necessary if:

- the foreign country is designated by the PPC as a country with a data protection regime with a level of protection equivalent to that of Japan (only EEA member countries and the UK have been designated to date);
- the third-party recipient has an equivalent system of data protection that meets the standards prescribed by the Ordinance issued by the PPC (the PPC Ordinance) – ie, either of the following:
 - (a) there is assurance, by appropriate and reasonable methodologies, that the recipient will treat the disclosed personal data in accordance with the spirit of the requirements on handling personal data under the APPI; or
 - (b) the recipient has been certified under an international arrangement, recognised by the PPC, regarding its system of handling personal data.

The implementation of the PPC Ordinance is set out in the PPC Guidelines, which provide that “appropriate and reasonable methodologies” include agreements between the data importer and the data exporter, or inter-group privacy rules, which ensure that the data importer will treat the disclosed personal data in accordance with the spirit of the APPI. With respect to a PPC recognised international framework, to date, the PPC Guidelines have identified only the Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) as a recog-

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,
Mori Hamada & Matsumoto

nised international framework on the handling of personal data.

3.6 Threat-Led Penetration Testing

The Guidelines for CSFS require that threat-led penetration testing (TLPT) be carried out on a regular basis.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

There is no uniform legislation on cyber-resilience. Specific aspects of cyber-resilience are stipulated in each of the individual regulations.

4.2 Key Obligations Under Legislation

Specific aspects of cyber-resilience are stipulated in each of the individual regulations.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

The Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements provides an evaluation index for the security functions of IoT products. This system will be provided by the IPA, and applications are scheduled to begin in March 2025.

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

Handling operators have to establish appropriate safeguards to protect personal data (Article 23 of the APPI) and have to report data breaches to the PPC and notify affected data subjects in cases where their rights and interests are likely to have been infringed (Article 26 of the APPI).

6.2 Cybersecurity and AI

The MIC and METI published the AI Business Guidelines for AI developers, AI service providers and AI users on 19 April 2024. These Guidelines urge businesses to invest in and implement robust security management throughout the entire AI lifecycle, including cybersecurity. They also suggest considering appropriate cyber-access controls.

6.3 Cybersecurity in the Healthcare Sector

The MHLW has issued the Guidelines on the Safety Management of Medical Information Systems (last amended in May 2023). While the MHLW Guidelines and an announcement issued by the MHLW on 29 October 2018 state that medical service providers should report a cybersecurity incident to the authority, no special rule has been issued for statutory data breach reporting and notifications in this regard.

The MIC and METI have jointly issued the Guidelines for Safety Management of Medical Information by Providers of Information Systems and Services Handling Medical Information (last amended in July 2023).

Trends and Developments

Contributed by:

Yasushi Kudo, Yukiko Konno and Takayuki Inukai
Nagashima Ohno & Tsunematsu

Nagashima Ohno & Tsunematsu is one of the foremost providers of international and commercial legal services, based in Tokyo. The firm has approximately 600 lawyers, including nearly 50 experienced foreign lawyers from various jurisdictions. Its overseas network includes offices in New York, Singapore, Bangkok, Ho Chi Minh City, Hanoi and Shanghai, Jakarta and collaborative relationships with prominent local law firms throughout Asia, Europe, North and South America, and other regions. The firm provides comprehensive assistance in the devel-

opment of cybersecurity systems, including the establishment of internal governance systems and vendor management. It also has extensive experience in crisis management in the event of a security incident. In collaboration with IT system experts, the firm also provides one-stop support for the entire process, from the initial response, including fact-finding and evidence preservation, to dealing with the authorities, information disclosure and the mass media, liaising with victims, root cause analysis and recurrence prevention measures.

Authors



Yasushi Kudo is a partner at Nagashima Ohno & Tsunematsu. He mainly focuses his practice on crisis management, including dealings with domestic and international authorities,

regulatory compliance, cybersecurity/data privacy, and advice on compliance systems and corporate governance, leveraging his expertise and experience gained from secondment to the Financial Services Agency and the Securities and Exchange Surveillance Commission. Recently, his focus has been on legal issues raised by cybersecurity incidents such as ransomware attacks, data compromise and business e-mail compromise, as well as the development of internal control systems so as to mitigate cybersecurity risks such as supply chain risk.



Yukiko Konno is a counsel at Nagashima Ohno & Tsunematsu. Her practice primarily focuses on domestic and global data governance and other emerging areas, including cybersecurity,

data privacy/data protection, AI and IoT issues, as well as cross-border general corporate matters across a range of industry sectors. She is a graduate of Keio University (2005), Chuo Law School (JD, 2008) and Columbia Law School (LLM, 2015). She was seconded to a private trading company (2015–17) and the Trade Policy Bureau of Ministry of Economy, Trade and Industry of Japan (METI) (2019–22).

Contributed by: Yasushi Kudo, Yukiko Konno and Takayuki Inukai,
Nagashima Ohno & Tsunematsu



Takayuki Inukai is an associate at Nagashima Ohno & Tsunematsu. His practice primarily focuses on technology, media and telecommunications (TMT) including data privacy,

cybersecurity, telecommunications regulation and intellectual property. He provides advice in various situations, utilising his technical expertise. He is a graduate of the Department of Computer Science and Engineering, Waseda University in 2018 (Bachelor of Engineering). He was seconded to the Telecommunications Bureau and Information and Communications Bureau of the Ministry of Internal Affairs and Communications (MIC) (2022-24).

Nagashima Ohno & Tsunematsu

JP Tower, 2-7-2 Marunouchi
Chiyoda-ku
Tokyo 100-7036
Japan

Tel: +81 368 897 396
Fax: +81 368 898 396
Email: yasushi_kudo@noandt.com
Web: www.noandt.com/en/lawyers/yasushi_kudo/

The logo for Nagashima Ohno & Tsunematsu, consisting of the firm's name in white serif capital letters on a dark blue rectangular background.

NAGASHIMA
OHNO &
TSUNEMATSU

Contributed by: Yasushi Kudo, Yukiko Konno and Takayuki Inukai,
Nagashima Ohno & Tsunematsu

Introduction

In 2024, as in previous years, numerous incidents involving the leakage of personal data occurred in Japan due to cyber-attacks such as ransomware and internal misconduct by outsourced contractors. In response, the Personal Information Protection Commission (PPC), the Japanese data protection authority, has decided to publish quarterly summaries of its supervision activities, detailing the content of its administrative guidance and advice. In this context, the PPC has focused on issues related to the “handling of large volumes of personal information”, identifying problems with security measures and the need for necessary and appropriate oversight of data processors. Taking into consideration past judicial precedents in Japan regarding data breaches, these insights provide valuable references in order for businesses managing significant volumes of personal information to assess the required security standards. This article highlights these developments and introduces trends in legal reforms surrounding cybersecurity in Japan.

Recent Enforcement and Administrative Guidance by the PPC

Since August 2024, the PPC has published quarterly reports summarising its “Overview of the Exercise of Monitoring and Supervisory Authority” and the “Handling Status of Breach Notifications” (as of the end of December 2024, the latest being the second quarter of FY2024). While the PPC has previously disclosed cases of administrative guidance or advice based on the severity of incidents, these announcements were limited in scope. The quarterly reports thus serve as valuable reference materials for businesses to understand the PPC’s enforcement policies on data breach incidents.

Handling status of breach notifications

In the second quarter of FY2024, there were 3,599 reports of breaches from businesses handling personal information. Of these, 1,087 cases (30.2%) stemmed from unauthorised access, including breaches caused by external cyber-attacks.

Overview of the exercise of monitoring and supervisory authority

During the second quarter of FY2024, it was reported that there were 87 cases in which the PPC gave administrative guidance and/or gave advice to private businesses. Of these, 70 cases related to security measures (Article 23 of the Japanese Act on Protection of Personal Information (APPI)) and supervision of contractors (Article 25 of the APPI), and 33 cases concerned delays in breach notification submissions. (Note: a single case may fall under multiple categories.)

Among the said 87 cases, 48 involved breaches due to unauthorised access. Excluding formal violations such as delayed reporting, administrative guidance on unauthorised access breaches was most frequent course of action. The PPC gave the following reasons to explain this trend.

- Unlike cases such as the leakage of sensitive personal information, which require reporting even for a single incident, unauthorised access incidents often involve a large number of individuals (most unauthorised access cases involved breaches affecting over 1,000 individuals).
- These incidents were often linked to businesses failing to implement the necessary security measures that should have been in place as a matter of course.

Contributed by: Yasushi Kudo, Yukiko Konno and Takayuki Inukai,
Nagashima Ohno & Tsunematsu

Causes of unauthorised access and content of administrative guidance

For unauthorised access incidents in the second quarter of FY2024, the causes and the types of attack were analysed as follows.

- By cause:
 - (a) software vulnerabilities: 27 cases (including VPN: six, e-commerce sites: five);
 - (b) weak ID/password protection: 22 cases; and
 - (c) misconfigured access controls: 16 cases.
- By type of attack:
 - (a) brute-force attacks: 12 cases;
 - (b) cross-site scripting: six cases;
 - (c) SQL injection: four cases; and
 - (d) ransomware: 21 cases.

Most of the identified inadequacies in security measures for FY2024 concerned technical safeguards. In the second quarter, the most common administrative guidance related to the requirement of “preventing unauthorised external access” (42 cases), followed by “identification and authentication of users” (eight cases).

Primary causes of breaches included:

- known vulnerabilities in VPN devices or applications used to build e-commerce sites left unaddressed by businesses;
- easily guessable IDs and passwords; and
- misconfigured system settings allowing improper database access control.

Such inadequacies in security measures often led to the PPC’s enforcement actions.

Implications for businesses

The PPC’s reports provide detailed case studies, including the specifics of incidents and deficiencies addressed in their administrative

guidance, offering valuable insights for practical countermeasures. Businesses in Japan, especially those handling substantial volumes of personal information, should regularly review these reports. They should also continuously update their technical security measures and implement robust oversight frameworks for contractors.

Practical Measures to be Taken by Companies in the Event of a Data Breach Procedures for reporting leakages and the like

In Japan, upon the occurrence of a leakage, or the like, in respect of personal data it is in principle necessary to report the incident to the authorities. In this regard: (i) for personal data, under the APPI the occurrence must be reported to the PPC (however, in relation to certain industries, the leakage, or the like, must be reported to the competent ministries such as the Ministry of Internal Affairs and Communications (MIC)); and (ii) for information to which the secrecy of telecommunications applies and/or which is specified user information, under the Telecommunications Business Act (TBA) the occurrence must be reported to the MIC. In addition: (iii) in the case of listed companies, timely disclosure under the relevant rules established by each security exchange in Japan and/or disclosure through extraordinary reports under the Financial Instruments and Exchange Act may be required in the event of a major incident. In such cases, careful consideration should be given to the scope of information to be disclosed, in order that the perpetrators of the incident or other persons do not use the information to cause further damage.

As regards (i) and (ii) above, these entail different scopes, procedures and institutional purposes. In the event of a leakage, or the like, it is important to be aware of the difference between (i) and

Contributed by: Yasushi Kudo, Yukiko Konno and Takayuki Inukai,
Nagashima Ohno & Tsunematsu

(ii), and to handle both at the same time and in a timely manner.

- (i) The situations that require reporting under the APPI (Article 26, paragraph 1 of the APPI) are when personal data has been leaked, etc (ie, leakage, loss, damage or other circumstances pertaining to the security of personal data) and there is a significant risk of harm to the rights and interests of individuals. Under the APPI, there are two types of reports: a preliminary report (promptly after learning of the situation); and a definitive report (within 30 days (60 days in certain cases) from the date of learning of the situation).
- (ii) The situations that require reporting under the TBA (Article 28 of the TBA) are: (a) when there is a leakage in respect of secrecy of telecommunications (eg, content of chats); (b) when there is a leakage of specified user information (eg, telecommunications account information) – in which case, only designated businesses are required to report; and (c) when a “threat” of such a situation arises. There are two types of reports under the TBA: a first report (promptly after becoming aware of the situation); and a detailed report (within 30 days).

In addition, as is common for both procedures, it is necessary to comply with the deadlines for submitting each of the above reports, and therefore it would be advisable to establish a response process in advance – ie, in normal times prior to any such incident. In addition, when submitting a report, it is necessary to (i) describe the status of implementation in respect of security control measures and supervision of contractors, and (ii) investigate the technical causes of the leak. With the increase in the number of cases of leakage, there is an inevitable increase in the number of cases necessitating the use of the reporting

procedures, and thus the day when a report is required may come at any time. Therefore, it is important, regarding (i), to establish and conduct the appropriate security control measures and supervisory procedures in advance, and, regarding (ii), to establish relationships with security vendors who have the necessary capabilities to conduct required investigations so that they can be immediately engaged when needed.

Risks in respect of disclosure of administrative guidance and recommendations

In addition, there has been an increase in the number of cases of public disclosure of administrative guidance, order and the like, and therefore de facto risks such as reputational risks, that are not purely legal in nature in recent years.

- In 2023, NTT West discovered that an employee of a re-outsourcer had accessed the server where customer data was stored and had illegally appropriated customer data for about ten years. In response, in 2024, the PPC issued recommendations and administrative guidance to the outsourcer and the re-outsourcer, directing them to improve the inadequate organisational security control measures. In addition, the MIC issued administrative guidance to NTT West, directing it to review its supervision of its outsourced companies and strengthen its measures. The content of said guidance, including the name of the company, has been made public.
- In 2023, an incident occurred involving NTT DOCOMO and NTT NEXIA, whereby temporary employees of NTT NEXIA, NTT DOCOMO's outsourcer for customer information management, appropriated personal data of a total of approximately 5.96 million people. In response, in 2024, the PPC issued administrative guidance to NTT DOCOMO and NTT

Contributed by: Yasushi Kudo, Yukiko Konno and Takayuki Inukai,
Nagashima Ohno & Tsunematsu

NEXIA, directing them to implement measures to prevent a recurrence and to report on the implementation status. The content of this guidance, including the names of the companies, was made public.

In both cases, the incidents occurred at the outsourcee, and the authorities identified issues related to the maintenance of organisational security control measures. It is becoming increasingly difficult for large companies that outsource parts of their business handling personal information to third parties to manage the personal information on their own, and thus it is important to ensure that security control measures are implemented, including at outsourcees.

As mentioned above, in recent years there have been an increasing number of cases of administrative guidance and public announcements in response to leaks. Businesses that handle large volumes of personal data are likely to be more vulnerable to attacks and to risks of leakage and therefore must employ caution because of the increased risk of administrative guidance, administrative order and public disclosure.

Civil risks

In 2014, a very well-known Japanese company (the “Company”) in educational and publishing industry suffered a massive leak (the “Case”), in which an insider (a former employee of the outsourcee) appropriated the personal information of tens of millions of people and sold the information to a directory company. Over the past few years, a series of court judgments have been issued to determine civil liability in the Case.

Corporate responsibility

In the Case, numerous victims filed lawsuits for damages. The court stated that “regarding information security, necessary measures must

be taken in consideration of each company’s business, environment, risks, and suchlike” and noted that “a large amount of personal information from customers forms the subject of business activities, and in light of the general public perception of information management, close attention is to be paid to information security measures.” As a result, the court concluded that “the Company is in a position to pay close attention to information security measures, in light of the fact that it handles a large amount of personal information from its customers in its business activities and in light of the general public perception of information management”, and partially granted the plaintiffs’ (victims’) damages claims against the Company (Tokyo High Court, 17 March 2021, (Ne) No 102).

From this, it can be concluded that businesses handling large volumes of personal data have a heightened duty of care in terms of the security measures required to prevent information leaks of personal data. Therefore, such businesses are susceptible to the risk that a finding of either default (contract liability) based on a breach of the obligation to implement security controls or negligence based on foreseeability (tort liability) may be easily made. In particular, since foreseeability is more likely to be established in relation to known security risks, it is of paramount importance for companies to constantly collect the latest information and take technical countermeasures.

Liability of company officers

If the company were to post an extraordinary loss due to payment of a large amount of compensation for damages or loss in respect of operating profit, the officers could be accused by shareholders and others of violating their duty of care (Article 330 of the Companies Act and Article 644 of the Civil Code) due to the inad-

Contributed by: Yasushi Kudo, Yukiko Konno and Takayuki Inukai,
Nagashima Ohno & Tsunematsu

equacy of their establishment and operation of a cybersecurity system.

In the Case, a shareholder derivative suit was filed against the officers (more precisely, the officers of the Company group's holding company) to hold them liable. In its judgment, the court held that it was necessary to establish an internal control system based on the nature and scale of the business, management conditions, and other related circumstances (Hiroshima High Court, Okayama Branch, 18 October 2019 (2018 (Ne) No 201)). Therefore, in the case of a large corporation, it is necessary to establish an appropriate internal control system from the perspective of cybersecurity, taking into account the trends in practice. In the Case, the responsibility of the officers of the holding company was in question, not the Company itself, since it was the holding company that had established the relevant internal control system. In conclusion, the court dismissed the claim against the officers of the holding company.

Additionally, in a case where the issue was whether or not there were deficiencies in the risk management system of a listed company due to the false statements made in the securities report required under the Financial Instruments and Exchange Act, as a result of fictitious sales being recorded by employees, the Japanese Supreme Court made its judgment based on (i) whether the company had a management system sufficient to prevent the type of misconduct that could normally be expected, and (ii) whether there were special circumstances that should have led the company to anticipate the misconduct that occurred (Supreme Court, 9 July 2009 (2008 (Ju) No 1602)).

If the responsibility of company officers for the inadequacy of risk management systems for

cyber-attacks is contested in court, this Supreme Court judgment may be cited as a precedent. In such cases, security incidents and tactics employed by attackers, as introduced in public alerts by relevant authorities like the PPC, such as the PPC's quarterly report and in publicised cases by other companies, would be taken into account. As a result, it should be noted that the court may assess whether a degree of control was exercised that could have prevented security incidents that occurred, assuming that the incidents were caused by normal, expected cyber-attacks.

Necessity of ensuring adequate security levels

As discussed above, the legal risks associated with cybersecurity are increasing, and so is the need to ensure an adequate level of cybersecurity. For example, the following are beneficial in ensuring adequate standards.

- Considering, from the viewpoint of system maintenance, the necessary cybersecurity measures from the perspective of maintenance of internal controls, with reference to the technical management described in the "Guidelines for Internal Fraud Prevention in Organizations" of the Information-technology Promotion Agency, Japan (IPA) and the evaluation items set forth in "Evaluation of the effectiveness of maintenance and operation status of internal controls using IT" listed in the "Standards for evaluation and audit of internal controls over financial reports" of the Financial Services Agency.
- Conducting cyber due diligence, including penetration tests (actual simulated attacks) and systemic checks, with a view to reducing risks before they occur.
- Participating in the Cyber Security Council (a council legally established under Article 17 of

Contributed by: Yasushi Kudo, Yukiko Konno and Takayuki Inukai,
Nagashima Ohno & Tsunematsu

the Cyber Security Basic Act, in which both the public and private sector participate) to obtain non-public information on the latest attack trends, and such like, from the viewpoint of information gathering.

Trends in Legal Reforms and in Other Areas *Discussion on the review of the APPI*

When the APPI was amended in 2020, it was decided that the regulatory regime would thenceforth be reviewed every three years. Based on this, the PPC is currently reviewing the regime, including the introduction of a surcharge system and revision of the system for demanding injunctions; and on 25 December 2024, the report of the Expert Panel was published (albeit in the form of both sides of the argument).

The report examines, with respect to both (i) violations of various conduct regulations and (ii) violations of regulations pertaining to leaks, and the like, as well as security control measures, narrowing down the cases to which the surcharge system applies.

Specifically, with respect to the situation in which the surcharge system is to be applied, the report proposes the following.

With respect to (i) above:

- limiting the subject acts (situations) to violations of the following four types: restrictions on provision to third parties (Article 27, Paragraph 1); prohibition of inappropriate use (Article 19); restrictions based on the purpose of use (Article 18); and appropriate acquisition (Article 20);
- limiting the subject cases to those where the violator can be said to have failed to have been negligent in respect of taking reasonable care to prevent the violation;

- limiting the subject cases to those where individual rights and interests have been infringed or there is a concrete threat of infringement; and
- limiting the subject cases to those where a large-scale breach has occurred (specifically, where the number of data subjects involved in the breach is 1,000 or more), etc.

With respect to (ii), above:

- limiting the subject acts to cases where a large-scale leakage, or the like of personal data and the like occurs as a result of a breach of the obligation to take security control measures (specifically, cases where the number of data subjects involved in the breach is 1,000 or more);
- limiting the subject cases to those where the violator can be said to have been extremely negligent in respect of taking reasonable care to prevent violations of the obligation to take security control measures; and
- limiting the subject cases to those where individual rights and interests have been infringed or there is a concrete threat of infringement.

With respect to the method of calculation of the surcharge, the report proposes the following.

With respect to (i) above:

- the surcharge be the full amount of financial gain (or an amount exceeding the full amount of such financial gain) obtained by the violating business operator from the violation or from the use of personal information acquired through the violation.

With respect to (ii), above:

Contributed by: Yasushi Kudo, Yukiko Konno and Takayuki Inukai,
Nagashima Ohno & Tsunematsu

- the surcharge be such amount as is obtained by multiplying (x) the amount of sales generated by the business activities of the business operator in violation of the obligation to take security control measures during the period of the relevant violation by (y) a certain “calculation rate” – this proposal is based on the viewpoint of speediness and efficiency of administrative penalties, and it is believed that the proposal considers the ease of calculation.

In addition, there are proposals to establish a provision for reducing penalties for violators who voluntarily report violations, and an additional provision to impose a surcharge of 1.5 times the normal surcharge on repeat violators.

From the viewpoint of civil law, with regard to the system for demanding an injunction, there is a proposal to grant qualified consumer organisations the right to demand an injunction under the APPI as their own right, targeting violations that are highly likely to infringe on the rights and interests of individuals.

Although the report of the expert panel is still in the process of being put forward for consideration, if these systems are introduced, both the administrative law and civil law risks from an enforcement perspective may increase in Japan in the future.

Trends in legal reforms in the national security sector

In 2024, the Act on the Protection and Use of Critical Economic Security Information came into effect. This Law stipulates:

- the designation of critical economic security information;

- the provision of critical economic security information; and
- restrictions on who can handle critical economic security information (so-called “security clearance”), among other matters.

It is important for businesses that handle critical infrastructure, such as information and communications, to comply with this Law.

In addition, recently the government has been preparing Active Cyber Defense legislation, and the bill was submitted to the Diet in February 2025. This bill aims to enhance Japan’s cybersecurity response capabilities to a level equal to or higher than that of major Western countries. Among other things, it stipulates provisions for:

- strengthening public-private sector co-operation, such as imposing reporting requirements on critical infrastructure operators when they notice certain types of cyber-attacks;
- the government’s use of communication information to understand the actual situation of cyber-attacks on Japan; and
- allowing the National Police Agency and the Self-Defense Forces to intrude into and neutralise servers possessed by attackers to prevent serious harm from cyber-attacks under certain conditions.

It will be necessary to keep a close eye on the deliberations on the bill in the Diet.

MEXICO



Law and Practice

Contributed by:

Alejandro Mendiola Diaz and Gunter Schwandt
Nader Hayaux & Goebel

Contents

1. General Overview of Laws and Regulators p.185

- 1.1 Cybersecurity Regulation Strategy p.185
- 1.2 Cybersecurity Laws p.186
- 1.3 Cybersecurity Regulators p.187

2. Critical Infrastructure Cybersecurity p.189

- 2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.189
- 2.2 Critical Infrastructure Cybersecurity Requirements p.189
- 2.3 Incident Response and Notification Obligations p.189
- 2.4 State Responsibilities and Obligations p.190

3. Financial Sector Operational Resilience Regulation p.190

- 3.1 Scope of Financial Sector Operational Resilience Regulation p.190
- 3.2 ICT Service Provider Contractual Requirements p.191
- 3.3 Key Operational Resilience Obligations p.191
- 3.4 Operational Resilience Enforcement p.192
- 3.5 International Data Transfers p.192
- 3.6 Threat-Led Penetration Testing p.192

4. Cyber-Resilience p.192

- 4.1 Cyber-Resilience Legislation p.192
- 4.2 Key Obligations Under Legislation p.193

5. Security Certification for ICT Products, Services and Processes p.193

- 5.1 Key Cybersecurity Certification Legislation p.193

6. Cybersecurity in Other Regulations p.193

- 6.1 Cybersecurity and Data Protection p.193
- 6.2 Cybersecurity and AI p.195
- 6.3 Cybersecurity in the Healthcare Sector p.196

Nader Hayaux & Goebel is a market leader in M&A, banking and finance, fintech, securities and capital markets, structured finance, antitrust, digital economy, telecommunications, tax, insurance and reinsurance, project finance, real estate, energy and infrastructure, restructuring and insolvency, and government procurement. The firm consists of 20 partners and more than 45 associates and is one of the

largest groups of corporate finance experts in the Mexican market, working together for more than 30 years. The only Mexican law firm with an office in London, Nader Hayaux & Goebel enjoys excellent working relationships with law firms in all major cities internationally, thanks to its strong focus on developing and pursuing business opportunities in Mexico, the UK and other European countries.

Authors



Alejandro Mendiola Diaz is an antitrust specialist at Nader Hayaux & Goebel, with extensive experience advising a range of companies on antitrust and digital economy matters. He is a

member of the United States–Mexico Chamber of Commerce, the American Bar Association and the International Chamber of Commerce, serving as vice-president of the International Chamber of Commerce Competition Committee. Alejandro is fluent in English and earned a LLM in international business law from Queen Mary University of London and a law degree from Universidad Latinoamericana.



Gunter Schwandt is a partner at Nader, Hayaux & Goebel and specialises in capital markets, M&A, fintech, structured finance, secured transactions, and cross-border lending. He is an expert

in highly complex public issuances and securitisations and has developed in-depth expertise in CKDs (development capital certificates) and FIBRAs (the Mexican equivalent of a US REIT), advising sponsors and underwriters alike. Gunter spent a year working at international law firm Mayer Brown LLP in Chicago after receiving an LLM (with honours) from the Northwestern University School of Law and a certificate in business administration from the Kellogg School of Management. He graduated as an attorney (with honours) from the Universidad Iberoamericana.

Nader, Hayaux & Goebel

Paseo de los Tamarindos
400 B
7th Floor
Colonia Bosques de las Lomas
Mexico City
CP 05120
Mexico

Tel: +52 554 170 3000
Fax: +52 552 167 3099
Email: info@nhg.com.mx
Web: www.nhg.com.mx



1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

In Mexico, there is no specific cybersecurity law; however, various legal provisions regulate aspects of cybersecurity indirectly, involving multiple regulatory bodies. By way of example, there are regulations concerning banking, personal data protection, criminal conduct, and telecommunications. These laws help shape the cybersecurity landscape by providing legal frameworks that institutions and businesses must follow to protect digital assets and personal information.

Additionally, several government agencies have issued their own cybersecurity guidelines. By way of example, the Central Bank of Mexico (Banxico), the country's central bank, released its cybersecurity strategy for 2024–27 (*Estrategia de Ciberseguridad del Banco de México 2024–27*), outlining its guiding principles and defining the responsibilities of an internal cybersecurity directorate. This initiative highlights the importance of financial cybersecurity and the

role of regulatory bodies in ensuring a secure banking environment. Moreover, financial institutions are required to adhere to strict cybersecurity protocols to prevent fraud, data breaches, and cyber-attacks that could compromise national financial stability.

In the past, the Mexican government conducted a multi-stakeholder process to develop a national cybersecurity strategy, which was published in 2017. This initiative aimed to promote concrete actions with social, economic and political impacts by establishing key principles and objectives. However, the administration that took office in 2018 did not continue this strategy and it remains to be seen whether the current administration, which began in 2024, will implement a concrete cybersecurity strategy. The absence of a dedicated national strategy has left a regulatory gap, leading businesses and government agencies to develop their own cybersecurity frameworks to mitigate risks.

A notable recent development is the creation of the Digital Transformation and Telecommunications Agency (*Agencia de Transformación Digital*

y *Telecomunicaciones*) in November 2024. This agency was granted the status of a Secretariat of State, giving it significant institutional weight in governmental digital policy. The agency includes a General Directorate of Cybersecurity, responsible for designing and executing cybersecurity strategies for the federal government and developing policies to standardise cybersecurity measures across government entities, among other duties. This new agency is expected to play a critical role in shaping the country's cybersecurity landscape by establishing nationwide policies and ensuring co-ordination among different regulatory bodies. Although the agency has been legally established, its implementation and execution of cybersecurity responsibilities remain to be seen, and its success will depend on its ability to enforce policies and collaborate with industry stakeholders.

There have been several cybersecurity law proposals submitted to Congress for discussion. However, none have been enacted into law, remaining as proposals that could serve as a foundation for future legislative discussions. These proposals generally aim to address cyber-crimes related to financial assets, personal freedoms, IP, the financial system, and information systems, among other things. Given the increasing frequency and sophistication of cybersecurity threats, there is a growing need for a comprehensive cybersecurity law that establishes clear regulations and penalties for cyber-related offences. Legislative progress in this area will be crucial for strengthening Mexico's cybersecurity posture and ensuring that individuals and businesses are adequately protected from cybersecurity threats.

Finally, considering Mexico's current legal framework, personal data protection regulations (DPRs) are the most directly relevant laws

to cybersecurity. The protection of personal data remains a central concern, given that unauthorised access, data breaches, and identity theft continue to pose significant risks. Strengthening data protection regulations and enforcing compliance will be essential in fostering a more secure digital environment and building public trust in cybersecurity measures.

1.2 Cybersecurity Laws

The following legal instruments, albeit not an exhaustive list (see 3.1 **Scope of Financial Sector Operational Resilience Regulation** for additional regulations in the financial sector), contain provisions relevant to cybersecurity in Mexico.

- The Federal Criminal Code (*Código Penal Federal*) and state criminal codes – these establish legal consequences for cyber-related crimes, including fraud, identity theft, illicit interception of communications, and unauthorised access to systems. They also criminalise hacking, data breaches, and cyber-enabled financial crimes.
- The Personal Data Protection Law (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*) – this governs the collection, processing, and storage of personal data, ensuring organisations implement adequate security measures to protect sensitive information. Until 20 December 2024, this law was enforced by the National Institute for Transparency, Access to Information, and Personal Data Protection (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*, or INAI) – see 1.3 **Cybersecurity Regulators** (Data Protection) for details of its replacement.
- The Transparency Law (*Ley Federal de Transparencia y Acceso a la Información Pública*) – this law includes provisions on informa-

tion security in public institutions, ensuring that government entities handle and protect sensitive data responsibly while maintaining accountability in cybersecurity-related incidents.

- The Fintech Law (*Ley para Regular las Instituciones de Tecnología Financiera*) – this law establishes compliance requirements for fintech companies and mandatory measures for secure financial transactions, among other things. Given the rapid growth of digital financial services, this law plays a crucial role in mitigating cyber-risks in the financial sector.
- General Provisions Applicable to Credit Institutions (*Disposiciones de Carácter General Aplicables a las Instituciones de Crédito*) – these impose strict standards on banks, requiring financial institutions to implement risk management frameworks, security controls, and incident response mechanisms to safeguard customer data and financial transactions.
- Circular 8/2019 – issued for participants in the Interbank Electronic Payments System, Mexico's real-time payment system, this regulation enhances cybersecurity by requiring financial entities to adopt encryption, authentication measures, and real-time monitoring to prevent cyberfraud.
- Principles for Strengthening Cybersecurity to Ensure Financial System Stability (*Principios para Reforzar la Seguridad de la Información en el Sistema Financiero*) – this is a set of best practices and regulatory guidelines aimed at reinforcing cybersecurity resilience within the financial sector, ensuring institutions implement risk-based approaches to counter cybersecurity threats.
- Mexican Official Standards (*Normas Oficiales Mexicanas*, or NOMs) – several NOMs provide additional mandatory cybersecurity and

information protection requirements. Notable among them are:

- (a) NOM-151-SCFI-2016 – regulates the conservation of digital data messages, ensuring electronic documents remain authentic, reliable, and unaltered over time, which is essential for cybersecurity, e-commerce, and legal compliance; and
- (b) NOM-004-SSA3-2012 – establishes criteria for the creation, management and conservation of medical records in Mexico, reinforcing data protection and ensuring confidentiality in healthcare services (see **6.3 Cybersecurity in the Healthcare Sector** for further details).

Given the ongoing legal changes, it will be crucial to monitor how these regulations evolve and their impact on Mexico's cybersecurity landscape. The Mexican government's current reforms, including the dissolution of certain regulatory agencies and the creation of new entities, may reshape the enforcement and implementation of cybersecurity policies in the coming years.

1.3 Cybersecurity Regulators

Cybersecurity regulation in Mexico is fragmented across various government agencies, primarily owing to the absence of a comprehensive legal framework and a central authority with broad oversight responsibilities. As a result, multiple entities assume roles in cybersecurity matters, each focusing on distinct areas such as law enforcement, the financial sector, and data protection. The landscape is continually evolving.

Law Enforcement and Cybercrime Investigation

The Attorney General's Office (*Fiscalía General de la República*, or FGR) and local prosecutors' offices play a central role in investigating

cybercrimes. The Federal Criminal Code defines various offences, including unauthorised access to information systems, data breaches, and the illegal disclosure of sensitive information. Cyber-crime investigations often involve co-ordination between various state and federal authorities.

In Mexico City, the Cybercrime Investigation Unit within the local prosecutor's office specialises in investigating digital offences. These include crimes against sexual privacy, such as the unauthorised sharing of intimate content on social media – something that is a growing concern in the digital age.

Financial Sector Cybersecurity Regulation

The National Banking and Securities Commission (*Comisión Nacional Bancaria y de Valores*, or CNBV) is responsible for overseeing incidents within the financial sector. The CNBV ensures that financial institutions mitigate risks that could compromise the confidentiality, integrity or availability of banking systems. It monitors and supervises the response to security breaches, data loss, and other violations of financial security regulations.

Banxico, as the central bank, also plays a critical role in securing the financial sector against cyberthreats. In response to the growing number of cyber-attacks targeting financial systems globally, Banxico works closely with financial institutions, sector regulators, and law enforcement. In 2018, Banxico spearheaded the formation of a Cybersecurity Incident Response Group, which collaborates with the Attorney General's Office and other stakeholders to enhance coordinated responses to major security incidents.

Data Protection

The INAI has historically been the primary authority in charge of ensuring data protection and the

public's right to access information. Given that the protection of personal data is closely tied to cybersecurity, the INAI has played a crucial role in safeguarding digital information. Recent government actions saw the INAI abolished and its functions transferred to the Ministry for Anti-Corruption and Good Governance (*Secretaría Anticorrupción y Buen Gobierno*). This shift has raised concerns about the future of data protection policies and how Mexico will address privacy in the face of evolving cybersecurity threats. The long-term implications of this transition on cybersecurity governance and enforcement remain to be seen.

Cybersecurity in Critical Infrastructure

The National Guard (*Guardia Nacional*) has a specialised cybersecurity unit dedicated to supporting agencies managing critical infrastructure. This unit's responsibilities include:

- identifying and assessing cybersecurity threats;
- managing cybersecurity incidents;
- acting as a national point of contact for cybersecurity threats; and
- conducting digital forensics to assist law enforcement agencies in investigating cyber-crimes.

In addition, the National Guard provides cybersecurity assistance to state authorities, reinforcing the protection of both federal and regional infrastructure. This co-ordination aims to create a unified response to protect national security and critical systems from cyber-attacks.

Other Governmental Involvement

Although the agencies outlined earlier in this section are among the most prominent players in Mexico's cybersecurity regulatory environment, other governmental bodies indirectly contribute

to cybersecurity efforts. By way of example, the Ministry of Infrastructure, Communications and Transportation (*Secretaría de Infraestructura, Comunicaciones y Transporte*, or SICT) has a role in regulating digital infrastructure and overseeing the integrity of communication networks.

As the nation continues its efforts to improve institutional and regulatory frameworks, attention must be paid to how changes in governance and legal reforms will influence the overall cybersecurity landscape. These shifts will likely have a profound impact on Mexico's ability to respond to evolving cybersecurity threats and safeguard its critical infrastructure, financial systems, and personal data.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

As mentioned in **1.1 Cybersecurity Regulation Strategy**, there is no specific cybersecurity law that regulates critical infrastructure in Mexico. However, the National Security Law (*Ley de Seguridad Nacional*) contains provisions related to the importance of protecting critical infrastructure – although it does not define in detail what constitutes such infrastructure.

Additionally, during the previous administration, a National Standardised Protocol for Managing Cybersecurity Incidents (*Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos*) was implemented. Although this protocol is not a legal document, it serves as a reference for establishing the terms and procedures that enable the strengthening of cybersecurity across government entities as well as the private sector. This initiative aims to ensure the continuous,

co-ordinated management of cybersecurity incidents, improving overall resilience and response to emerging threats.

2.2 Critical Infrastructure Cybersecurity Requirements

In Mexico, there are no specific obligations related to cybersecurity for the protection of critical infrastructure. While various regulatory frameworks address cybersecurity issues, there is no detailed legislation that comprehensively regulates the measures that entities managing essential infrastructures – such as energy, telecommunications, and transportation – must adopt. The absence of a clear legal framework for the protection of critical infrastructure against cybersecurity threats leaves those institutions responsible for these key sectors with some flexibility but also creates a regulatory gap that could jeopardise the country's resilience in the face of cyber-incidents.

2.3 Incident Response and Notification Obligations

There are no specific reporting obligations for cybersecurity incidents related to critical infrastructure in Mexico. However, the National Standardised Protocol for Managing Cybersecurity Incidents mentioned in **2.1 Scope of Critical Infrastructure Cybersecurity Regulation** does include a series of recommendations on how high-level, critical and impactful cybersecurity incidents should be reported to the National Guard. By way of example, the protocol outlines mechanisms for incident notification, specifying how incidents should be classified and how government entities should carry out the reporting process. Strengthening this protocol through new regulations that grant it mandatory status could significantly enhance the ability to respond to cybersecurity incidents, offering bet-

ter protection for critical infrastructure sectors in Mexico.

2.4 State Responsibilities and Obligations

As mentioned in **1.3 Cybersecurity Regulators** (Cybersecurity in Critical Infrastructure), there are obligations on the part of the government regarding resilience responsibilities and threat identification, which are contained in protocols or guidelines, such as the protocol mentioned in **2.1 Scope of Critical Infrastructure Cybersecurity Regulation** and **2.3 Incident Response and Notification Obligations**. However, these obligations are not specifically outlined in a particular law. This fragmented approach can make it difficult to implement effective security measures, as authorities and private entities may interpret the guidelines differently or may not be legally required to adopt them uniformly.

To improve the situation, it would be advisable for Mexico to move towards creating laws that establish obligations related to cybersecurity resilience and threat identification in critical infrastructure. This would enable more coherent and co-ordinated management of cyber-risks, ensuring that all parties involved follow a common set of rules that strengthen protection and response to cybersecurity incidents. The implementation of more formal legislation could also improve co-operation between the public and private sectors, enhancing the ability to respond to cybersecurity challenges.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

Operational resilience in Mexico's financial sector is primarily regulated by:

- the CNBV;
- Banxico; and
- the National Commission for the Protection and Defence of Financial Services Users (*Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros*, or CONDUSEF).

Mexico does not have a standalone operational resilience regulation. Nevertheless, financial institutions such as banks, fintechs, insurance companies and other market participants are required to comply with a combination of laws, regulations and supervisory guidelines aimed at ensuring business continuity, cybersecurity and risk management. These regulatory norms and provisions include:

- the General Provisions Applicable to Credit Institutions issued by the CNVB (see **1.2 Cybersecurity Laws**);
- CNBV Guidelines on Cybersecurity and Information Security;
- the Fintech Law (*Ley para Regular las Instituciones de Tecnología Financiera*);
- the Payment Systems Law (*Ley de Sistemas de Pagos*);
- Circular 8/2019 – directed at participants of the Interbank Electronic Payments System and issued by Banxico (see **1.2 Cybersecurity Laws**);
- Principles for Strengthening Cybersecurity to Ensure Financial System Stability – issued by Banxico (see **1.2 Cybersecurity Laws**);

- Coordinating Bases for Information Security (*Bases de Coordinación en Materia de Seguridad de la Información*) – established by the Ministry of Finance (*Secretaría de Hacienda y Crédito Público*, or SHCP), Banxico, the CNBV, the CONDUSEF and other governmental agencies and market participants; and
- the Cybersecurity Strategy of Banxico 2024–27 (see **1.1 Cybersecurity Regulation Strategy**).

Additionally, Mexico is an active participant in several international treaties, agreements, and frameworks that focus on cybersecurity, financial sector resilience, and digital crime prevention. Mexico has not formally ratified the Budapest Convention on Cybercrime, but it has aligned its financial cybersecurity regulations with international standards through frameworks such as the Financial Action Task Force (FATF) (*Grupo de Acción Financiera Internacional*, or GAFI) (of which it is a member), Basel III guidelines on operational risk and cyber-resilience, and G20 initiatives. Furthermore, regional and bilateral cooperation – particularly with the USA, the Organization of American States, and the Pacific Alliance – enhances its financial sector’s operational and cyber resilience.

3.2 ICT Service Provider Contractual Requirements

Information and communications technology (ICT) service providers in Mexico are obligated to meet specific contractual and regulatory requirements when working with financial institutions. Such requirements focus on cybersecurity, data protection, operational resilience, third-party risk management, and the ability to afford regulatory supervision. These requirements are set by Banxico, the CNBV, the Federal Telecommunications Institute (*Instituto Federal de Telecomunicaciones*, or IFT) and the INAI. Please note

that the authority and functions of these two last agencies are in the process of being transferred to other agencies within the federal government as a result of recent constitutional reforms.

ICT service providers working with financial institutions must adhere to outsourcing and cybersecurity regulations issued by Banxico and the CNBV, which include:

- cybersecurity requirements for ICT providers handling banking systems;
- data encryption, access controls and authentication measures;
- service-level agreements;
- audit rights; and
- incident response obligations.

Such providers must also comply with Banxico’s cybersecurity and operational resilience standards and grant Banxico regulatory oversight and audit access.

Under Mexico’s Personal Data Protection Law, ICT contracts must establish data protection obligations, and providers must implement technical and organisational security measures. If an ICT provider processes personal data on behalf of a financial institution, the contract must specify processing purposes and permitted activities, data retention policies, and obligations to notify data breaches.

Mexico is expected to introduce enhanced outsourcing regulations for ICT providers, similar to those set forth in EU’s Digital Operational Resilience Act (DORA).

3.3 Key Operational Resilience Obligations

As pointed out in **3.1 Scope of Financial Sector Operational Resilience Regulation**, Mexico

does not currently have dedicated digital operation resilience regulation such as that of the EU, but it has multiple regulatory frameworks that collectively govern operational resilience, cybersecurity, and incident reporting for financial institutions and ICT providers. The main objectives of such regulation include:

- ensuring business continuity and system availability;
- bolstering cybersecurity and IT risk management;
- mitigating risks related to third-party providers and cloud computing;
- improving crisis management and incident response;
- safeguarding personal data and financial information, while enhancing consumer protection and data security; and
- following international standards.

Additionally, financial institutions and other participants such as ICT service providers, payment processors and cloud providers in Mexico must comply with incident reporting obligations. Such reporting obligations include cybersecurity breaches, operational disruptions, financial fraud, phishing attacks, and third-party ICT failures. Financial institutions must also keep logs and forensic reports for potential regulatory audits.

3.4 Operational Resilience Enforcement

Enforcement of operational resilience obligations by regulators in relation to critical ICT services providers in Mexico is done through supervisory audits, compliance inspections, penalty assessments, and mandatory incident reporting. The primary authorities overseeing enforcement include the CNBV, Banxico and, for certain specific matters related to their mandate, the IFT and the INAI.

3.5 International Data Transfers

Mexico does not impose strict data localisation requirements; however, international data transfers must comply with the provisions of the Personal Data Protection Law, financial sector rules, and trade agreements. These rules apply to financial institutions, ICT providers, and businesses in general that process or store personal or sensitive data outside Mexico. Mexican businesses are obligated to implement contractual safeguards, consent mechanisms and cybersecurity measures to ensure compliance. Note that the United States–Mexico–Canada Agreement (USMCA) contains provisions on cross-border data flows and data localisation.

3.6 Threat-Led Penetration Testing

Mexico does not have a formal threat-led penetration testing (TLPT) regulation; however, financial institutions and ICT providers must conduct penetration tests, cyber-resilience assessments and simulated cyber-attacks (“red teaming”) under Banxico, CNBV and IFT regulations, as part of regulatory compliance. Specifically for fintech platforms and banking infrastructure, as well as financial institutions handling electronic payments, the CNBV and Banxico mandate penetration testing and perform cybersecurity assessments to test resilience against cybersecurity threats.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

Resilience obligations in Mexico are primarily related to financial services. Please refer to 3. **Financial Sector Operational Resilience Regulation.**

4.2 Key Obligations Under Legislation

Resilience obligations in Mexico are primarily related to financial services. Please refer to **3. Financial Sector Operational Resilience Regulation**.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

In Mexico, there is no law that requires companies or individuals to obtain certification in cybersecurity. Although the country has established some regulations related to data protection, particularly through the Personal Data Protection Law, these do not impose mandatory cybersecurity certification for organisations or professionals. Instead, the regulations generally require businesses to implement appropriate technical security measures to protect personal data from risks such as alteration, destruction, or unauthorised access.

Despite the absence of a legal requirement for certification, many companies in Mexico recognise the importance of cybersecurity and voluntarily pursue various certifications to enhance their security posture. These certifications, such as ISO/IEC 27001, are often seen as best practices to demonstrate companies' commitment to safeguarding sensitive information and mitigating cybersecurity threats.

Given the growing complexity and frequency of cyber-attacks, Mexico may eventually adopt more stringent regulations that mandate cybersecurity certifications for companies or professionals operating in certain sectors – particularly those responsible for managing critical infrastructure or sensitive data. Until such regulations

are enacted, voluntary certification remains an essential tool for organisations aiming to mitigate risks and enhance their cybersecurity measures.

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

Mexico's data privacy regulations are closely linked to cybersecurity, primarily owing to the increasingly complex landscape of personal data processing in contemporary society. However, the current legal framework does not explicitly address cybersecurity in a dedicated manner. Instead, it outlines general principles and obligations that require organisations to implement security practices, which implicitly include cybersecurity measures as part of broader data protection strategies.

Security Measures and Obligations Under Mexican DPRs

The Mexican DPRs require data controllers (entities responsible for processing personal data) to adopt technical security measures to safeguard personal data against various threats. These threats include damage, loss, alteration, destruction, and the unauthorised use, access or processing of sensitive information. The regulations specify that these measures should be designed with an understanding of evolving technological developments, reflecting the dynamic nature of cybersecurity challenges.

However, the regulations do not provide clear or specific guidelines on what constitutes “technical security measures” nor do they articulate concrete cybersecurity obligations. The provisions are somewhat vague, leaving room for interpretation, and do not set out explicit requirements or standards for the types of cybersecu-

ity practices that data controllers should adopt. This lack of specificity creates challenges in ensuring comprehensive compliance and uniformity in practices across different sectors and organisations.

Data Breach Notification Requirements

In the event of a data breach, public entities that handle personal data have an obligation to notify affected individuals (data subjects) about the incident. They are also required to inform the INAI, which plays a central role in monitoring compliance with the Mexican DPRs and enforcing regulations. This is a crucial step in ensuring transparency and accountability in cases of data breaches.

Private data controllers, on the other hand, have a more limited obligation. They are only required to notify those data subjects directly affected by the breach, rather than making a broader public notification.

When notifying affected individuals, the data controller must provide detailed information, including:

- a description of the nature of the incident;
- the personal data that was compromised;
- recommendations for the data subjects to protect their interests following the breach;
- an overview of the immediate corrective measures taken upon detecting the breach; and
- information on how individuals can seek further details about the incident.

Despite these requirements, the Mexican DPRs do not offer a detailed, standardised procedure for data breach notification. The absence of clear guidance on the format, timing, and channels for notification can lead to inconsistencies

in how organisations manage and communicate data breaches.

INAI's Role and Best Practices in Data Breach Management

In light of the gaps in the legal framework, the INAI proactively issued recommendations and guidelines to assist organisations in preparing for potential data breaches. These guidelines provide recommendations on how to assess the severity of data incidents, implement appropriate response measures, and manage incidents according to best practices in incident management and data protection.

The INAI's involvement was critical in guiding organisations through the complex process of breach management and ensuring compliance with Mexico's data privacy laws. Although the INAI's recommendations were not legally binding, they helped to establish a more standardised approach to data breach management across sectors.

Differences Between Public and Private Sector Obligations

The Mexican DPRs distinguish between the obligations of public and private sector entities in processing personal data. Public entities face more extensive obligations, including the requirement to report breaches both to affected individuals and the INAI. In contrast, private sector entities have less stringent requirements and are only compelled to notify individuals directly affected by a breach. This differentiation creates a potential imbalance in the level of protection afforded to individuals, depending on whether their data is handled by public or private entities.

Moreover, local legislation may provide additional provisions related to cybersecurity, further complicating the regulatory landscape. Although

the INAI was responsible for compliance with national data privacy regulations, local authorities may also play a role in cybersecurity, particularly when it comes to sector-specific data protection practices.

Need for a More Comprehensive Legal Framework

The absence of an explicit and comprehensive legal framework addressing cybersecurity within the Mexican DPRs suggests a need for future reforms. Given the increasing frequency and sophistication of cybersecurity threats, it is crucial for the legal framework to evolve in tandem with emerging risks. A more detailed and clear articulation of specific cybersecurity obligations would help organisations implement more robust and consistent cybersecurity practices, improving overall data protection and reducing vulnerability to cyber-attacks.

In conclusion, even though Mexico's data privacy regulations provide essential safeguards for personal data protection, they lack clear, specific provisions on cybersecurity obligations. The regulations generally require data controllers to implement security measures but fail to offer detailed guidance on what constitutes adequate cybersecurity. This gap leaves organisations with significant room for interpretation, potentially leading to inconsistent practices.

As Mexico continues to address the challenges posed by an increasingly digital society, the integration of more specific cybersecurity requirements into the data privacy regulations will be crucial. Strengthening these provisions will help mitigate the growing risks associated with cybersecurity threats and improve the country's overall ability to safeguard personal data in an interconnected world.

6.2 Cybersecurity and AI

As of early 2025, Mexico does not have dedicated cybersecurity regulations specifically targeting AI. Despite AI technologies significantly transforming a wide range of sectors, from healthcare to finance, the country's legal framework has not yet fully addressed the unique cybersecurity challenges posed by AI systems. However, AI systems that process personal data must still comply with existing data protection regulations – particularly the Mexican DPRs, which primarily focus on safeguarding personal information. This intersection between data protection and AI represents a crucial but limited area of AI governance and cybersecurity in Mexico.

To address these emerging challenges, Mexico could look to international frameworks and guidelines for AI governance and cybersecurity. By way of example, organisations such as the EU have regulated AI – with the Artificial Intelligence Regulations, which includes provisions on high-risk AI systems, specifically addressing cybersecurity measures. Additionally, global cybersecurity bodies such as the Global Forum on Cyber Expertise (GFCE) are working to develop international norms and best practices for securing AI systems, which is a critical component of their governance.

By aligning with such international efforts, Mexico could adopt best practices and standards in AI cybersecurity, fostering a stronger regulatory environment for emerging technologies. Participation in international forums would also allow Mexico to collaborate with other nations and share knowledge, risks, and solutions related to securing AI systems – thereby ensuring that the field remains competitive while effectively addressing the cybersecurity challenges inherent in AI.

6.3 Cybersecurity in the Healthcare Sector

Data protection legislation comes into play, given that sensitive personal data related to individuals' health is processed. Also, there are additional regulations contained in official standards, which are mandatory. In this case, a Mexican Official Standard called NOM-004-SSA3-2012 establishes the criteria for the creation, management and conservation of medical records in Mexico. As mentioned in **1.2 Cybersecurity Laws**, the primary objective of NOM-004-SSA3-2012 is to ensure the proper documentation, confidentiality and accessibility of medical information while protecting patients' rights and improving health-care quality, as follows.

- Scope and application – NOM-004-SSA3-2012 applies to all healthcare facilities and professionals in public and private sectors. It covers medical records in hospitals, clinics, laboratories, and private practices.
- Medical record content – medical records must include personal patient data, medical history, diagnoses, treatment plans, laboratory tests, and progress notes. Specific documentation is required for hospitalisation, surgeries, emergency care, and specialised treatments.
- Patient rights and confidentiality – medical records are confidential and can only be accessed by authorised personnel or with patient consent, except in cases required by law. Patients have the right to access their records and request corrections.
- Retention and storage – medical records must be kept for at least five years after the last patient interaction. Digital and physical records must follow security and data protection protocols.
- Legal and ethical responsibilities – health-care professionals are responsible for accurate, complete and timely documentation. Institutions must implement internal policies to ensure compliance with NOM-004-SSA3-2012.

PORTUGAL



Law and Practice

Contributed by:

Ricardo Henriques and Diogo Pereira Duarte
Abreu Advogados

Contents

1. General Overview of Laws and Regulators p.199

- 1.1 Cybersecurity Regulation Strategy p.199
- 1.2 Cybersecurity Laws p.199
- 1.3 Cybersecurity Regulators p.200

2. Critical Infrastructure Cybersecurity p.201

- 2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.201
- 2.2 Critical Infrastructure Cybersecurity Requirements p.201
- 2.3 Incident Response and Notification Obligations p.202
- 2.4 State Responsibilities and Obligations p.203

3. Financial Sector Operational Resilience Regulation p.203

- 3.1 Scope of Financial Sector Operational Resilience Regulation p.203
- 3.2 ICT Service Provider Contractual Requirements p.205
- 3.3 Key Operational Resilience Obligations p.205
- 3.4 Operational Resilience Enforcement p.207
- 3.5 International Data Transfers p.207
- 3.6 Threat-Led Penetration Testing p.209

4. Cyber-Resilience p.209

- 4.1 Cyber-Resilience Legislation p.209
- 4.2 Key Obligations Under Legislation p.210

5. Security Certification for ICT Products, Services and Processes p.211

- 5.1 Key Cybersecurity Certification Legislation p.211

6. Cybersecurity in Other Regulations p.211

- 6.1 Cybersecurity and Data Protection p.211
- 6.2 Cybersecurity and AI p.212
- 6.3 Cybersecurity in the Healthcare Sector p.213

Abreu Advogados is a big four independent law firm with over 30 years of experience in the Portuguese market, navigating in tomorrow's sectors and industries. The firm continuously attracts strategic opportunities for its clients in key areas such as finance, corporate and M&A, tax, litigation, and competition, among others. The firm invests in multidisciplinary teams that tackle increasingly complex transactions with cost-effective solutions and anticipate clients' needs with a business-oriented vision. Either

from Portugal or internationally, Abreu is chosen to provide legal advice in international transactions across Portuguese-speaking countries, particularly Angola, Mozambique and Timor-Leste. Abreu Advogados partnered with FBL Advogados in 2007 and with JLA Advogados in 2010 to meet clients' interests in the Angolan, Mozambican and Portuguese markets while benefitting from an international decision-making process when presenting innovative legal solutions to its clients.

Authors



Ricardo Henriques is a member of the board of directors of the Knowledge Institute and partner at Abreu Advogados, whose practice focuses particularly on technology law in Portugal and

international markets. He focuses on software licensing, emerging technologies compliance, e-commerce, GDPR implementation, and IP/IT litigation. He also advises national and international clients from several industries on brand protection, patent strategies, advertising, and data protection. Additionally, he assists clients with compliance matters, including ethics codes, anti-corruption, and anti-money laundering measures. His global network of law firms allows him to support clients in their international expansion and IP protection.



Diogo Pereira Duarte is a partner and co-coordinator of the finance practice area at Abreu Advogados and a Professor of Civil Law and Financial Law at Faculdade de

Direito da Universidade de Lisboa. He is an expert on fintech law, with a deep knowledge of a wide range of areas, including blockchain, smart contracts, artificial intelligence, quantum computing, cryptocurrencies, ICOs, AML/FT compliance, cloud computing, open banking, APIs, payment services, financial products, start-up financing, crowdfunding, and data protection. Diogo Pereira Duarte was selected by Banco de Portugal to join the Market Contact Group on the Digital Euro.

Abreu Advogados

Av. Infante Dom Henrique 26
1149-09
Lisbon
Portugal

Tel: (+351) 217 231 800
Fax: (+351) 217 231 899
Email: lisboa@abreuadvogados.com
Web: abreuadvogados.com/en/



1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

Portugal has demonstrated a strong commitment to enhancing the country's cybersecurity by defining a National Cybersecurity Strategy for 2019 to 2023. This government initiative outlines three strategic objectives to ensure a high national level of cybersecurity: i) maximising digital resilience; ii) promoting innovation in cyberspace; and iii) generating and securing resources. To achieve these objectives, the government has set six priorities:

- cyberspace security structure;
- prevention, education, and awareness;
- protection of cyberspace and infrastructures;
- response to threats and combating cyber-crime;
- research, development, and innovation; and
- national and international co-operation.

The National Cybersecurity Centre (CNCS), as the national cybersecurity authority, has undertaken various actions to implement the Action Plan of the National Cybersecurity Strategy. The CNCS has particularly focused on preventing cyber-risks and raising awareness among citizens and companies.

However, the CNCS highlights in its 2024 Society report that the increasing number and sophistication of cyber-attacks, driven by the growing online presence of Portuguese citizens, reveal a lack of resources in the Portuguese public administration to address these new challenges. Currently, there is no national cybersecurity strategy for the upcoming years, although the CNCS has indicated that an updated strategy will be developed to address the sector's most pressing needs.

On another note, the EU has taken on the role of legislator in cybersecurity matters, delegating the transposition and implementation of these laws to member states, considering their national contexts. Given that cybersecurity is a fundamental challenge for the Union, it is essential for member states to maintain a consistent and robust legal framework. This ensures that countries like Portugal can benefit from shared resources and guidelines, promoting a high level of cybersecurity in the borderless cyberspace.

1.2 Cybersecurity Laws

The primary laws and regulations governing cybersecurity in Portugal are the following:

- Regulation (EU) 2016/679, of 27 April 2016 on the protection of natural persons with regard

to the processing of personal data and on the free movement of such data (the GDPR);

- Regulation (EU) 2019/881, of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act);
- Commission Implementing Regulation (EU) 2024/482, of 31 January 2024;
- Regulation (EU) 2022/2554, of 14 December 2022 (DORA);
- Directive (EU) 2022/2555, of 14 December 2022 (NIS 2 Directive);
- Directive (EU) 2022/2556, of 14 December 2022 (amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector);
- Directive (EU) 2022/2557, of 14 December 2022 (Resilience of Critical Entities);
- Regulation (EU) 2024/2847, of 23 October 2024 (Cyber-Resilience Act);
- Regulation (EU) 2025/38, of 19 December 2024 (Cyber-Solidarity Act);
- Law No 46/2018, of 13 August (The Legal Framework for Cyberspace Security);
- Decree-Law No 65/2021, of 30 July (Regulates the Legal Framework for Cyberspace Security);
- Decree-Law No 3/2012, of 16 January (Approves the organisation of the National Security Office);
- Decree-Law No 20/2022, of 28 January (Approves the procedures for identifying, designating, protecting and increasing the resilience of national and European critical infrastructures);
- CNCS Regulation No 183/2022, of 21 February (Regulation setting out technical instructions on communications between organisa-

tions and the National Cybersecurity Centre); and

- Regulation (EU) 2023/2854, of 13 December (Data Act).

1.3 Cybersecurity Regulators

The CNCS is the national cybersecurity authority, pursuant to the terms of the implementing Law of NIS1 Directive (Law No 46/2018). This authority operates within the framework of the National Security Office, and its mission is to ensure the safe and free use of cyberspace in Portugal.

The CNCS is responsible for developing the national capacity to prevent and detect cybersecurity incidents, both by promoting training and by developing innovation projects in the field of cybersecurity. The CNCS is also responsible for ensuring the security of government information and communication systems and critical national infrastructures.

As the national authority responsible for the security of cyberspace, the CNCS is a national single point of contact for international co-ordination and plays a central role in liaising with other national actors in the field of cybersecurity.

From a regulatory standpoint, this authority has the power to issue cybersecurity regulations and to monitor compliance with the cybersecurity legal framework. In this context, the CNCS has the power to instruct administrative proceedings against offenders and to impose fines.

The CNCS also assumes the role of the National Cybersecurity Certification Authority (ANCC), in accordance with Decree-Law 65/2021, which implements Regulation (EU) 2019/881.

Pursuant to the current cybersecurity legal framework for critical infrastructures (ie, Decree-Law No 20/2022), there are sectoral entities which have the obligation to elaborate a list of potential national and European critical infrastructures.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

The NIS 2 Directive (Directive (EU) 2022/2555) sets out cybersecurity risk management measures and reporting obligations for critical infrastructures regardless of their size, as well as for essential and important entities. This Directive is complemented by the CER Directive (Directive (EU) 2022/2557, of 14 December 2022). Both directives came into effect in 2022 and became applicable from 18 October 2024, the date on which EU member states had to ensure the transpositions into national law. However, Portugal has not yet approved such legislation, thus infringing this requirement.

In this regard, we note that on 6 February, the Council of Ministers approved the draft legislation authorisation law establishing the new Cybersecurity Legal Framework, which transposes the NIS 2 Directive. However, due to the recent political landscape of Portugal, the proposed Draft Law has been dropped.

For the moment, companies that are qualified as critical infrastructures are currently governed by Law No 46/2018, which provides the general cybersecurity legal framework, and Decree-Law No 20/2022, governing the resilience of national critical infrastructures. The concept of “critical infrastructures”, as contemplated in Decree-Law

No 20/2022 and the CER Directive, includes all the facilities or networks that are necessary for the provision of a service deemed crucial for society. Pursuant to this Directive, member states must indicate a list of critical entities that belong to any of the categories established in the Annex (eg, entities operating in the electricity sector).

Therefore, stakeholders are currently waiting for the implementation of the NIS 2 Directive, as this law is currently undergoing a legislative process with no clear end date.

2.2 Critical Infrastructure Cybersecurity Requirements

In accordance with Decree-Law No 20/2022, critical infrastructure is required to enhance its resilience and safeguard the infrastructure that enables the provision of essential services. This must be achieved through collaboration between national and European critical infrastructure. Additionally, the Decree-Law mandates that each national critical infrastructure develop an operator security plan.

Such infrastructure is required to designate security liaison officers, who function as a point of contact for security-related issues between the operator and other critical infrastructure. The designation of the officer must be communicated to the National Security Office, the Secretary-General of the internal security system, and the Portuguese National Authority for Emergency and Civil Protection. Moreover, the infrastructure must also designate a point of contact to establish communication with emergency and civil protection authorities.

Under Law No 46/2018, critical infrastructure operators must implement technical and organisational measures that are proportionate

and appropriate to prevent, detect, and mitigate cybersecurity risks to their networks and information systems. These measures are further detailed in Decree-Law No 65/2021, which also requires that operators of critical infrastructures elaborate risk assessments and an annual report describing the main developed activities in terms of cybersecurity and demonstrating an aggregated assessment of all the incidents with a substantial or relevant impact (see Article 8 of Decree-Law No 65/2021).

Additionally, they are required to fulfil specific notification obligations in the event of a cybersecurity incident.

2.3 Incident Response and Notification Obligations

In the Portuguese legal framework, the notification requirements for critical infrastructure owners and operators are laid down in Law No 46/2018, and regulated in detail in Decree-Law No 65/2021.

When operators have knowledge of a significant incident that substantially impacts the continuity of services, they must proceed with an initial notification. The term to notify the CNCS shall be the moment of knowledge of the incident, or up to two hours after that knowledge. Regardless of the notification obligation, the entity should prioritise the implementation of mitigation measures for the risks.

The following information must be included in the initial notification:

- name, telephone number and email address of a representative of the organisation;
- date and time when the incident began or, if unknown, when it was detected;
- brief description of the incident;

- estimate of the impact, considering:
 - (a) the number of users affected by the service disruption;
 - (b) the duration of the incident; and
 - (c) the geographical distribution, with regard to the area affected by the incident, including an indication of cross-border impact;
- other information deemed relevant.

Additionally, operators should submit a notification to the CNCS communicating the end of the relevant impact of the incident, which shall be done at the moment of knowledge of the incident, or up to two hours after that knowledge.

Information that should be included in the notification communicating the end of the relevant impact of the incident:

- an update, if any, of the information provided in the initial notification;
- a brief description of the measures taken to deal with the incident;
- a description of the impact situation at the time of the loss of relevant or significant impact, namely:
 - (a) the number of users affected by the service interruption;
 - (b) the duration of the incident;
 - (c) the geographical distribution in terms of the area affected by the incident, including an indication of the cross-border impact; and
 - (d) the estimated time for full restoration of services.

Lastly, critical infrastructure must issue a final notification within 30 working days from the moment the incident ceased.

Information that should be included in the final notification:

- the date and time when the incident attained relevant or significant impact;
- the date and time when the incident lost its relevant or significant impact;
- the impact of the incident;
- the indication of the measures taken to mitigate the incident;
- a description of any residual effects remaining at the time of the final notification;
- where applicable, information on the submission of the notification of the incident to the competent authorities (eg, the Public Prosecutor's Office and the National Data Protection Authority); and
- any other information deemed relevant.

2.4 State Responsibilities and Obligations

The mission of the Portuguese state, through the National Security Office and the CNCS, is to ensure that Portuguese citizens benefit from a free, reliable and secure cyberspace. To this end, the state has created entities that are empowered to implement the necessary measures to anticipate, detect, respond to and recover from situations that, due to the threat or occurrence of incidents or cyber-attacks, jeopardise the functioning of critical infrastructure and national interests.

In this regard, the National Computer Security Incident Response Team (CERT.PT) was created. This team is responsible for co-ordinating the response to cybersecurity incidents at the operational level, as well as monitoring incidents with a national impact. For that purpose, it can activate early warning mechanisms to mitigate the impact of incidents.

The Portuguese government is also responsible for approving the National Cyberspace Security Strategy, which defines the state's objectives and actions in this domain. Portugal currently has a National Cyberspace Security Strategy for 2019-2023, and the government has not presented any other plans for the following years.

Additionally, Decree-Law No 20/2022 requires operators of critical national infrastructure to draw up a security plan to be submitted for approval to the Secretary-General of the Internal Security System.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

In Portugal, as an EU country, the DORA Regulation applies (ie, Regulation (EU) 2022/2554, of the European Parliament and the Council, of 14 December, 2022, on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, No 648/2012, (EU) No 600/2014, No 909/2014 and No 2016/1011).

As for its material scope, the DORA Regulation applies to the following entities (Article 2):

- credit institutions;
- payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366;
- account information service providers;
- electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC;
- investment firms;
- crypto-asset service providers as authorised under a Regulation of the European Parlia-

ment and of the Council on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (“the Regulation on markets in crypto-assets”) and issuers of asset-referenced tokens;

- central securities depositories;
- central counterparties;
- trading venues;
- trade repositories;
- managers of alternative investment funds;
- management companies;
- data reporting service providers;
- insurance and reinsurance undertakings;
- insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries;
- institutions for occupational retirement provision;
- credit rating agencies;
- administrators of critical benchmarks;
- crowdfunding service providers;
- securitisation repositories (the aforesaid are jointly referred to as “financial entities”); and
- ICT third-party service providers.

DORA applies to all the above-mentioned entities that provide services in the EU and are located herein.

Additionally, the territorial scope of DORA is broad and extends to organisations based outside the EU, where, for example, they (in the case of financial entities) offer certain financial services in the EU market or (in the case of ICT providers) contract with financial entities that are in scope of DORA.

At the national level, the implementation of all obligations arising from DORA remains ongoing. The competent authorities (Bank of Portugal (BdP), Portuguese Securities Market Com-

mission (CMVM) and Portuguese Insurance and Pension Funds Supervisory Authority (ASF)) are in the process of drafting the regulations that will implement the framework. At this stage, developments have been observed in the following areas:

Regarding risk management associated with information and communication technologies, a significant development is the revision of Bank of Portugal Instruction No 4/2021, which governs the management and reporting of operational and security risks by payment service providers. This revision will eliminate the annual reporting requirement for operational and security risks to prevent redundancy with EBA/GL/2019/04, which may itself be subject to amendment by the European Banking Authority (EBA).

For incident reporting and cyber threats, a transitional arrangement requires severe ICT incidents and voluntary cyber threat notifications to be sent to dorareport@bportugal.pt until a final reporting mechanism is established.

The CMVM, in response to the implementation of DORA in Portugal, has outlined its plans through the Annual Circular on Financial Intermediation and Crowdfunding Services, with the national regulation of DORA set as one of its key objectives for 2025.

In the insurance sector, implementation has been carried out through Regulatory Standard No 9/2024-R, which governs the reporting of severe incidents related to information and communication technologies to the ASF and Regulatory Standard No 7/2024-R, regarding the security and governance of information and communication technologies, and subcontracting to cloud computing service providers within the management of pension funds.

3.2 ICT Service Provider Contractual Requirements

ICT services are defined as digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which include the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services (Article 3(20) of DORA).

An ICT service provider is defined as an undertaking providing ICT services (Article 3(19) of DORA).

The DORA Regulation also defines what is considered a critical ICT third-party service provider, namely entities designated as such in line with Article 31 of the Regulation, which considers a series of criteria laid out in said article, such as the systemic impact on stability, continuity or quality of the service or the systemic character or importance of the financial entities that rely on the relevant ICT third-party service provider.

DORA also requires a register of ICT service agreements, reinforcing oversight of third-party dependencies. At the national level, while this overlaps with Bank of Portugal Notice No 8/2023, which governs outsourcing agreements, the annual submission of outsourcing records will continue. Adjustments may follow once the EBA Guidelines on Outsourcing (EBA/GL/2019/02) are revised by late 2025.

For the entities subject to CMVM supervision, the regulation of reporting obligations under DORA is currently underway, in alignment with the content and formats defined by European legislation. Until the required files can be submitted via the Electronic One-Stop Shop (BUE),

as part of the ongoing regulatory development, an alternative submission method is via email to cmvm@cmvm.pt.

3.3 Key Operational Resilience Obligations

The main objective of the DORA Regulation is to achieve a high common level of digital operational resilience (Article 1(1)).

For that purpose, the Regulation lays down uniform requirements concerning the security of network and information systems supporting the business process of financial entities, which are as follows:

- requirements applicable to financial entities in relation to:
 - (a) information and communication technology (ICT) risk management;
 - (b) reporting of major ICT-related incidents and notifying, on a voluntary basis, significant cyber threats to the competent authorities;
 - (c) reporting of major operational or security payment-related incidents to the competent authorities by financial entities;
 - (d) digital operational resilience testing;
 - (e) information and intelligence sharing in relation to cyber threats and vulnerabilities; and
 - (f) measures for the sound management of ICT third-party risk;
- requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities;
- rules for the establishment and conduct of the oversight framework for critical ICT third-party service providers when providing services to financial entities; and
- rules on co-operation among competent authorities, and rules on supervision and

enforcement by competent authorities in relation to all matters covered by this Regulation.

Some of the main obligations under the DORA Regulation for financial entities are as follows:

- implementing an ICT risk management framework, which shall include at least strategies, policies, procedures, ICT protocols and tools necessary to duly and adequately protect all information and ICT assets;
- using and maintaining updated ICT systems, protocols and tools that are appropriate to the magnitude of operations;
- continuously monitoring and controlling the security and functioning of ICT systems and tools;
- having mechanisms in place to promptly detect anomalous activities, including ICT network performance issues and ICT-related incidents, and identifying potential material single points of failure;
- establishing a comprehensive ICT business continuity policy; and
- developing and maintaining back-up policies and procedures and restoration and recovery procedures and methods, for the purpose of ensuring the restoration of ICT systems and data with minimum downtime and limited disruption and loss.

Given that Portugal is still in the implementation phase, there are currently few specific rules governing the obligations related to operational resilience.

The ASF Regulatory Standard No 9/2024-R establishes the information elements, format and deadlines for reporting severe incidents related to ICT, under the information reporting obligation incumbent upon entities supervised

by the ASF, in accordance with their supervisory responsibilities.

The ASF Regulatory Standard No 7/2024-R sets the following requirements and general principles concerning the security and governance of ICT, as well as specific requirements regarding subcontracting to cloud computing service providers within the management of pension funds:

- the definition of general governance requirements for ICT, including the responsibilities of the management body in this area, the obligation for pension fund management companies to have an ICT strategy, the integration of ICT and security-related risks into the company's overall risk management system, and the conduct of periodic audits;
- the establishment of requirements related to information security, notably that pension fund management companies must have an information security policy and an information security function;
- the regulation of duties that pension fund management companies must comply with concerning the operational management of ICT;
- the provision of requirements applicable to business continuity management within the scope of ICT;
- the definition of general governance requirements for the subcontracting of cloud computing services; and
- the establishment of requirements prior to entering into a cloud computing service subcontracting agreement, and the regulation of the rights and obligations that must be clearly identified and specified in the written agreement.

It should be noted that insurance companies managing pension funds are already subject to

the requirements applicable to the insurance activity under Regulatory Standard No 6/2022-R. However, Regulatory Standard No 7/2024-R further supplements the implementation of provisions related to subcontracting to cloud computing service providers in relation to the pension fund management activities of these companies.

3.4 Operational Resilience Enforcement

DORA mandates the identification and designation of critical ICT third-party service providers (CTPPs) based on a set of qualitative and quantitative criteria, including the number of financial institutions they serve, the potential systemic impact, continuity of quality of the provision of financial services in the event of a large-scale operational failure and the degree of substitutability of the ICTT (Article 31(2)).

Once designated as a CTPP, an ICT provider falls under the direct oversight of a Lead Overseer (see Article 33).

The Lead Overseer is vested with broad oversight powers (Article 35 (1)), including:

- requiring all relevant information and documentation related to ICT risk management frameworks;
- conducting general investigations and inspections;
- issuing recommendations to enhance operational resilience measures; and
- imposing corrective measures in cases of non-compliance, ensuring financial stability and service continuity.

Regulatory enforcement under DORA incorporates a graduated and proportionate approach, balancing oversight with proportionate interventions.

Nevertheless, the Lead Overseer, before issuing recommendations or imposing a periodic penalty payment, shall give the representatives of the ICTT the opportunity to be heard (Article 35 (3) (11)).

Key enforcement actions include:

- a periodic penalty payment to compel the ICT third-party service to comply with those measures; this penalty is imposed on a daily basis until compliance is achieved (and for no more than a period of six months), which amounts to 1% of the average daily worldwide turnover of the ICTT in the preceding business year; and
- possible service restrictions, including potential prohibitions on providing ICT services to financial entities if resilience obligations are not met.

We are still awaiting the national implementing law for DORA, which may provide further details on sanctioning powers.

At present, the authorities with sectoral competence in supervising and enforcing digital operational resilience requirements are as follows:

- Bank of Portugal for credit institutions;
- Portuguese Securities Market Commission (CMVM) for investment firms, market operators, and crowdfunding service providers; and
- Portuguese Insurance and Pension Funds Supervisory Authority (ASF) for insurance companies.

3.5 International Data Transfers

DORA requires financial institutions to ensure that third-party ICT service providers meet specific requirements in their contractual relationships. These include incorporating certain con-

tractual provisions (Article 30) and assessing whether conditions for supervisory oversight, such as those related to subcontracting, are satisfied (Article 28(4)(b)).

When the service provider is based in a third country (ie, outside the European Union) and is classified as critical, the institution must also ensure compliance with EU data protection rules and verify the effective enforcement of such laws in that country (Article 29(2)).

In this regard, international data transfers between financial institutions and ICT service providers will likely involve the processing of both personal and non-personal data.

On the one hand, financial institutions must ensure that the international transfer of personal data directed to data importers (eg, ICT service providers) located in a third country provides appropriate safeguards to data subjects (ie, banking clients), as outlined in Chapter V of the GDPR.

In particular, financial institutions may transfer personal data to a third country covered by an adequacy decision, which ensures that such a country or region provides an adequate level of protection for data subjects. Currently, the Commission has issued several adequacy decisions, including for Canada, Israel and Japan.

If the third country is not subject to an adequacy decision by the Commission, financial institutions, as data controllers and data exporters, must implement appropriate safeguards, which may take the form of:

- binding corporate rules;
- standard data protection clauses adopted by the Commission;

- standard data protection clauses adopted by a supervisory authority with the approval of the Commission;
- an approved code of conduct, complemented by binding commitments of the controller or processor in the third country; or
- an approved certification mechanism, complemented by binding commitments of the controller or processor in the third country.

The GDPR provides additional exceptions that may legitimise international data transfer in the absence of an adequacy decision or the implementation of appropriate safeguards. In the context of financial institutions as data controllers, the explicit and informed consent of data subjects may be an appropriate legal basis for the transfer. Other exceptions may be relevant for this purpose, such as the exercise or defence of legal claims (Article 49 GDPR).

Non-personal data, on the other hand, is not covered by the GDPR and is therefore not subject to any specific restrictions on international data transfers. Nevertheless, Article 32 of the Data Act (Regulation (EU) 2023/2854) provides that customers of cloud service providers who store their non-personal data in the EU are entitled to protection against international and third-country governmental access and transfer of data. Providers of data processing services must therefore take appropriate measures to prevent such unlawful access and transfer.

Ultimately, financial institutions are required to ensure that the contractual provisions established with third-party ICT service providers located in a third country meet both the requirements of DORA and the appropriate safeguards described in the GDPR.

3.6 Threat-Led Penetration Testing

Financial entities (with some exceptions) under the DORA Regulation shall carry out, at least every three years, advanced testing by means of threat-led penetration testing (TLPT). This TLPT shall cover several or all critical or important functions of a financial entity, and shall be performed on live production systems supporting such functions.

At the end of the testing, after reports and remediation plans have been agreed, the financial entity and, where applicable, the external testers, shall provide to the competent authority a summary of the relevant findings, the remediation plans and the documentation demonstrating that the TLPT has been conducted in accordance with the requirements.

Financial entities must contract testers for the purposes of undertaking TLPT in line with the DORA Regulation. Whenever financial entities use internal testers for the purpose of undertaking the TLPT, they shall contract external testers every three tests.

Financial entities shall only use testers for the carrying out of the TLPT that:

- are of the highest suitability and reputability;
- possess technical and organisational capabilities and demonstrate specific expertise in threat intelligence, penetration testing and red team testing;
- are certified by an accreditation body in a member state or adhere to formal codes of conduct or ethical frameworks;
- provide an independent assurance, or an audit report, in relation to the sound management of risks associated with the carrying out of TLPT, including the due protection of the financial entity's confidential information and

redress for the business risks of the financial entity; and

- are duly and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence.

When using internal testers, financial entities shall ensure that, in addition to the above-mentioned requirements, (i) such use has been approved by the relevant competent authority designated in line with applicable law; (ii) the relevant competent authority has verified that the financial entity has sufficient dedicated resources and ensured conflicts of interest are avoided throughout the design and execution phases of the test; and (iii) the threat intelligence provider is external to the financial entity.

At the national level, the TIBER-PT framework for resilience testing will be updated in line with TIBER-EU, expected by mid-2025. The Bank of Portugal will continue to use this framework to certify digital resilience testing under DORA.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

In October 2024, the EU introduced the Cyber Resilience Act, a regulation that harmonises security requirements for products with digital elements, ensuring a consistently high level of cybersecurity.

This Regulation is directly applicable in Portugal and requires the adoption of national implementing legislation only for specific provisions that empower the national legislature (eg, provisions on penalties).

Due to its limited material scope, other legislations, such as Regulation (EU) 2023/988 on

general product safety requirements, apply to products with digital elements that pose safety risks not covered by the Cyber Resilience Act. Additionally, this regulation does not affect the health and safety requirements established in Regulation (EU) 2023/1230, when applicable.

As a result, since the first provisions of the Cyber Resilience Act will only be applicable in September 2026 (see Article 71), Portugal currently relies on the general cybersecurity legal framework indicated in **1.2 Cybersecurity Laws** and detailed in **2 Critical Infrastructure Cybersecurity**. Furthermore, there is not yet a proposal of a draft law for the implementation of the Regulation.

4.2 Key Obligations Under Legislation

The Cyber Resilience Act provides a robust level of cybersecurity for products with digital elements to be placed on the internal market.

At the outset, it is essential to clarify that the Regulation identifies three categories of products with digital elements:

- products with digital elements not classified as important or critical;
- important products with digital elements, which possess the core functionality of a product category outlined in Annex III, further subclassified into Class I and Class II; and
- critical products with digital elements, which possess the core functionality of a product category outlined in Annex IV.

Although the level of compliance varies, products with digital elements that are subject to this Regulation must comply with the key obligations outlined below.

Presentation of the CE Marking

It shall be mandatory for products with digital elements covered by this Regulation to bear the CE marking as the visible proof for users of conformity with the essential cybersecurity requirements set out in Annex I. Prior to applying the CE marking, a conformity assessment procedure, harmonised by the Regulation, must be conducted.

Conformity Assessments Procedure

The conformity assessment of products with digital elements, which are not listed as important or critical products with digital elements in this Regulation, can be carried out by the manufacturers themselves, according to the procedure laid down in Decision No 768/2008/EC.

However, due to the high impact of products with digital elements classified as “important”, they are subject to different procedures:

- For Important Class I Products: Manufacturers can assess these products themselves, provided that they adhere to harmonised standards, common specifications or comply with a European cybersecurity certification. If the manufacturer chooses not to apply the above security measures, it must undergo a third-party conformity assessment.
- For Important Class II Products: The conformity assessment must always involve a third party.

For critical products with digital elements, and in accordance with their importance for society, it is mandatory that they have a certification under the European Cybersecurity Certification Scheme with a minimum level of “substantial”. If this condition is not met, critical products are subject to the conformity assessment defined for Class II important products.

Assessment of the Cybersecurity Risks

Manufacturers of products with digital elements must carry out and document an assessment of the cybersecurity risks of the product, and demonstrate that it complies with the essential cybersecurity requirements listed in Annex I. This assessment shall be integrated into the technical documentation of the product.

Reporting Obligations

The Regulation mandates that manufacturers of products with digital elements must report to both the designated Computer Security Incident Response Team (CSIRT) and ENISA, via a single platform to be established by the latter authority. The reporting comprises a notification on (i) actively exploited vulnerabilities in their products and (ii) serious incidents impacting the security of these products.

The law also sets out different obligations for the different actors in the supply chain (ie, manufacturers, importers and distributors) to ensure that the essential requirements for cybersecurity are met from the manufacturing stage onwards. This aligns with the primary aim of the Cyber Resilience Act, which is to establish essential cybersecurity requirements for the design, development, and manufacture of products with digital elements, as well as their monitoring once they are available on the market.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

The Cybersecurity Act (Regulation (EU) 2019/881) establishes the “European cybersecurity certification framework” and provides a harmonised standard for cybersecurity certification across

the EU. The European Commission has adopted an implementing act for the voluntary European Common Criteria-based cybersecurity certification scheme (EUCC) (Commission Implementing Regulation (EU) 2024/482, of 31 January 2024).

Portugal has designated the CNCS as the National Cybersecurity Certification Authority (ANCC), responsible for implementing a national cybersecurity certification framework. In this context, the CNCS has developed the EC QNRCS certification, based on European schemes.

The EC QNRCS certification scheme has been designed for central and local administration organisations, operators of critical infrastructure, essential and important service providers, digital service providers, and other private and non-governmental organisations, whether for profit or not. The CNCS manages and supervises this national certification scheme in co-operation with the Portuguese Quality Institute (IPQ) and the Portuguese Accreditation Institute (IPAC).

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

The cornerstone of data protection in the EU, and consequently in Portugal, is the General Data Protection Regulation (Regulation (EU) 2016/679 – GDPR).

One of the main principles of the GDPR is the integrity and confidentiality principle, established in Article 5(1)(f), which provides that personal data “shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate

technical or organizational measures (“integrity and confidentiality”).

This principle is materialised by Article 32 (security of processing) and Articles 33 and 34, which relate to notification and communication obligations in the event of a personal data breach.

In light of this legal framework, Controllers and Processors are required to adopt “appropriate” technical and organisational measures to ensure a level of security that is appropriate to the potential risks. The adjective “appropriate” allows for a risk-based approach regarding the controls that should be implemented, taking into account the state of the art. For this purpose, the Article lists some controls that represent the professional consensus on security controls for processing, such as encryption and pseudonimisation. When assessing the adequacy of the technical and operational measures to be implemented, the Controller or Processor concerned may take into consideration the cost of implementation, the risks associated with the processing activities and their severity for the rights and freedoms of data subjects.

However, it is mandatory that Controllers and Processors have in place adequate mechanisms for detecting personal data breaches, which corresponds to a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed (see Article 4(12)).

When the Controller becomes aware of such a breach, it must consider the obligation to notify the supervisory authority without undue delay where there is a foreseeable risk to the rights and freedoms of natural persons. If the Controller or the supervisory authority subsequently

concludes that there is a high risk to the rights of data subjects, it is obliged to communicate the personal data breach to the data subjects without undue delay and in accordance with the provisions of Article 34.

The national law implementing the GDPR (Law No 58/2019) does not provide any further specifications regarding the security of processing. Nevertheless, it is worth noting that the Portuguese data protection authority (*Comissão Nacional de Proteção de Dados*, or CNPD) has issued guidelines (Diretriz/2023/1, CNPD, available in Portuguese [here](#)) proposing indicative security measures to be implemented by data Controllers. In terms of organisational measures, the CNPD suggests that Controllers and Processors consider implementing analysis procedures for monitoring network flows and carrying out periodic IT security audits and vulnerability assessments. With regard to technical measures, the CNPD suggests, inter alia, increasing the robustness of servers.

Given the synergies between cybersecurity and the protection of personal data, the CNCS acts in collaboration with the CNPD whenever a cybersecurity incident involves a breach of personal data.

6.2 Cybersecurity and AI

As artificial intelligence systems are composed of digital components, they are particularly vulnerable to cyber-attacks and cybersecurity incidents. These incidents can impact not only the AI system’s performance but also its end users. For instance, a cybersecurity breach affecting the algorithm or training data of a credit scoring AI system could have severe consequences for users seeking to obtain credit.

Therefore, the Artificial Intelligence Regulation (Regulation (EU) 2024/1689) emphasises the necessity for high-risk AI systems to maintain a high level of accuracy, robustness, and cybersecurity (see Article 15). AI systems with a high risk for individuals' rights and freedoms must be resistant to unauthorised access and equipped with adequate measures for detecting, preventing, and responding to cybersecurity incidents.

For this purpose, providers of high-risk AI systems can seek cybersecurity certification under Regulation (EU) 2019/881. In such a case, Article 43 of the AI Regulation established a presumption of compliance with the cybersecurity requirements outlined in Article 15. Additionally, the cybersecurity measures implemented by the provider must be included in the technical documentation accompanying the system.

When the AI Regulation was approved, there was not yet a final agreement from European legislative bodies on the Cyber Resilience Act. Nonetheless, the AI Regulation's recitals mention the co-ordination between the two laws. Recitals 77 onwards of the AI Regulation are mirrored in Recital 51 and Article 12 of the Cyber Resilience Act, which presumes compliance with Article 15 of the AI Regulation when the high-risk AI system meets the essential cybersecurity requirements in Annex I of the Cyber Resilience Regulation.

Furthermore, the procedure for assessing compliance with the essential cybersecurity requirements for a product with digital elements that is simultaneously classified as a high-risk AI system will follow the provisions of Article 43 of Regulation (EU) 2024/1689. However, in the event that the application of this provision would lead to a reduction in the level of security required for critical or important products with

digital elements, the conformity assessment procedure provided for in the Cyber Resilience Regulation with regard to the essential cybersecurity requirements should apply by way of derogation from this rule.

6.3 Cybersecurity in the Healthcare Sector

Entities operating in the healthcare sector are considered essential, especially if they fall under and meet the requirements of the NIS 2 Directive, making them subject to the cybersecurity framework for essential entities.

Their value and impact on basic societal functions make them prime targets for cyber-attacks, often aimed at compromising health data and the safety of individuals.

As such, Regulations (EU) 745/2017 and 746/2017 on medical devices and in vitro diagnostic medical devices have introduced cybersecurity concerns. These regulations ensure that devices placed on the EU market are equipped to address new technological challenges related to cybersecurity risks.

The Medical Devices Regulation (MDR) requires medical devices with electronic programmable systems and software to meet minimum cybersecurity requirements. This includes devices such as pacemakers and insulin pumps. Consequently, these requirements cover hardware, IT network characteristics and IT security measures, including protection against unauthorised access, to ensure that the software works as intended.

According to the guidance on cybersecurity for medical devices (MDCG 2019-16 Rev.1, December 2019, available [here](#)), manufacturers must implement state-of-the-art cybersecurity meas-

ures. This guidance is intended to help manufacturers comply with the essential cybersecurity requirements outlined in Annex I of the MDR and the In Vitro Diagnostic Medical Devices Regulation.

The MDR does not define “IT security”, so the Medical Device Coordination Group document refers to the definition provided by ENISA. “IT security” is thus defined as the protection against threats to the technical infrastructure of a cyber system that could change its characteristics to perform unintended activities (Definition of Cybersecurity – Gaps and overlaps in standardisation, December 2015, available [here](#)). The same applies to the definitions of operational security and information security.

In Portugal, Decree-Law No 29/2024 ensures the national implementation of the MDR and provides that healthcare entities deploying a medical device must report to the competent authority (ie, INFARMED, I.P) all security measures implemented and their performance.

Also at the national level, Order No 8877/2017 establishes the governance model to be followed by the Shared Services of the Ministry of Health (*Serviços Partilhados do Ministério da Saúde, E. P. E.*, or SPMS), in conjunction with the National Security Office and the CNCS. The same Order requires all health entities of the national health service to adopt a cybersecurity policy and a contingency plan for cybersecurity incidents.

Overall, the health sector is covered by the general legal framework for cybersecurity as discussed in this chapter.

Trends and Developments

Contributed by:

Ricardo Henriques, Diogo Pereira Duarte, José Maria Alves Pereira and Leonor de Sá e Frade
Abreu Advogados

Abreu Advogados is a big four independent law firm with over 30 years of experience in the Portuguese market, navigating in tomorrow's sectors and industries. The firm continuously attracts strategic opportunities for its clients in key areas such as finance, corporate and M&A, tax, litigation, and competition, among others. The firm invests in multidisciplinary teams that tackle increasingly complex transactions with cost-effective solutions and anticipate clients' needs with a business-oriented vision. Either

from Portugal or internationally, Abreu is chosen to provide legal advice in international transactions across Portuguese-speaking countries, particularly Angola, Mozambique and Timor-Leste. Abreu Advogados partnered with FBL Advogados in 2007 and with JLA Advogados in 2010 to meet clients' interests in the Angolan, Mozambican and Portuguese markets while benefitting from an international decision-making process when presenting innovative legal solutions to its clients.

Authors



Ricardo Henriques is a member of the board of directors of the Knowledge Institute and partner at Abreu Advogados, whose practice focuses particularly on technology law in Portugal and

international markets. He focuses on software licensing, emerging technologies compliance, e-commerce, GDPR implementation, and IP/IT litigation. He also advises national and international clients from several industries on brand protection, patent strategies, advertising, and data protection. Additionally, he assists clients with compliance matters, including ethics codes, anti-corruption, and anti-money laundering measures. His global network of law firms allows him to support clients in their international expansion and IP protection.

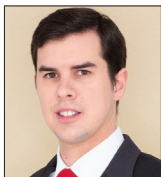


Diogo Pereira Duarte is a partner and co-coordinator of the finance practice area at Abreu Advogados and a Professor of civil law and financial law at Faculdade de

Direito da Universidade de Lisboa. He is an expert on fintech law, with a deep knowledge on a wide range of areas, including blockchain, smart contracts, artificial intelligence, quantum computing, cryptocurrencies, ICOs, AML/FT compliance, cloud computing, open banking, APIs, payment services, financial products, startup financing, crowdfunding, and data protection. Diogo Pereira Duarte was selected by Banco de Portugal to join the Market Contact Group on the Digital Euro.

PORTUGAL TRENDS AND DEVELOPMENTS

Contributed by: Ricardo Henriques, Diogo Pereira Duarte, José Maria Alves Pereira and Leonor de Sá e Frade, Abreu Advogados



José Maria Alves Pereira is a senior associate at Abreu Advogados, whose practice focuses particularly on technology law in Portugal and international markets. He

focuses on compliance, e-commerce, telecommunications, GDPR implementation, and cybersecurity matters.



Leonor de Sá e Frade is a trainee lawyer at Abreu Advogados, whose practice has been focused particularly on technology law.

Abreu Advogados

Av. Infante Dom Henrique 26
1149-096
Lisbon
Portugal

Tel: (+351) 217 231 800
Fax: (+351) 217 231 899
Email: lisboa@abreuadvogados.com
Web: abreuadvogados.com/en/

Abreu:
advogados

Contributed by: Ricardo Henriques, Diogo Pereira Duarte, José Maria Alves Pereira and Leonor de Sá e Frade, Abreu Advogados

Eyes Wide Open: The Portuguese Cybersecurity Agency Dives Deeper into Market Practices

Introduction: NIS 2 transposition

The growing importance of cybersecurity for businesses is undeniable. Consequentially, EU institutions revisited the NIS Directive (Directive (EU) 2016/1148) in 2022 and issued a new regulation – known as NIS 2 Directive (Directive (EU) 2022/2555) – the transposition of which is expected to both extend and develop already applicable cybersecurity regulations in Portugal, complementing, in particular, Regulation (EU) 2022/2554 (known as the Digital Operational Resilience Act or DORA Regulation), which requires specific cybersecurity measures to be adopted by banking and financial institutions.

While the deadline for EU member states to transpose the NIS 2 Directive into national law was 17 October 2024, Portugal is still in the process of doing so. Following a public consultation on the draft legislation, which ran from late November to late December 2024 and garnered over 140 contributions, we are faced with a setback in the legislative process. The Draft Law has fallen along with the Portuguese Government.

Although the process of transposition is still ongoing, and despite the period between publication and implementation, we have already noticed market actors' interest in the Directive, and its transposition process. We have received multiple requests to assess the subjective scope of the new NIS 2 Directive – ie, whether a certain company is, or is not, subject to those new norms – and several requests to keep our clients posted regarding the process of elaboration and approval of the NIS 2 transposition law.

This concern is perfectly understandable. Among the specific features of the previously proposed Portuguese transposition (such as a clearer definition of the functions and competences of the Cybersecurity Officer, affording greater certainty to market actors, or the qualification of the temporary banning of administrators as an ancillary sanction only) the most recent version of the transposition statute, provided for fines of up to EUR200,000 for individual members of management bodies.

Given the upcoming transposition of Directive (EU) 2022/2555 (Directive NIS 2) in Portugal – and especially of the personal and individual liability for administrators for the breach of cybersecurity regulations as outlined above – market actors in those sectors should be keen on ensuring compliance. Compliance with cybersecurity requires great investment on the part of undertakings – both financially and in terms of human resources. This includes purchasing and implementing antivirus software, setting up multi-factor authentication, developing plans, policies and procedures, and allocating additional resources, such as time, to adhere to these policies. Not to mention the costs associated with staff training, software updates, and the increasing marginal costs as the volume of protected information grows.

However, the potential penalties can be even more costly. In addition to fines of up to EUR200,000 for individual administrators specific to the Portuguese jurisdiction, the NIS 2 Directive already provides for fines as high as EUR10 million for breaching companies and entities.

The oversight by the CNCS

The Portuguese National Cybersecurity Agency (*Centro Nacional de Cibersegurança*, or CNCS) is the agency responsible for the oversight and

Contributed by: Ricardo Henriques, Diogo Pereira Duarte, José Maria Alves Pereira and Leonor de Sá e Frade, Abreu Advogados

enforcement of cybersecurity legislation in Portugal (including the future NIS 2 Directive transposition statute).

Up to now, the CNCS has largely adopted a proactive, supportive approach. Their core principle revolves around educating and mitigating the risks of breaches and damage by fostering a strong culture of compliance with legal requirements. This is evidenced by the relatively infrequent use of sanctions for breaches of cybersecurity statutes. The CNCS has been notably active, but their focus has primarily been on organising talks, conferences and newsletters, and developing best practice codes and standards to cultivate a culture of legal compliance within the Portuguese market.

Very recently, in fact, the CNCS published a series of reports on market cybersecurity conditions and practices. While these reports do not represent legal enforcement actions in themselves, their creation signifies preparatory steps towards such actions. And the publication of these reports – containing a framework of analyses, a comparative baseline, international standards and recommendations – may inspire other jurisdictions to also pay closer attention to market practices.

Within these reports, the CNCS identified significant disparities in cybersecurity practices and the level of protection afforded to information stored in digital systems across various sectors, despite the widespread use of digital tools. We have compiled some of the data from these reports below to enable a comparison between sectors, with the aim of gleaning insights and recommendations.

Market state and sector practices

- Regarding policies for staff training, and cybersecurity managers, despite the obligations provided in the NIS 2 Directive, Law No 46/2018, of 13 August, and Decree-Law No 65/2021 of 30 July:
 - (a) Digital infrastructure providers have the worst results of all the sectors analysed by CNCS. 33% have untrained cybersecurity managers, and 74% of companies in the Portuguese digital infrastructure sector have less than 25% of staff trained to even a basic level. 58% of companies do not even offer training in cybersecurity.
 - (b) 20% of companies in the Portuguese energy sector, in turn, have untrained cybersecurity managers, and nearly half (45%) have less than 25% of staff trained to even a basic level. 33% of companies do not even offer training in cybersecurity, despite the legal mandate, and, of those that do, half offer it on an optional basis.
 - (c) Similarly, in the transport sector, 19% of companies in the Portuguese transport sector have untrained cybersecurity managers, and over half (57%) have less than 50% of staff trained to even a basic level.
 - (d) Healthcare providers report better scores. 36% have untrained cybersecurity managers, and 60% of companies in the Portuguese healthcare sector have less than 50% of staff trained to even a basic level.
 - (e) Banking and financial institutions are overall the best prepared. All claim to have duly trained cybersecurity managers, despite 25% of companies in the Portuguese banking admitting to having less than 50% of staff trained to even a basic level.
- Regarding cybersecurity documentation, in particular, regarding the preparation and implementation of cybersecurity plans, inci-

Contributed by: Ricardo Henriques, Diogo Pereira Duarte, José Maria Alves Pereira and Leonor de Sá e Frade, Abreu Advogados

dent response plans and report obligations – all of which, again, were already mandated under Law No 46/2018 and Decree-Law No 657/2021, and are further detailed in the NIS 2 Directive and its transposition statute, the situation is quite similar:

- (a) As for providers of digital infrastructure, there is a clear disconnect between the acknowledged importance of data security and actual practice. 54% concede they lack both a cybersecurity plan and an incident response plan. Furthermore, 4% failed to submit their mandatory annual reports to the CNCS in 2023.
 - (b) In the energy sector, 33% admit to not having a cybersecurity plan implemented at all, 20% admit to not having an incident response plan, and 10% have not submitted their mandatory annual reports to CNCS in 2023.
 - (c) In the transport sector, the figures are 35%, 48% and 12%, respectively.
 - (d) Among healthcare providers, 54% admit to not having a cybersecurity plan, 38% admit to not having an incident response plan, and 13% have not submitted their mandatory annual reports to CNCS in 2023 – despite the sensitivity of the data they manage on a daily basis.
 - (e) And, lastly, again, the banking and financial institutions sector shows greater compliance, with only 13% admitting to not having a cybersecurity plan implemented at all.
- Finally, regarding statutorily required good cybersecurity practices, the numbers are telling:
 - (a) Only 23% of healthcare providers regularly conduct risk analysis assessments, as compared to 36% of the providers of digital infrastructure, 50% in the energy and transport sector, and, again, being

the best prepared sectors overall, 75% of companies in banking and financial institutions.

- (b) Regarding the maintenance of logs for post-incident reconstruction and analyses, 50% of companies in the Portuguese transport and healthcare sector do not keep logs for this purpose; neither do 48% of companies in the digital infrastructure sector; 30% in the energy sector; and, lastly, 23% among financial institutions.
- (c) Regarding the undertaking of vulnerability checks and vulnerability management policies, only 20% of companies in the digital infrastructure sector undertake them regularly, compared to 70% of companies in the energy and transport sectors. Notably, the banking and financial institutions sector reports complete adherence, with all companies claiming to conduct these checks.

The implications of the aforementioned statistics become increasingly concerning when considered alongside the pervasive reliance on digital tools and devices within these sectors:

- 56% of companies in the Portuguese energy sector report that between 75% and 100% of their workforce utilise digital devices and tools for their daily tasks. Conversely, only 10% of these companies indicate that less than 25% of their staff engage in such usage.
- In the banking and financial market institutions sectors, 100% of companies report that virtually all their employees access and manage digital devices and tools to perform their work.
- Lastly, in the Portuguese digital infrastructure sector, 58% of companies state that over 50% of their staff utilise digital devices and

Contributed by: Ricardo Henriques, Diogo Pereira Duarte, José Maria Alves Pereira and Leonor de Sá e Frade, Abreu Advogados

tools, compared to only 14% of companies in the Portuguese healthcare sector.

The combination of less than 25% of staff receiving basic cybersecurity training, the lack of dedicated cybersecurity officers, the absence of log records, and the deficiency of cybersecurity plans highlights the urgent need for companies to reflect on and adapt to new regulations. This is particularly critical when, for a significant majority (well over 50%) of these companies, at least 50% of their staff rely on digital devices and tools for their daily work.

While the banking and financial institutions sector demonstrates better compliance compared to others, it is important to acknowledge that this sector is subject to specific, stringent cybersecurity regulations, such as the DORA regulation. This explains their significantly higher compliance levels. However, it also underscores that they operate under stricter norms and standards. Therefore, their relative success should not lead to complacency among their administrators.

The data concerning energy, digital infrastructure and healthcare is particularly concerning: all three are designated as essential services, critical to the maintenance of a modern workable society – and yet all three show significant deficiencies in their cybersecurity actions and policies.

Recommendations

Having now comprehensively examined technological specificities and threats, capacity building, identifiable investment in cybersecurity, applicable standards and good practices, and market shortcomings, the CNCS is now far better positioned to determine the legal compliance status of providers and other market participants. This enhanced insight allows them to hold

both these entities and, crucially, their administrators personally accountable for breaches of cybersecurity norms.

The data presented above unequivocally demonstrates that staff training must be a priority for providers across all sectors subject to cybersecurity requirements, including public administration entities, postal services, and food production and distribution, not just the previously mentioned sectors. These training programmes should encompass both basic cybersecurity practices – such as strong password adoption, the avoidance of sharing personal or sensitive information online, and screen locking – and more advanced topics like incident response protocols and reporting obligations. A robust enterprise cybersecurity strategy must focus on both incident prevention and effective response to safeguard digital infrastructure and sensitive data.

Equally important is the implementation of legally mandated good practices. Regular risk assessments, vulnerability checks, and the maintenance of comprehensive log-in and log-out records are essential for demonstrating clear compliance. Crucially, the production of thorough documentation proving adherence to cybersecurity requirements is paramount. Companies and cybersecurity managers are accountable for maintaining legally required documentation. The absence of such documentation constitutes a breach in itself and will lead to the presumption that the underlying obligation, which should have been evidenced by the documentation, has also been unmet.

Beyond these reports, which, again, are more akin to an enforcement tool than to an act of enforcement, the CNCS, in collaboration with ANACOM (the Portuguese National Authority

Contributed by: Ricardo Henriques, Diogo Pereira Duarte, José Maria Alves Pereira and Leonor de Sá e Frade, Abreu Advogados

for Telecommunications), has been developing statutorily mandated enforcement tools, such as the ANACOM-CSIRT (“computer security incident response team”). This suggests a shift towards a more reactive and less pedagogical stance as the competent supervisory authority.

In conclusion, the CNCS has got its eyes wide open. To avoid falling under its scrutiny, companies, particularly those that have not yet begun preparations for implementing the acts and procedures required by Directive NIS 2, should urgently analyse the new proposals to ascertain the extent to which organisational adaptations are necessary.

SINGAPORE

Law and Practice

Contributed by:

Lim Chong Kin, David N Alfred, Albert Pichlmaier and Goh Boon Yeow
Drew & Napier LLC



Contents

1. General Overview of Laws and Regulators p.225

- 1.1 Cybersecurity Regulation Strategy p.225
- 1.2 Cybersecurity Laws p.226
- 1.3 Cybersecurity Regulators p.228

2. Critical Infrastructure Cybersecurity p.230

- 2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.230
- 2.2 Critical Infrastructure Cybersecurity Requirements p.230
- 2.3 Incident Response and Notification Obligations p.232
- 2.4 State Responsibilities and Obligations p.232

3. Financial Sector Operational Resilience Regulation p.232

- 3.1 Scope of Financial Sector Operational Resilience Regulation p.232
- 3.2 ICT Service Provider Contractual Requirements p.233
- 3.3 Key Operational Resilience Obligations p.234
- 3.4 Operational Resilience Enforcement p.234
- 3.5 International Data Transfers p.236
- 3.6 Threat-Led Penetration Testing p.237

4. Cyber-Resilience p.239

- 4.1 Cyber-Resilience Legislation p.239
- 4.2 Key Obligations Under Legislation p.239

5. Security Certification for ICT Products, Services and Processes p.239

- 5.1 Key Cybersecurity Certification Legislation p.239

6. Cybersecurity in Other Regulations p.240

- 6.1 Cybersecurity and Data Protection p.240
- 6.2 Cybersecurity and AI p.241
- 6.3 Cybersecurity in the Healthcare Sector p.242

Drew & Napier LLC established a dedicated Data Protection, Privacy and Cybersecurity Practice to leverage its unrivalled experience in data privacy and data and cyber governance and offer clients best-in-class solutions to address their legal and compliance needs in Singapore and across the region. The firm represents many regional companies, multinationals, industry associations, government bodies and regulators, and regularly assists them on a wide range of matters in Singapore and ASEAN member countries. At the forefront of

data protection law in Singapore since 2013, the Data Protection, Privacy and Cybersecurity Practice Group has worked on significant data protection enforcement cases and appeals, including those involving cybersecurity elements. Building on its experience in this field, the Drew Data Protection and Cybersecurity Academy was established in 2020 to offer clients services relating to data protection and cybersecurity compliance, including training, consulting and external Data Protection Officer services.

Authors



Lim Chong Kin is the managing director of Drew & Napier's Corporate and Finance department, heads the Telecommunications, Media and Technology Practice and

co-heads the Data Protection, Privacy and Cybersecurity Practice. With his strong background in competition, data protection and technology laws, Chong Kin offers clients expert commercial advice. He has been an external legal and regulatory adviser for the Personal Data Protection Commission of Singapore since it was established in 2013. He also played a key role advising Singapore's Infocom regulator, the Info-communications Media Development Authority. Chong Kin is highly regarded by his peers, clients and rivals for his expertise, and is consistently recommended as a leading lawyer by major international legal publications.



David N Alfred is a director of Drew & Napier LLC and co-head of the firm's Data Protection, Privacy and Cybersecurity Practice Group. He is concurrently co-head and

programme director of the Drew Data Protection and Cybersecurity Academy. David is a data protection, cybersecurity and technology lawyer with over 25 years' experience advising on a broad range of matters relating to digital technology, telecommunications and the internet. He has substantial experience advising on data protection and cybersecurity compliance, regulatory enforcement, data breaches and international aspects of data protection. Prior to joining the firm, David was the first Chief Counsel of Singapore's data protection authority, the Personal Data Protection Commission.



Albert Pichlmaier is a senior cybersecurity and privacy engineer with Drew & Napier LLC and concurrently a senior learning technology designer of the Drew Data Protection and

Cybersecurity Academy. Albert is an IT professional with over 30 years of international experience in the private and public sectors. He has worked in a wide range of IT and security domains, from smart card firmware development and test automation to AI and blockchain development, as well as IT security product certifications. Albert holds a degree in computer science and CISSP and CDPSE certifications. Prior to joining the firm, Albert worked for over ten years in the public sector in Singapore, most recently for Singapore's data protection authority.



Goh Boon Yeow is an associate director of Drew & Napier's corporate and finance department. Boon Yeow's main areas of practice are technology, media and telecommunications

(TMT), broadcasting, cybersecurity, data protection and privacy, and employment law. He regularly advises leading global and local telecommunications and broadcasting companies on corporate, commercial, licensing and regulatory issues. Prior to joining Drew & Napier, Boon Yeow served in the public service as a legal counsel on an overseas scholarship, where he advised on a broad range of contentious and non-contentious issues.

Drew & Napier LLC

10 Collyer Quay
10th Floor
Ocean Financial Centre
Singapore 049315

Tel: +65 6531 4110
Fax: +65 6535 4864
Email: chongkin.lim@drewnapier.com
Web: www.drewnapier.com



1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

The first iteration of the Singapore Cybersecurity Strategy was published by the Cyber Security Agency of Singapore (CSA). It outlined measures to build resilient infrastructure, and create a safer cyberspace for Singapore, among other objectives. The strategy was revised in 2021 to take a more proactive stance to addressing the evolving cyber threat landscape. The Singapore Cybersecurity Strategy 2021 extends the previous strategy by recognising the emergence of disruptive technologies like edge computing and quantum technologies, alongside increasingly sophisticated threat actors exploiting pervasive connectivity.

Developed in consultation with multiple stakeholders, including industry, and local and overseas academia, the 2021 strategy aims to proactively defend Singapore's cyberspace, simplify cybersecurity for users, and advance international cybersecurity norms. The 2021 strategy also emphasises the importance of a strong cybersecurity workforce and ecosystem as key enablers of Singapore's cybersecurity. Key components of the 2021 strategy include the following.

Three Strategic Pillars

- Building resilient infrastructure: beyond expanding the CSA's regulatory remit under the Cybersecurity Act 2018, the CSA also encourages enterprises and organisations to adopt a risk management mindset (as opposed to a compliance mindset) and invest in their digital infrastructure.
- Enabling a safer cyberspace: the government will take the lead in securing digital infrastructure and support the development of a

healthy digital environment. In particular, the government will make it easier for everyone to secure their devices and use secure applications.

- Enhancing international cyber co-operation: the government will advance the development and implementation of voluntary, non-binding norms, which sit alongside international law. The government will also advocate the development and adoption of technical and interoperable standards and step up operational co-operation with international partners.

Two Foundational Enablers

- Developing a vibrant cybersecurity ecosystem: the government will galvanise the cybersecurity industry and academia to develop advanced capabilities, build world-class products and services, and grow Singapore's cybersecurity market.
- Growing a robust cyber talent pipeline: the government will work closely with schools to educate students in cybersecurity and nurture budding cybersecurity enthusiasts and partner with industry and institutes of higher learning to develop skills and competency frameworks for cybersecurity professionals.

The Singapore Cybersecurity Strategy 2021 underscores Singapore's commitment to a multi-faceted approach to cybersecurity, recognising the shared responsibility of all stakeholders in safeguarding the nation's digital interests.

In terms of cybersecurity regulation, the dedicated cybersecurity law, the Cybersecurity Act 2018 (see further details at **1.2 Cybersecurity Laws**), had three objectives when it was first promulgated:

- first, to strengthen the protection of Singapore's critical information infrastructure (CII) against cyber-attacks;
- secondly, to authorise the CSA to lead in the prevention and response to cybersecurity threats and incidents;
- thirdly, to establish a licensing framework to regulate cybersecurity service providers.

In 2024, the government saw the need to update the Act to keep pace with changes in technology, business models and the cyber threat landscape. In so doing, the amendments will allow CSA to extend their regulatory oversight to important systems and entities not previously covered under the Cybersecurity Act 2018, adopting a risk-based approach to regulating entities for cybersecurity.

1.2 Cybersecurity Laws

Cybersecurity in Singapore is broadly regulated by a set of overlapping pieces of legislation which address the issues of national cybersecurity, cybercrimes, and personal data protection and management. In addition, certain sectoral regulators are empowered to directly address cybersecurity issues in their respective sectors through the issuance of regulatory codes, guidelines, notices and instruments.

Cybersecurity Act 2018 (Cybersecurity Act)

The Cybersecurity Act is the dedicated cybersecurity law which sets out the overarching framework for the oversight of national cybersecurity issues in Singapore, including the designation of computer systems as CII in essential sectors and co-ordinating the national response to cybersecurity incidents, amongst other things.

The Cybersecurity Act requires owners of CII to notify the Commissioner of Cybersecurity in the event of the occurrence of certain cybersecurity

incidents related to their CII. In this regard, a cybersecurity incident refers to an act or activity carried out without lawful authority on or through a computer or computer system that jeopardises or adversely affects its cybersecurity or the cybersecurity of another computer or computer system.

Since 2022, the Cybersecurity Act provides for the licensing of certain cybersecurity service providers (CSPs). At present, this includes CSPs that provide penetration-testing and managed security operations centre monitoring services.

To keep up with the evolving cybersecurity threats and nature of businesses, the Cybersecurity (Amendment) Bill was passed in Singapore Parliament on 7 May 2024 to expand the CSA's oversight to new entities beyond CII owners. The four new categories (please see 2.2 **Critical Infrastructure Cybersecurity Requirements** for further details) of entities are:

- essential service providers who use CII owned by a third party;
- major foundational digital infrastructure (FDI) service providers;
- entities of special cybersecurity interest; and
- owners of systems of temporary cybersecurity concern.

Importantly, the amendments have extended the definition of CII to include any computer or computer system, whether they are physical or virtual, located wholly or partly in Singapore which may be designated as CII. Such designation may arise if the Commissioner is satisfied that the computer or computer systems are necessary for the continuous delivery of an essential service, and the loss or compromise of such systems will have a debilitating effect on the availability of the essential service in Singapore. At

the time of writing, the amendments have yet to come into force.

Computer Misuse Act 1993 (CMA)

The CMA sets out the enforcement and penalty framework against perpetrators of cyber-related offences, such as the unauthorised access to and modification of computer material, unauthorised use or interception of a computer service, unauthorised obstruction of use of a computer and unauthorised disclosure of a password or access code. The CMA empowers the police and other government authorities to investigate and prosecute perpetrators of cybercrimes.

Personal Data Protection Act 2012 (PDPA)

The PDPA applies to all private sector organisations that collect, use, disclose or otherwise process personal data (both electronic and non-electronic data). Personal data is defined as data about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access.

As part of complying with the PDPA, organisations are required to make reasonable security arrangements (which may include technical and cybersecurity measures) to protect personal data in their possession or under their control to prevent (i) unauthorised access, collection, use, disclosure, copying, modification, disposal, or similar risks; or (ii) the loss of any storage device or medium on which personal data is stored.

The PDPA also includes notification requirements in the event of a data breach, that is (i) the occurrence of unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or (ii) loss of any storage device or medium on which personal data is stored where unauthorised access, col-

lection, use, disclosure, copying, modification or disposal of personal data is likely to occur.

The Do Not Call (DNC) provisions under the PDPA regulate the sending of certain marketing messages to Singapore telephone numbers. These provisions are intended to give individuals more control over the type of marketing messages they may receive by allowing individuals to register their telephone numbers with the DNC Registry and imposing obligations on organisations in respect of sending marketing messages. This thereby reduces the number of unsolicited messages received by individuals and the risk of being exposed to cybersecurity attacks.

The DNC provisions impose restrictions on whether an organisation may send specified messages (as defined in Section 37 of the PDPA) to a Singapore telephone number. Organisations must check that the Singapore telephone number it intends to send a specified message to is not registered with the DNC Registry before sending the specified message, unless the user or subscriber of the Singapore telephone number has given clear and unambiguous consent in evidential form. Further, Section 48B prohibits organisations from sending any message to a recipient's telephone number where that telephone number was obtained by a dictionary attack or through address-harvesting software. Section 48A of the PDPA defines dictionary attack as the method by which the telephone number of a recipient is obtained using an automated means that generates possible telephone numbers by combining numbers into numerous permutations. On the other hand, address-harvesting software refers to software that is designed for searching the internet for telephone numbers and harvesting those numbers. Thus, although the DNC provisions primarily target marketing messages, they serve a secondary

role of reducing the ways in which malicious actors may conduct cyber-attacks.

Spam Control Act 2007 (SCA)

The SCA provides for the control of spam and for matters connected with spam in Singapore. The SCA generally regulates the sending of electronic messages with a Singapore link and contains specific obligations relating to senders of unsolicited commercial electronic messages in bulk. Such obligations include the use of the label “<ADV>” to mark unsolicited commercial electronic messages and to offer an unsubscribe option to recipients. The SCA also prohibits the sending of an electronic message to an electronic address obtained through the use of a dictionary attack or address-harvesting software. The SCA is a civil penalty regime where non-compliance with these requirements may result in civil actions against the spammer.

Public Sector (Governance) Act 2018 (PSGA)

Aside from the confidentiality and secrecy provisions found across various legislation, data protection and management in the public sector is also governed under the PSGA. The PSGA, which aims to strengthen public sector data governance, imposes criminal penalties on public officers who recklessly or intentionally disclose data without authorisation, misuse data for a gain or re-identify anonymised data. Specific data security policies are further set out in the Government Instruction Manual on IT Management.

Other Sectoral Frameworks

Two notable examples are in the telecommunications and banking and finance sectors.

First, in the area of telecommunications, the telecoms and media regulator, the Info-communications Media Development Authority (IMDA),

has published a Telecommunications Cybersecurity Code of Practice to enhance cybersecurity preparedness of designated telecommunication licensees such as internet service providers in Singapore. This Telecommunications Cybersecurity Code of Practice, which was formulated in line with international standards and best practices including the ISO/IEC 27011 and IETF Best Current Practices, sets out requirements on security incident management and other controls to help licensees prevent, protect, detect and respond to cybersecurity threats.

Secondly, the Singapore financial regulatory authority, the Monetary Authority of Singapore (MAS), has issued its Technology Risk Management (TRM) Guidelines (the “TRM Guidelines”), which set out risk management principles and best practices to guide financial institutions (FIs) in establishing sound and robust technology risk governance and oversight, as well as in maintaining IT and cyber-resilience. In conjunction with this, the MAS has also issued legally binding Notices on TRM and Cyber Hygiene which give effect to some of the requirements in the TRM Guidelines. Please also see 3.1 Scope of Financial Sector Operation Resilience Regulation for further details.

1.3 Cybersecurity Regulators

Cyber Security Agency of Singapore

The regulatory authority responsible for the administration and enforcement of the Cybersecurity Act is the CSA. The CSA is part of the Prime Minister’s Office and is managed by the Ministry of Digital Development and Information (MDDI), and led by the Commissioner of Cybersecurity. The Minister for Digital Development and Information (as the Minister-in-charge of Smart Nation and Cybersecurity) may appoint Assistant Commissioners from sectoral regulators who understand the unique context and

complexity of their respective sectors to advise and assist the Commissioner on the co-ordination of cybersecurity efforts.

Under the Cybersecurity Act, the Commissioner's functions and duties include, but are not limited to:

- advising the Singapore government or any other public authority on cybersecurity matters;
- monitoring and responding to cybersecurity threats, whether such cybersecurity threats occur in or outside Singapore;
- identifying and designating computer systems as CII in essential sectors, and regulating owners of CII;
- establishing cybersecurity codes of practice and standards of performance for implementation by owners of CII;
- developing and promoting the cybersecurity services industry in Singapore; and
- licensing and establishing standards in relation to CSPs.

In general, the Cybersecurity Act (as it currently stands) applies to any computer or computer system located wholly or partly in Singapore which may be designated as CII. When the upcoming amendments to the Cybersecurity Act take effect, such CII can also involve any computer or computer system, whether they be physical or virtual. The Commissioner may confer such a designation when they are satisfied that the computer or computer systems are necessary for the continuous delivery of an essential service, and the loss or compromise of such systems will have a debilitating effect on the availability of the essential service in Singapore.

The Cybersecurity Services Regulation Office was set up within the CSA in 2022 to administer the licensing framework of CSPs under the Cybersecurity Act, responding to the industry's queries and feedback, and sharing of resources on licensable cybersecurity services.

Currently, the Singapore government has gazetted a list of 11 sectors in which there may be essential services (ie, services which are essential to national security, defence, foreign relations, the economy, public health, public safety or the public order of Singapore). The 11 sectors include: energy; info-communications; media; water; healthcare; banking and finance; security and emergency services; aviation; land transport; maritime; and services relating to the functioning of the government.

The Commissioner has broad powers to investigate and prevent cybersecurity threats or incidents, including making requests for information to be provided or, in serious cases, direct remedial measures to be taken by any person (including those who are not owners of CII).

Personal Data Protection Commission

The Personal Data Protection Commission (PDPC) is Singapore's data protection authority. The PDPC, which is under the purview of the MDDI, was established in January 2013 and tasked with enforcing and administering the PDPA. With effect from 1 October 2016, the PDPC was merged into the then newly formed IMDA and IMDA was designated as the PDPC. The PDPC is led by the Commissioner for Personal Data Protection.

The PDPA broadly applies to private sector organisations, whether or not formed or recognised under the laws of Singapore or resident or having an office or a place of business in Singa-

pore. As such, foreign businesses that carry out activities involving personal data in Singapore may be subject to the data protection provisions under the PDPA. In terms of notable exclusions, the PDPA does not apply to individuals acting in a personal or domestic capacity, employees acting in the course of their employment with an organisation, and public agencies.

The PDPA confers powers on the PDPC to enforce the PDPA, which include powers relating to:

- alternative dispute resolution (eg, mediation);
- reviews of data subjects' access and correction requests;
- investigations to ensure compliance with the PDPA (including the DNC provisions); and
- undertakings.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

Please refer to **1.2 Cybersecurity Laws** and **1.3 Cybersecurity Regulators** for further details on when a CII may fall under the scope of the Cybersecurity Act.

2.2 Critical Infrastructure Cybersecurity Requirements

Generally, owners of CII are required to comply with a set of general duties, such as:

- to comply with notices issued by the Commissioner to provide information on the technical architecture of the CII;
- to comply with codes of practice, standards of performance or written directions in relation to the CII;

- to notify the Commissioner of any change in ownership of the CII;
- to notify the Commissioner of any prescribed cybersecurity incidents (please refer to **2.3 Incident Response and Notification Obligations**);
- to conduct regular audits of the compliance of the CII with the Cybersecurity Act, codes of practice and standards of performance;
- to conduct regular risk assessments of the CII as required by the Commissioner; and
- to participate in cybersecurity exercises as required by the Commissioner.

The Cybersecurity Code of Practice for Critical Information Infrastructure (the "CII Cybersecurity Code") requires owners of CII to put in place security baseline configuration standards for all operating systems, applications and network devices of a piece of CII that is commensurate with the cybersecurity risk profile of that CII. The security baseline configuration standards address the following security principles:

- least access privilege and separation of duties;
- enforcement of password complexities and policies;
- removal of unused accounts;
- removal of unnecessary services and applications (eg, removal of compilers and vendor support applications);
- closure of unused network ports;
- protection against malware; and
- timely update of software and security patches that are approved by system vendors.

The CII Cybersecurity Code sets out the following protection requirements that owners of CII need to put in place.

- Access control – CII owners must implement authentication techniques for access into the CII, maintain logs of all access into a CII and of all attempts to access the CII, and review these logs for anomalous activities on a regular basis.
- System hardening – CII owners must establish security baseline configuration standards for the CII.
- Remote connection – CII owners must ensure that all remote connections to the CII have effective cybersecurity measures to prevent and detect unauthorised access.
- Removable storage media – CII owners shall ensure that strict control is exercised over the connection of removable storage media and portable computing devices to a CII.
- Vulnerability assessment and penetration testing – CII owners shall conduct a vulnerability assessment of their CII to identify security and control weaknesses within 12 months from when the CII is designated under the Cybersecurity Act, and at least once every 12 months thereafter for CII that are IT systems; each vulnerability assessment should include (i) a host security assessment, (ii) a network security assessment, and (iii) an architecture security review.

Following the passing of the Cybersecurity (Amendment) Bill, the upcoming Cybersecurity Act will cover four new classes of entities.

- Designated providers of essential services that do not own the CII used for the continuous delivery of the essential services they are responsible for (third-party-owned CII): the providers of such essential services are required to obtain legally binding commitments from the third-party to provide the necessary information or adhere to prescribed standards relating to cybersecurity, etc. The

Commissioner may order such providers to cease using the third-party-owned CII if they do not obtain the legally binding commitments.

- Owners of computers or computer systems designated as systems of temporary cybersecurity concern: for example, the temporary systems used to support the distribution of critical vaccines during a pandemic could fall under this category.
- Designated entities of special cybersecurity interest: if the function of such designated entities perform is disrupted, or if the sensitive information contained in their computer systems is disclosed, there will be a significant detrimental effect on the defence, foreign relations, economy, public health, public safety or public order of Singapore.
- Designated providers of major foundational digital infrastructure services: these services promote the availability, latency, throughput or security of digital services, and relate to cloud computing services and data facility services.

The upcoming amendments to the Cybersecurity Act impose obligations on these new entities that are similar to those already in force relating to CII, such as:

- providing the Commissioner with information;
- complying with any codes of practice, standards of performance or written directions that may be issued or approved by the Commissioner; and
- notifying the Commissioner of any prescribed cybersecurity incident – the exact scope of incident reporting and the applicable cybersecurity codes of practice/standards/guidelines applicable to these new entities have not been published at the time of writing.

2.3 Incident Response and Notification Obligations

Under the Cybersecurity (Critical Information Infrastructure) Regulations 2018, cybersecurity incidents that must be reported to the Commissioner include:

- any unauthorised hacking of the CII or the interconnected computer or computer system to gain unauthorised access to or control of the CII or interconnected computer or computer system;
- any installation or execution of unauthorised software, or computer code, of a malicious nature on the CII or the interconnected computer or computer system;
- any man-in-the-middle attack, session hijack or other unauthorised interception by means of a computer or computer system of communication between the CII or the interconnected computer or computer system, and an authorised user of the CII or the interconnected computer or computer system, as the case may be; and
- any denial-of-service attack or other unauthorised act or acts carried out through a computer or computer system that adversely affects the availability or operability of the CII or the interconnected computer or computer system.

2.4 State Responsibilities and Obligations

The Cybersecurity Act sets out a number of duties and functions of the Commissioner of Cybersecurity in relation to the identification and response to cyber threats.

Under Section 5 of the Cybersecurity Act, the Commissioner of Cybersecurity has a duty, among others:

- to monitor cybersecurity threats in or outside of Singapore;
- to advise the government or any other public authority on the national needs and policies in respect of cybersecurity matters generally; and
- to respond to cybersecurity incidents that threaten the national security, defence, economy, foreign relations, public health, public order or public safety, or any essential services of Singapore, whether such cybersecurity incidents occur in or outside Singapore.

Additionally, the Singapore Computer Emergency Response Team (SingCERT), which is part of the CSA, routinely issues cybersecurity and cyber hygiene advisories and alerts. SingCERT also works with the sectoral regulators to issue relevant alerts and advisories to industry players and to inform companies and affected individuals on cybersecurity threats and incidents.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

Please refer to **1.2 Cybersecurity Laws** for a summary of the sectoral cybersecurity laws applicable to the banking and finance sector.

In the banking and finance sector, the MAS has issued a set of legally binding Notices on TRM and Cyber Hygiene which apply to FIs (eg, banks, insurers, capital markets services licence holders, operators, and settlement institutions of designated payment systems). These Notices impose obligations on FIs to enhance information security and mitigate the growing risks of cyberthreats.

The TRM Notices include requirements to:

- put in place a framework and process to identify critical systems;
- make reasonable efforts to maintain a high availability of critical systems;
- establish a recovery time objective for each critical system;
- notify the MAS of a system malfunction or IT security incident;
- submit a root cause and impact analysis report to the MAS of the relevant incident within 14 days; and
- implement IT controls to protect customer information from unauthorised access or disclosure.

The Notices on Cyber Hygiene include requirements to:

- secure administrative accounts;
- apply security patching;
- establish baseline security standards;
- deploy network perimeter defences;
- implement anti-malware measures; and
- strengthen multi-factor authentication.

3.2 ICT Service Provider Contractual Requirements

Under the TRM Guidelines, MAS sets out a number of principles and best practices to in relation to third-party service providers, which include:

- ensuring service providers have the requisite level of competence and skills to perform IT functions and manage technology risks;
- conducting IT security awareness training programmes for service providers who have access to FIs' information assets;
- identifying threats and vulnerabilities applicable to information assets that are maintained or supported by service providers;

- assessing service providers' disaster recovery capability and ensuring that disaster recovery arrangements are established, tested and verified to meet FIs' business needs;
- ensuring service providers are accorded the same level of protection and subject to the same security standards in data security as FIs;
- involving service providers in scenario-based cyber exercises to validate FIs' response and recovery, as well as communication plans against cyber threats; and
- reporting of phishing attempts to service providers.

More generally, ICT service providers may fall under the upcoming category of designated providers of major foundational digital infrastructure services under the Cybersecurity Act. "Foundational digital infrastructure services" are services that promote the availability, latency, throughput or security of digital services, and have been specified in the Third Schedule to the upcoming Cybersecurity Act. This will include a "cloud computing service" and a "data centre facility service", as set out below.

- A "cloud computing service" is defined as a service, delivered from a computer or computer system in Singapore or outside Singapore, that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources.
- A "data centre facility service" is defined as any service which relies on a computer or computer system in Singapore to facilitate data storage, processing and transmission by another person through the centralised accommodation, interconnection and operation of one or more computers or computer

systems, encompassed within a facility in Singapore dedicated to that purpose.

Under the upcoming Cybersecurity Act, designated providers of major FDI services will be subject to obligations such as providing the Commissioner with information, reporting prescribed cybersecurity incidents, and complying with codes of practices and directions that may be issued or approved by the Commissioner.

On 1 March 2024, the legislature announced that the inter-agency Taskforce on the Resilience and Security of Digital Infrastructure and Services is studying the introduction of a Digital Infrastructure Act to further enhance the resilience and security of key digital infrastructure and services in Singapore. At the time of writing, there is no publicly available information on the obligations imposed on digital infrastructure providers under the upcoming Digital Infrastructure Act.

3.3 Key Operational Resilience Obligations

The key obligations relating to digital operation resilience in the financial sector can be derived from Part 8 of the TRM Guidelines relating to IT resilience. The best practices that FIs should aim to comply with include:

- establishing system availability commensurate with its business needs;
- establishing system recoverability aligned to its business resumption and system recovery priorities;
- regularly testing their disaster recovery plans to validate their effectiveness and meet the defined recovery objectives;
- establishing a system and data backup strategy so that systems and data can be recovered in the event of a system disruption or when data is corrupted or deleted; and

- conducting a Threat and Vulnerability Risk Assessment for their data centres to identify potential vulnerabilities, and the protection that should be established to safeguard the data centres against physical and environmental threats.

In terms of incident reporting obligations, FIs should establish cyber-incident response and management plans to swiftly isolate and neutralise cyber threats and to securely resume affected services. The plan should describe communication, co-ordination and response procedures to address plausible cyber threat scenarios. Each FI should seek to understand their exposure to technology risks and place a robust risk management framework to ensure cyber resilience.

FIs may also be designated as CII under the Cybersecurity Act. For more information on the designation of CII and the obligations imposed on CII under the Cybersecurity Act, please refer to **1.2 Cybersecurity Laws**, **1.3 Cybersecurity Regulators** and **2.2 Critical Infrastructure Cybersecurity Requirements**.

3.4 Operational Resilience Enforcement

There are no specific obligations relating to operation resilience in relation to critical ICT service providers. However, critical ICT service providers in the financial sector can take guidance from Part 8 of the TRM Guidelines (please refer to **3.3 Key Operational Resilience Obligations** for further details).

Generally, under Section 29(1) of the Financial Services and Markets Act, MAS has the power to issue directions or make regulations concerning any FI or class of FIs as the MAS considers necessary for:

- the management of technology risks, including cybersecurity risks;
- the safe and sound use of technology to deliver financial services; and
- the safe and sound use of technology to protect data.

In terms of enforcement action, an FI that fails to comply with a direction issued to it under Section 29(1) or contravenes any regulation mentioned in that subsection shall be guilty of an offence and shall be liable on conviction to a fine not exceeding SGD1 million and, in the case of a continuing offence, to a further fine of SGD100,000 for every day or part of a day during which the offence continues after conviction.

The maximum penalty of SGD1 million is commensurate with the most serious types of breaches that can be committed by FIs. This quantum was derived after considering comparable existing penalty regimes of other Singapore government agencies and the need to signal the importance of TRM.

Additionally, under the current Cybersecurity Act, the Commissioner has broad powers under Sections 19 and 20 to investigate and prevent cybersecurity incidents and “serious” cybersecurity incidents respectively. These include powers to require persons to attend interviews, require the production of relevant information (such as physical or electronic records, or documents that are in the possession of that person), carry out questioning, give directions to carry out remedial measures or cease activities, require assistance with investigations, enter premises, access and inspect computer systems, among others.

It is an offence for any person to fail to co-operate with the CSA without reasonable excuse and

such persons shall be liable on conviction to be punished in accordance with the fines, terms of imprisonment or both, as set out in the relevant statutory provisions.

Under the upcoming Section 18K(1) of the upcoming Cybersecurity Act, the Commissioner may require major FDI service providers to furnish information. If the major FDI service provider fails to, without reasonable excuse, furnish the required cybersecurity-related information within the specified period or continues providing the designated FDI service despite the non-compliance, they shall be guilty of an offence. They shall be liable for a fine not exceeding the greater of SGD200,000 or 10% of the annual turnover of the service provider’s business in Singapore.

The upcoming Section 18L(1) also empowers the Commissioner to issue written instructions to major FDI service providers which may relate to the action to be taken by the provider in relation to a cybersecurity threat, compliance with any prescribed technical standards relating to cybersecurity, among others. Any major FDI service provider who fails to comply with such a written direction and continues to provide FDI infrastructure service after the deadline for compliance will be liable on conviction to a fine not exceeding the greater of SGD200,000 or 10% of the annual turnover of the person’s business in Singapore.

Further, under the upcoming Section 18M (1), major FDI service providers must notify the Commissioner of the occurrence of a prescribed cybersecurity incident in respect of the major FDI, where the incident results in a disruption or degradation to the continuous delivery of the foundational digital infrastructure service or the major FDI service provider’s business operations in Singapore. Any major FDI service provider

who, without reasonable excuse, fails to comply with this obligation shall be guilty of an offence and liable on conviction to a fine not exceeding the greater of SGD200,000 or 10% of the annual turnover of the person's business in Singapore.

As the provisions relating to the obligations for major FDI service providers have yet to come into force, there are no enforcement decisions against major FDI service providers for the failure to comply with the Cybersecurity Act.

3.5 International Data Transfers

There are no specific obligations imposed by MAS in relation to financial institutions carrying out international data transfers. However, generally, organisations transferring personal data overseas must comply with Section 26 of the PDPA. Under Section 26, organisations need to ensure that the personal data transferred overseas is accorded a standard of protection that is comparable to the protection under the PDPA.

Under the Personal Data Protection Regulations 2021 (the "PDP Regulations"), the transferring organisation must take appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data is bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA.

"Legally enforceable obligations" include any of the following obligations which are imposed on the recipient of the personal data under:

- any law;
- any contract requiring the recipient to provide a standard of protection for the personal data transferred to the recipient that is at least comparable to the protection under the PDPA

and specify the countries and territories to which the personal data may be transferred under the contract;

- any binding corporate rules that require every recipient of the transferred personal data that is related to the transferring organisation to provide a standard of protection for the personal data transferred to the recipient that is at least comparable to the protection under the PDPA; and which specifies:
 - (a) the recipients of the transferred personal data to which the binding corporate rules apply;
 - (b) the countries and territories to which the personal data may be transferred under the binding corporate rules; and
 - (c) the rights and obligations provided by the binding corporate rules; and
- any other legally binding instrument, including the Asia-Pacific Economic Cooperation (APEC) Privacy Recognition for Processors System or the APEC Cross Border Privacy Rules System, which are recognised under the PDP Regulations as one of the modes of transferring data overseas.

The transferring party is required to specify the countries and territories to which the personal data may be transferred under the contract if the party relies on imposing contractual obligations on the recipient for the data transfer.

A transferring party has taken the appropriate steps to ensure that the recipient is bound by legally enforceable obligations to provide the personal data transferred a standard of protection that is comparable to that under the PDPA if:

- the data subject whose personal data is to be transferred gives their consent to the transfer of their personal data, after being provided with a reasonable summary in writing of the

extent to which the personal data transferred to those countries and territories will be protected to a standard comparable to the protection under the PDPA; or

- the transfer is necessary for the performance of a contract between the organisation and the data subject, or to do anything at the data subject's request with a view to their entering a contract with the organisation.

As good practice, however, organisations are encouraged to rely on the above circumstances only if they are unable to rely on legally enforceable obligations or specified certifications.

In respect of international data transfers between regulatory authorities in the financial sector, the MAS is a signatory to the Administrative Arrangement (AA) for the Transfer of Personal Data between European Economic Area (EEA) Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities.

The AA sets out the safeguards relating to data transfers between regulatory authorities which include purpose limitation, data quality and proportionality, transparency, security and confidentiality, data subject rights, onward transfers and sharing of personal data, data retention periods, and redress. As a signatory, MAS confirms that it adheres to the safeguards outlined in the AA.

More generally, Singapore joined the APEC Cross-Border Privacy Rules System and Privacy Recognition for Processors System in 2019, which are accountability-based and enforceable certifications developed by APEC economies for cross-border transfers of personal data.

In January 2021, the member states of the Association of Southeast Asian Nations (ASEAN) approved the ASEAN Data Management Frame-

work (DMF), and the Model Contractual Clauses for Cross Border Data Flows (MCCs), which are resources and tools for ASEAN businesses to utilise in their data-related business operations. In summary, the DMF provides a common data protection framework for businesses on good data management practices and best practices, while the MCCs are a set of template contractual terms and conditions that may be included in the binding legal agreements between parties transferring personal data to each other across borders.

In May 2023, the Joint Guide to ASEAN MCCs and EU Standard Contractual Clauses (SCCs) was launched (the "Joint Guide"). The Joint Guide provides a comparison between ASEAN MCCs and SCCs for organisations looking to transfer or receive consumer data from overseas partners. Companies already familiar with the ASEAN MCCs can use the Joint Guide as a reference in their contractual negotiations on data transfers with their EU business partners.

3.6 Threat-Led Penetration Testing Critical Information Infrastructure

Under the CII Cybersecurity Code, owners of CII are required to conduct regular penetration testing on CII to identify security vulnerabilities that could be exploited by a cyber threat actor. This allows organisations to determine exploitable vulnerabilities in their systems and address them.

Owners of CII are required to conduct a penetration test on the CII:

- at least once every 12 months, for CII which is an information technology system; and
- at least once every 24 months, for CII which is an operational technology system.

Owners of CII must also conduct penetration tests on relevant CII assets after implementing any major system changes to the CII. Major system changes include commissioning any new systems to be connected to the CII, implementing new application modules, system upgrades and technology refresh.

It is the responsibility of CII owners to ensure that third-party penetration testing service providers and their penetration testers possess industry-recognised accreditations and certifications respectively, for example CREST or equivalent accreditations and certifications.

Relatedly, owners of CII are also required to establish a red teaming or purple teaming attack simulation plan, and conduct a red teaming or purple teaming attack simulation on its CII at least once every 24 months to test and validate the effectiveness of its cybersecurity measures against prevalent cybersecurity threats.

Cybersecurity Service Provider Licences

The Cybersecurity Services Regulation Office (CSRO) was set up to administer the licensing framework for CSPs under the Cybersecurity Act. It aims to address three main considerations:

- provide greater assurance of security and safety to consumers;
- improve the standards and standing of CSPs; and
- address the information asymmetry between consumers and CSPs.

All providers of a managed security operations centre monitoring services and penetration testing services as defined in the Cybersecurity Act to the Singapore market must apply to the CSRO for a cybersecurity service provider's

licence, regardless of whether they are companies or individuals or third-party CSPs that provide these services in support of other CSPs.

IoT Devices

On 3 March 2020, the MDDI (then Ministry of Communication and Information) introduced the Cybersecurity Labelling Scheme (CLS) as part of Singapore's Safer Cyberspace Masterplan 2020. The CLS was formally launched on 7 October 2020, initially as a voluntary scheme for Wi-Fi routers and smart home hubs, and was subsequently expanded to include all smart home devices.

The CLS provides different cybersecurity rating levels for registered IoT devices and other smart devices to help consumers easily assess the level of security offered and make informed choices in purchasing a device. A Level 1 certification indicates that the product meets basic security requirements such as ensuring unique default passwords and providing software updates, whilst a Level 4 certification indicates that the product has undergone structured penetration tests by approved third-party test labs and fulfilled the requirements of all lower levels (ie, Levels 1, 2 and 3).

In 2024, the CSA updated Singapore's Operational Technology Cybersecurity Masterplan. The updated Masterplan now includes operators of operational technologies that support physical control functions such as IoT and industrial IoT devices, as such devices have become new attack surfaces for threat actors to exploit. The key initiatives under the Masterplan include:

- enhancing the operational technology cybersecurity talent pipeline;
- enhancing information sharing and reporting;

- uplifting operational technology cybersecurity resilience beyond CII; and
- promoting secure-by-development principles.

ICT Systems Containing Personal Data

As Section 24 of the PDPA requires organisations to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks, penetration testing may be helpful in determining whether the organisation is in compliance with the PDPA. Furthermore, the PDPC's Guide to Data Protection Practices for ICT Systems and Guide to Data Protection by Design for ICT Systems generally recommend the conduct of penetration testing to ensure data protection measures operate as intended and to detect any vulnerabilities.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

The Singapore Cybersecurity Strategy 2021 emphasises enhancing response capabilities for the state, organisations and individuals rather than an emphasis on expanding legislation relating to cyber-resilience (please refer to **1.1 Cybersecurity Regulation Strategy** for more details).

As such, apart from the Cybersecurity Act, and the patchwork of other cybersecurity and sectoral legislation mentioned in **1.2 Cybersecurity Laws**, the legislative status of cyber-resilience in Singapore remains relatively sparse compared to other jurisdictions such as the European Union which has the dedicated Cyber Resilience Act.

4.2 Key Obligations Under Legislation

Please refer to **1.2 Cybersecurity Laws**, **2.2 Critical Infrastructure Security Requirements**, **3.2 ICT Service Provider Contractual Requirements**, **3.3 Key Operational Resilience Obligations** and **4.1 Cyber-Resilience Legislation**.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

While there is no prescribed cybersecurity certification legislation in Singapore, the CSA offers, administers and supports the use of certification schemes to provide assurance to customers that the product has been objectively assessed from a cybersecurity standpoint.

The CSA Cybersecurity Certification Centre operates three schemes which cover ICT product security in general. For example, besides the CLS, the Singapore Common Criteria Scheme (SCCS) provides a cost-effective regime to evaluate and certify the security of IT products in Singapore against the Common Criteria (CC) standards (ie, ISO/IEC 15408 series). CC is a common set of standards initially developed through a collaboration among national security and standards organisations in Canada, France, Germany, the Netherlands, the UK and the USA. Under the Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security (also known as Common Criteria Recognition Arrangement (CCRA)), which forms the basis of international recognition of CC certifications, Singapore's SCCS is recognised as a Certificate Authorising Scheme. The CC harmonises the evaluation (which ranges from document review to deep penetration testing) of IT products by defining a common set of security func-

tions which product developers use, to establish the security requirements of their IT products in a standardised language.

The PDPC and the IMDA jointly developed the Data Protection Trustmark (DPTM) Certification to help organisations demonstrate compliance with the PDPA. The DPTM Certification serves as a visible indicator that organisations have adopted sound data protection practices, strengthening trust between customers, business partners and regulators to increase business competitiveness. The DPTM Certification aligns its requirements with the PDPA and also incorporates elements of international benchmarks and data protection best practices.

Singapore has also joined the APEC Cross-Border Privacy Rules System and Privacy Recognition for Processors System in 2019 (see **3.5 International Data Transfers**).

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

In terms of broad focus and application, the Cybersecurity Act addresses national cybersecurity issues and protects computers and computer systems in Singapore by imposing obligations on owners of CII. In contrast, the PDPA seeks to protect consumers and individuals by imposing obligations on private sector organisations that collect, use, disclose or otherwise process personal data.

General Requirements Under the PDPA

In the context of personal data protection, organisations are required to, amongst other things, put in place data protection policies and practices to ensure and demonstrate compli-

ance with their obligations under the PDPA. Specifically, these requirements include:

- appointing a data protection officer to oversee compliance with the PDPA;
- developing and implementing data protection policies, practices and procedures (which include technical security arrangements) to ensure proper processing of personal data;
- providing adequate training to staff that handle and process personal data; and
- conducting a data protection impact assessment to determine that the proposed collection, use or disclosure of the personal data is not likely to have an adverse effect on the individual (where applicable).

Protection Obligation

Additionally, under the protection obligation (Section 24 of the PDPA), an organisation is required to make reasonable security arrangements to protect personal data in their possession or under their control in order to prevent (i) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and (ii) the loss of any storage medium or device on which personal data is stored.

Data Breach Notification

With effect from 1 February 2021, a mandatory data breach notification regime has been introduced into the PDPA.

A “data breach” in relation to personal data is defined in the PDPA to mean:

- the unauthorised access, collection, use, disclosure, copying, modification, or disposal of personal data; or
- the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection,

use, disclosure, copying, modification, or disposal of the personal data is likely to occur.

Where an organisation has reason to believe that a data breach affecting personal data in its possession or control has occurred, it must conduct an assessment of whether the data breach is a “notifiable data breach” in a reasonable and expeditious manner.

A data breach is a “notifiable data breach” if the data breach (i) results in, or is likely to result in, significant harm to an affected individual; or (ii) is, or is likely to be, on a significant scale (ie, affecting at least 500 persons).

According to the Personal Data Protection (Notification of Data Breaches) Regulations 2021 (the “Data Breach Regulations”), a data breach is deemed to result in significant harm to an individual if the data breach relates to the following:

- the individual’s full name or alias or identification number, and any of the personal data or classes of personal data relating to the individual as set out in the schedule to the Data Breach Regulations.
- all of the following personal data relating to an individual’s account with an organisation:
 - (a) the individual’s account identifier, such as an account name or number; or
 - (b) any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to, or use of, the individual’s account.

Notification to the PDPC

Upon assessing that the data breach is a “notifiable data breach”, the organisation must notify the PDPC in the prescribed form and manner as soon as practicable but no later than three

calendar days after assessment. This notification to the PDPC must contain all the relevant information of the data breach to the best of the knowledge and belief of the organisation.

Notification to Affected Individuals

Upon notifying the PDPC, the organisation must also notify each individual affected by the data breach, unless an exception applies. An organisation does not need to notify affected individuals in two circumstances:

- if, on or after assessing that the data breach is a “notifiable data breach”, the organisation takes any action that renders it unlikely that the data breach will result in significant harm to the affected individual; or
- if the organisation had implemented, prior to the occurrence of the data breach, any technological measure that renders it unlikely that the data breach will result in significant harm to the affected individual.

Notification to the Primary Organisation

Where a data intermediary processing personal data on behalf of another organisation has reason to believe a data breach has occurred, it must, without undue delay, notify the primary organisation.

6.2 Cybersecurity and AI

Computers or computer systems which support AI solutions may be designated as a CII under the Cybersecurity Act if they are necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore, and the computer or computer system is located wholly or partly in Singapore. For more details on which entities may be designated as CII and the obligations that a CII will have to

comply with, please refer to **1.2 Cybersecurity Laws**, **1.3 Cybersecurity Regulators** and **2.2 Critical Infrastructure Cybersecurity Requirements**.

While there are no express cybersecurity obligations relating to AI in Singapore at the time of writing, a number of voluntary frameworks and guidelines have been published relating to the development and use of AI.

The second edition of the Model AI Framework was published by the PDPC on 21 January 2020. The framework sets out the common definitions and principles relating to the responsible use of AI generally, making practical recommendations that organisations can readily adopt to deploy AI responsibly.

On 30 May 2024, the Model AI Governance Framework for Generative AI, which sets out a systematic and balanced approach to address generative AI concerns while facilitating innovation, was published by IMDA and AI Verify Foundation. In particular, the framework recommends that generative AI developers adapt the “security-by-design” concept, which involves designing security into every phase of the systems development life cycle of an AI, to fit the specific characteristics of generative AI. New security safeguards which the framework recommends be developed include input filters, which are moderation tools designed to detect unsafe prompts, and digital forensics tools, which can be used to investigate digital data to reconstruct cybersecurity incidents stemming from a generative AI model.

The framework also makes recommendations with regard to incident reporting. As part of an overall proactive security approach, AI software product owners should adopt vulnerability

reporting before incidents happen. After incidents happen, organisations need internal processes to report the incident for timely notification and remediation. Depending on the impact of the incident and how extensively AI was involved, organisations should consider notifying both the public as well as the government.

On 15 October 2024, the CSA published the Guidelines and Companion Guide on Securing AI Systems. The Guidelines address potential security risks through the AI lifecycle, and help to protect AI systems against traditional cybersecurity risks such as supply chain attacks, and novel risks such as adversarial machine learning. On the other hand, the companion guide offers practical security control measures that system owners may consider in implementing these guidelines. Key recommendations include taking a lifecycle approach to consider security risks and beginning with a risk assessment.

Lastly, the Engaging with Artificial Intelligence guide, which was published on 25 January 2024 by the Australian Signals Directorate’s Australian Cyber Security Centre in conjunction with the CSA and 13 other international agencies, also provides organisations with guidance on how to use AI systems securely. The guide summarises some important threats related to AI systems and prompts organisations to consider steps they can take to engage with AI while managing risk. The document provides cybersecurity mitigations to assist organisations that use self-hosted and/or third-party hosted AI systems.

6.3 Cybersecurity in the Healthcare Sector

While there are no specific cybersecurity obligations pertaining to the healthcare sector, the healthcare sector has been gazetted as one of 11 sectors providing essential services. As such,

designated owners of CII within the healthcare sector would be subject to the same requirements as laid out in **2.2 Critical Infrastructure Cybersecurity Requirements**.

Beyond CII, there are a number of security requirements relating to devices in the medical field. Depending on the type of medical device, the relevant regulators may include the Health Sciences Authority (HSA), the National Environment Agency and the IMDA. Where applicable, healthcare providers must also comply with the National Telemedicine Guidelines, which include data protection and security requirements. Insofar as a medical device is used by an organisation to collect personal data (eg, device test results are uploaded onto a server owned by the organisation), the organisation must comply with the protection obligation under the PDPA (as described in **6.1 Cybersecurity and Data Protection** above).

On 4 December 2023, the Cyber and Data Security Guidelines for Healthcare Providers (Healthcare Guidelines) was published. The Healthcare Guidelines provide guidance on the cyber and data security measures to be put in place for the proper storage, access, use and sharing of health information to improve the security posture amongst healthcare providers. Healthcare providers looking to better understand and meet the Healthcare Guidelines can also refer to the Cyber and Data Security Guidebook for healthcare providers for explanations and references to resources from the CSA and PDPC. While not mandatory, the requirements within the Healthcare Guidelines will eventually be imposed as regulatory requirements under the upcoming Health Information Act, which has yet to come into force at the time of writing.

In October 2024, the Cybersecurity Labelling Scheme for Medical Devices (CLSMD), which was jointly developed by the CSA, Ministry of Health, HSA and Synapse, was launched. Under this voluntary scheme, medical devices are rated according to four levels of cybersecurity provisions, with each level indicating a progressively higher standard of security. The label aims to improve security awareness by making the cybersecurity provisions of medical devices more transparent to healthcare users, thereby empowering them to make more informed purchasing decisions.

The CLSMD applies to medical devices as described in the First Schedule of the Health Products Act 2007 that have any of the following characteristics:

- handle personal identifiable information and clinical data, and can collect, store, process, or transfer such data; and
- connect to other devices, systems, and services, and can communicate using wired and/or wireless communication protocols through a network of connections.

Trends and Developments

Contributed by:

Sheena Jacob, Jaya Malhotra, Sherman Poon and Andre Choo

CMS

CMS is a future facing firm with 85 offices in 49 countries and over 6,300 lawyers worldwide, combining deep local market understanding with a global overview. In a rapidly evolving world where technology is pivotal to global strategies, CMS provides clear, business-focused advice to help clients navigate the future with confidence. Its global cybersecurity practice offers market-leading expertise in managing all aspects of a cyber breach, from pre-breach readiness and stress testing to incident response co-ordination. The firm assists

clients with cybersecurity preparation, including reviewing security policies and advising on regulatory and licensing regimes. CMS takes a holistic approach, leveraging local knowledge to address region-specific challenges. Trusted by high-profile clients across various sectors, the firm provides strategic solutions for business-critical, multi-jurisdictional cybersecurity challenges, ensuring clients are equipped to respond effectively to cyber-risks and regulatory requirements.

Authors



Sheena Jacob heads the technology, media, IP and competition (TMIC) group at CMS Holborn Asia and leads the technology practice in Asia. With over 30 years of specialist

experience in the region, she is widely regarded as a leading technology lawyer, with expertise spanning cybersecurity, media, privacy and fintech. Sheena advises major entertainment and media players, including streaming platforms, on cybersecurity, privacy and data localisation issues across Asia. Her leadership roles on industry committees and boards underscore her position as a thought leader in these areas, with her contributions to the TMT, IP and data privacy sectors consistently recognised by leading directories.



Jaya Malhotra is a senior associate in CMS Holborn Asia's technology, media, IP and competition (TMIC) team. Jaya has advised multinational companies on regulatory issues

in the media, telecommunications, technology and healthcare sectors in Asia. She has advised on regional matters involving data protection and privacy, consumer protection regulations, telecommunications, and cloud computing. Prior to joining CMS, Jaya spent four years as in-house counsel at Amazon, supporting the Devices and Digital Content business in APAC and Amazon Web Services' Network Infrastructure business in APAC and the Middle East.

SINGAPORE TRENDS AND DEVELOPMENTS

Contributed by: Sheena Jacob, Jaya Malhotra, Sherman Poon and Andre Choo, CMS



Sherman Poon is a Singapore qualified associate in CMS Holborn Asia's technology, media, IP and competition (TMIC) team. He regularly advises on technology, media and telecommunication (TMT) matters from both a regulatory compliance and transactional perspective. His experience includes advising clients on their data protection and cybersecurity compliance, representing clients in data breach proceedings before the regulator, and advising and negotiating on technology transactions (eg, software development contracts and SaaS licensing agreements). Sherman also has experience advising and representing clients in both contentious and non-contentious IP matters.



Andre Choo is a Singapore qualified associate in CMS Holborn Asia's technology, media, IP and competition (TMIC) team. Andre has advised multinational companies (technology, commerce, mass media, entertainment), SMEs and other companies on regulatory issues in the media, telecommunications, technology, healthcare and life sciences sectors in Asia. He has co-ordinated local and regional matters involving data protection and privacy, cybersecurity, gaming and gambling and IP. He has also handled data and cybersecurity incidents, licensing requirements, and content regulation and approval.

CMS

7 Straits View
Marina One East Tower #19-01
Singapore 018936

Tel: +65 6720 8278
Fax: +65 6720 8279
Email: sheena.jacob@cms-holbornasia.com
Web: www.cms.law



Introduction

The rapid technological advancements of the 21st century and digital transformation have accelerated the development of national cybersecurity concerns globally. As a result, the issue of cybersecurity as a lynchpin of national security has moved to the forefront of many governments' agendas. Both the volume of cyber threats and their constant evolution have made cyber warfare, cybercrime and cyber-risk the new battleground of the digital revolution. Given Singapore's position as a financial and digital transformation leader in Asia, ensuring the city state tackles cybersecurity risks is critical to its security.

Cybersecurity Threats and Trends

Escalation of cybercrimes

Global costs from cybercrime are estimated to reach USD10.5 trillion annually in 2025, despite an estimated USD101.5 billion projected spending on cybersecurity services (see [here](#)). Singapore has not been able to avoid the growing threat of cybercrime. The Singapore Police Force reported an 18% increase in scam and cybercrime incidents from January to June 2024, as compared to the same period in 2023 (see [here](#)). The total losses from cybercrime increased from SGD334.5 million to SGD385.6 million during this period. This increase is accompanied by an increase in the sophistication of cyber scams which have escalated with the use of AI as an effective tool in the hands of cyber criminals.

Surge in phishing attempts

The Cyber Security Agency (CSA) identified a rise in phishing attempts reported to the Singapore Cyber Emergency Response Team ("SingCert") in recent years. The CSA noted that scammers are employing new methods to make their phishing attempts appear more authentic, such as including HTTPS protocols in

their phishing URLs or utilising more legitimate looking domains like ".com" instead of ".xyz".

In Singapore, organisations in the banking and financial services, government and technology sectors were the most frequently attacked. In 2023, 63% of all reported phishing attempts involved spoofs of companies in the banking and financial services sector (see [here](#)). The use of tools like generative AI have also enabled scammers to produce more convincing phishing content, and the threat of sophisticated, large-scale phishing will continue as a key cybersecurity risk.

Continued growth of ransomware

Ransomware remains another key risk in Singapore, with 132 reported cases in both 2022 and 2023. A survey by cybersecurity firm Cohesity noted that over 190 firms reported being subject to ransomware attacks in 2024 (see [here](#)). Threat actors have targeted businesses across a wide range of industries, and the CSA noted in 2023 that companies engaged in manufacturing and construction were amongst the most targeted industries (see [here](#)).

A Singapore law firm suffered an Akira ransomware attack in April 2024. Although the firm reported that there was no evidence indicating that its document management systems containing client data were affected, it allegedly paid 21.07 bitcoins to Akira ransomware group. The incident illustrates the attractiveness of targeting organisations holding large amounts of sensitive client data, especially since victims of ransomware may be subject to additional pressure from their clients to pay the ransom to protect their affected data.

Many incidents could have been avoided with reasonable security precautions implemented

and the CSA noted that local organisations averaged only a 70% adoption rate of essential cybersecurity measures, with only a third of organisations fully implementing at least 60% of measures recommended in the national cybersecurity standards.

The dilemma of cyber-insurance

The evolving threat landscape has prompted more insurers to offer cyber-insurance for organisations seeking to mitigate the financial risks of cyber-incidents. As costs of a cybersecurity incident or threat can be significant, cyber-insurance coverage is important to manage the various types of costs that may be incurred, including lawyers, computer forensics experts, crisis management and public relations consultants, and ransomware negotiators. Cyber-insurance helps companies mitigate the risk of harm perpetuated by threat actors, allowing organisations to mitigate or even recoup their financial losses (see [here](#)).

However, while cyber-insurance often makes commercial sense for organisations, insurance payouts which go towards paying the ransom costs may create a perverse incentive for threat actors, since having more organisations holding cyber-insurance policies which cover extortion cost payouts may encourage threat actors to launch further attacks. As such many governments, including the Singapore government, discourage victims from paying ransoms, pointing out that doing so perpetuates a cycle where hackers and scammers target firms that have previously made payouts or new organisations with cyber-insurance, as they may be more inclined to pay the extortion costs. As cyber-insurance becomes more widely adopted, the impact on the rates of cyber-attacks remains to be seen.

Is it time to rethink the laws on ransomware payments?

While ransomware payments are not prohibited by law in many countries including in Singapore, anti-money laundering (AML) and countering the financing of terrorism (CFT) regulations, as well as criminal laws, are applicable to such payments. Since cyber threat actors may well be involved in criminal activity, money laundering or terrorism financing, victims seeking to make payment could potentially breach AML and CFT regulations, especially where the attacker is tied to known criminal organisations.

Countries are considering the need to revisit their approach to ransomware payments, such as introducing guidelines balancing victims' urgent need to resolve cyber-attacks with the need for compliance with international AML/CFT standards. This could include developing a legal framework requiring businesses to report such incidents without facing penalties, mirroring the Australian regime of requiring organisations to disclose ransomware payments. Conversely, Singapore could mandate that organisations procure cyber-insurance and prohibit the coverage of claims for ransomware payments, with the hope that organisations are deterred from making such payments if the money comes out of their pockets. This also may thwart threat actors' attempts to identify soft targets likely to make payments.

Improving Cybersecurity Initiatives

The Singapore government has made significant efforts to expand on and further develop Singapore's cybersecurity infrastructure in light of the evolving cyber threat landscape.

The Cybersecurity (Amendment) Act 2024, which passed in May 2024, introduced sever-

al changes to the Cybersecurity Act 2018 (the “Act”) although it has yet to come into force.

Changes to the CII regime

Key amendments include:

- widening the ambit of the Act to cover virtual computers, in light of the increasing reliance on cloud technology;
- broadening the CSA’s jurisdiction to monitor and regulate certain offshore computers where the owner is in Singapore and where the computers would be regulated as CII if they were located at least partly in Singapore;
- expanding the incident reporting duties of CII owners to include threats to their supply chain or of any incidents where their supply chain has been affected; and
- regulating the providers of essential services, where those services are provided on digital infrastructure owned by third parties.

Designation of STCCs, ESCIs and major FDIs

Furthermore, the Act will regulate new entities and systems.

First, computers may be designated as systems of temporary cybersecurity concern (STCC) where there is a high risk of a cybersecurity risk or threat against it, and where any harm against it will have serious detrimental effects. This enables the CSA to monitor the cybersecurity of key computers which may be more attractive to threat actors, such as the systems implemented to facilitate the distribution of during the COVID-19 pandemic. STCCs will be regulated similarly to CIIs.

Secondly, certain organisations may be designated as entities of special cybersecurity interest (ESCI) if they store sensitive information or use a computer to perform a function, where the

disruption of the computer will have a significant detrimental effect on key interests like foreign relations, the economy or public health, such as Singapore’s autonomous universities. However, ESCIs will be subject to less stringent regulatory requirements than CIIs.

Thirdly, entities which provide cloud computing services and/or data centre facility services may be designated major foundational digital infrastructure (“major FDI”) service providers if they provide FDI services (in Singapore or outside Singapore, if the offshore FDI service is provided to persons within Singapore), and any impediment to the provision of the FDI service would likely disrupt or affect the operation of many organisations in Singapore which utilise that FDI.

The amendments will reinforce Singapore’s cybersecurity framework, enabling the authorities to proactively survey the threat landscape and to take the necessary steps to counter adverse outcomes.

Parliament has also announced that it is studying the possibility of introducing a new Digital Infrastructure Act, a piece of legislation complementary to the Cybersecurity Act 2018 that focuses on related aspects of cybersecurity and digital infrastructure. The proposed law is envisaged to focus more broadly on the governance, regulation and protection of key digital infrastructure, as large cloud service providers and data centres are crucial to the smooth operations of a variety of digital services that organisations and consumers use daily (see [here](#) and [here](#)).

Importance of constantly re-assessing cyber-readiness

The importance of continually updating cyber-related laws to keep abreast of a myriad of potential threats was further highlighted by the global

CrowdStrike outage in July 2024. The incident affected several businesses and caused a variety of service disruptions, including significant delays affecting more than 100 flights at Changi airport. While the outage was reported to be the result of an innocuous software update and most affected services recovered in a day, its effects were far-reaching and caused wide-spread chaos. The resulting harms placed a spotlight on the importance of cyber-resilience across all segments of Singapore's infrastructure, since threat actors targeting cyber-infrastructure may attempt to cripple critical functions which can cause catastrophic downstream effects.

Organisations must continually assess their cybersecurity frameworks and develop robust contingency plans and remediation frameworks to safeguard the continuity of business operations and remedy the cause of cyber-incidents as quickly as possible. The government is committed to working with private organisations, providing key support and guidance for organisations to build up their cyber-resilience. Such government initiatives include SingCERT's advisory on building digital resiliency, the practical resources and financial assistance offered by the Ministry of Digital Development and Information to encourage robust IT practices and the CSA's cybersecurity toolkits.

Introduction of MAS Notices on cyber considerations

The Monetary Authority of Singapore (MAS) has also released notices and guidelines promoting responsible cyber-management, including Notices on Cyber Hygiene and Notices on Technology Risk Management.

The Notices on Cyber Hygiene outline mandatory requirements for entities and individuals providing financial services, such as operators of

designated payment services, merchant banks and insurance agents. With a focus on cyber hygiene, the Notices require compliance with best practices like the application of appropriate security patches, the enactment and implementation of adequate security standards, the implementation of malware protection and the execution of multi-factor authentication.

Similarly, the Notices on Technology Risk Management oblige financial service providers to make all reasonable efforts to maintain high availability for their critical systems, such that the maximum unscheduled downtime for each critical system does not exceed a total of four hours within any period of 12 months. The service provider must establish a recovery time objective not exceeding four hours for each critical system and must notify MAS within an hour of the discovery of an IT security incident which significantly impacts the provider's operations or services.

With the heightened risks of cybersecurity threats to Singapore's financial infrastructure, the identification of and strict adherence to best practices will enable entities to adapt to and better manage emerging risks. Given the importance of safeguarding Singapore's reputation as a financial hub, it is imperative that all stakeholders work cohesively to maintain the trust of customers and investors.

Considerations Regarding the Use of AI Increase in AI-powered cyber-attacks

Threat actors are increasingly harnessing AI to enhance the sophistication and effectiveness of their cyber-attacks. By utilising machine learning algorithms, scammers and hackers can automate the discovery of system vulnerabilities, bypass security measures, and launch more targeted attacks, AI tools can be used to craft highly personalised phishing emails or elaborate

deepfakes that are more likely to deceive victims and cause significant losses. For example, an employee of a multinational company operating in Hong Kong was duped into transferring approximately USD25.5 million to scammers, when he was misled after taking part in a video call that criminals set up using deepfakes of several members of staff, including the company's chief financial officer.

Additionally, attackers may exploit AI to launch brute-force attacks on passwords or encryption protocols, cracking them by rapidly predicting potential combinations at a much faster rate. As AI technology continues to evolve, attackers employing AI are staying one step ahead of traditional cybersecurity defences, making it increasingly difficult for organisations to detect and defend against threats. This underscores the need for organisations to implement stronger defence mechanisms, such as harnessing AI in the protective measures to counter AI-enhanced threats.

Encouraging Robust Cybersecurity of AI Systems

As Singapore invests more heavily in AI initiatives and develops its AI capabilities, the increasing reliance on AI systems across multiple sectors might incentivise threat actors to attack AI systems directly or use the AI systems as a springboard to launch their offensives. The CSA has published the Guidelines on Securing Artificial Intelligence Systems (the "Guidelines") to provide systems owners with a useful framework through which to plan the cybersecurity of their AI systems.

The Guidelines warn against defensive measures focusing on overly siloed aspects of the lifecycle of an AI system (the "AI lifecycle"), with such an approach being insufficient to establish

a holistic defensive framework against threat actors. Instead, the Guidelines provide key considerations to bear in mind when systems owners establish security frameworks. The key considerations are derived from the following five stages spanning the AI lifecycle.

- Planning and design: potential systems owners should not adopt AI systems without first obtaining an understanding of the risks of doing so, and the choice to adopt an AI system must be followed by raising awareness and competency amongst all personnel.
- Development: to prevent the distortion of an AI system's operation, systems owners should secure the supply chain feeding their AI system and implement processes to identify, track and protect AI-related assets from threat actors.
- Deployment: when rolling out AI systems into their organisations, systems owners should take steps to safeguard the propriety of their AI system.
- Operations and maintenance: once AI systems have been rolled out, systems owners should continually monitor the functions and operations of their systems to ensure that the inputs to and outputs from the AI systems are safeguarded.
- End of life: system owners should comply with all legal regulations and industry standards/practices when decommissioning their AI systems, such as destroying or disposing of data repositories from which their AI models were trained or operated.

While AI presents a new frontier of opportunities for entities, threat actors may be inclined to direct their threats towards AI systems. Singapore is quickly establishing itself as a global AI heavyweight, but as AI adoption rates increase, so should organisations secure their AI systems

for Singapore to cement its status as a technological leader.

Conclusion

Singapore has witnessed significant advancements and challenges in its cybersecurity landscape. The integration of AI and other technological advancements have dramatically scaled the sophistication and complexity of potential cyber threats. The inability of traditional cyber defences to protect against the ever-growing threat landscape highlights the need for enhanced threat detection and response. Singapore must continually assess and, where necessary, improve its existing measures to fortify its cybersecurity framework. Moving forward, the government must continue to foster increased collaboration and dialogue between stakeholders, including government agencies, private organisations and other international stakeholders. Developing a forward-looking approach to cyber-readiness will therefore be crucial to securing Singapore's cyber defence against the growing arsenal of AI-powered threats.

SWEDEN



Law and Practice

Contributed by:

Anders Bergsten and Victoria Nordenberg
Mannheimer Swartling

Contents

1. General Overview of Laws and Regulators p.254

- 1.1 Cybersecurity Regulation Strategy p.254
- 1.2 Cybersecurity Laws p.254
- 1.3 Cybersecurity Regulators p.256

2. Critical Infrastructure Cybersecurity p.257

- 2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.257
- 2.2 Critical Infrastructure Cybersecurity Requirements p.258
- 2.3 Incident Response and Notification Obligations p.258
- 2.4 State Responsibilities and Obligations p.259

3. Financial Sector Operational Resilience Regulation p.259

- 3.1 Scope of Financial Sector Operational Resilience Regulation p.259
- 3.2 ICT Service Provider Contractual Requirements p.259
- 3.3 Key Operational Resilience Obligations p.260
- 3.4 Operational Resilience Enforcement p.261
- 3.5 International Data Transfers p.261
- 3.6 Threat-Led Penetration Testing p.261

4. Cyber-Resilience p.262

- 4.1 Cyber-Resilience Legislation p.262
- 4.2 Key Obligations Under Legislation p.262

5. Security Certification for ICT Products, Services and Processes p.263

- 5.1 Key Cybersecurity Certification Legislation p.263

6. Cybersecurity in Other Regulations p.263

- 6.1 Cybersecurity and Data Protection p.263
- 6.2 Cybersecurity and AI p.264
- 6.3 Cybersecurity in the Healthcare Sector p.265

Mannheimer Swartling is the largest law firm in the Nordics and is a leading adviser in the premium segment for business law in Sweden. Its full-service practice is unique for Sweden in that the lawyers have a high degree of specialisation. The firm can therefore cover all the specialist advice needs of its clients – of any size or complexity – in-house. The corporate commercial team consists of 75 lawyers based in Stockholm, Gothenburg and Malmö. The team regularly acts on large IT procurements and out-

sourcings where complex cybersecurity issues arise. Cybersecurity matters within digitalisation projects, online currencies and collaboration agreements are also frequently handled by the team. Another strength is data protection mandates ranging from GDPR compliance to data breaches. Clients also benefit from the team's close collaboration with the M&A department to assist with technology-related set-ups. Clients from the healthcare, automotive and technology sectors mandate Mannheimer Swartling.

Authors



Anders Bergsten is a member of Mannheimer Swartling's corporate, tech and IP practice group, and is based in Stockholm. He advises clients on a wide range of national and international commercial matters, focused on the IT and technology area. Anders' practice consists mainly of advising on complex delivery, outsourcing and procurement projects, together with advising on cybersecurity, protective security, digital compliance and personal data matters. Anders joined the firm in 2006 and is a member of the Swedish Bar Association. He has an LLM degree from the University of Uppsala and has studied law at the University of Sydney.



Victoria Nordenberg is a member of Mannheimer Swartling's corporate, tech and IP practice group. She advises Swedish and international clients across a wide range of industries, with a particular focus on societal functions and critical infrastructure. Victoria has extensive experience in drafting and negotiating IT contracts, outsourcing agreements and other complex commercial agreements. In addition, Victoria has significant experience working with cybersecurity and digital communications regulation. Victoria joined the firm in 2016 and is a member of the Swedish Bar Association. She holds an LLM degree from the University of Uppsala.

Mannheimer Swartling Advokatbyrå AB

Norrlandsgatan 21
111 43
Stockholm
Sweden

Tel: +46 859 506 000
Fax: +46 859 506 001
Email: felicity.trocme@msa.se
Web: www.mannheimerswartling.se



**MANNHEIMER
SWARTLING**

1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

Sweden's approach to cybersecurity regulation is characterised by a diverse array of legal frameworks tailored to the specific needs and risks of each sector. Historically, this sectoral approach has allowed for targeted cybersecurity measures that address the unique challenges faced by different industries.

In response to the deteriorating global security landscape and increasing digitalisation, Sweden has initiated several new measures to strengthen its cybersecurity posture and take a more comprehensive approach to cybersecurity. A key development is the formulation of a strategy that addresses the country's foreign and security policy in relation to cyber and digital issues. The main focus of Sweden's cybersecurity strategy and efforts is to prevent cyberattacks and build resilience against them. This includes protecting critical infrastructure and sensitive information while ensuring that the country can recover and adapt quickly in the face of cyber threats. By improving resilience, Sweden aims to maintain

the integrity and security of its digital environment, thereby safeguarding its national interests and the well-being of its citizens.

Overall, Sweden aims to address transnational cyber threats more effectively and improve its overall resilience through regulation and by working with international partners, particularly within the European Union and NATO, with a focus on protecting national interests and promoting global security.

1.2 Cybersecurity Laws

- The Electronic Communications Act (*Lag (2022:482) om elektronisk kommunikation*) and the Electronic Communications Regulation (*Förordning (2022:511) om elektronisk kommunikation*) transpose the Directive of the European Parliament and of the Council (2018/1972) of 11 December 2018 establishing the European Electronic Communications Code (recast). The act and the regulation regulate electronic communications, with a focus on the security and integrity of networks and services. They ensure that communication providers implement measures to protect against cybersecurity threats.

- The Accounting Act (*Bokföringslagen* (1999:1078)) contains provisions on the secure handling and storage of financial data, which is crucial for cybersecurity in financial reporting.
- The Camera Surveillance Act (*Kamerabevakningslagen* (2018:1200)) regulates camera surveillance, balancing security needs with privacy rights, and ensuring that surveillance systems are secure against unauthorised access.
- The Protective Security Act (*Säkerhetsskyddslagen* (2018:585)) and the Protective Security Regulation (*Säkerhetsskyddsförordningen* (2021:955)) focus on protective security, and require organisations to protect information that concerns security-sensitive activities from cyber threats, thus playing an important role in the broader cybersecurity framework.
- The Information Security for Critical and Digital Services Act (*Lag* (2018:1174) *om informationssäkerhet för samhällsviktiga och digitala tjänster*) and the Information Security for Critical and Digital Services Regulation (*Förordning* (2018:1175) *om informationssäkerhet för samhällsviktiga och digitala tjänster*) transpose Directive of the European Parliament and of the Council (2016/1148) of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. The act and the regulation impose obligations on operators of essential services and digital service providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. See **2 Critical Infrastructure Cybersecurity**.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), sets the standard for data protection and privacy in the EU, and requires organisations to implement robust security measures to protect personal data. The Data Protection Act containing supplementary provisions to the GDPR (*Lag* (2018:218) *med kompletterande bestämmelser till EU:s dataskyddsförordning*) complements the GDPR by providing additional national rules for data protection in Sweden, ensuring comprehensive data security. See **6.1 Cybersecurity and Data Protection**.
- The Patient Data Act (*Patientdatalag* (2008:355)) and the Patient Data Regulation (*Patientdataförordning* (2008:360)) complement the GDPR and include regulations for handling personal data in the healthcare sector.
- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA) aims to enhance digital operational resilience within the financial sector by setting uniform requirements across the EU. See **3 Financial Sector Operational Resilience Regulation**.
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (“Cybersecurity Act”) establishes the European Union Agency for Cybersecurity (ENISA) and a framework for cybersecurity certification of ICT products, see **5.1 Key Cybersecurity Certification Legislation**.

- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (“AI Act”) establishes rules for artificial intelligence, including security requirements for AI systems, to ensure they are safe and trustworthy. See **6.2 Cybersecurity and AI**.
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (“eIDAS Regulation”) governs electronic identification and trust services, ensuring secure electronic transactions across the EU and setting the standards for secure electronic signatures and transactions.

1.3 Cybersecurity Regulators

- The Electronic Communications Act and the Electronic Communications Regulation: The Swedish Post and Telecom Authority (PTS) is the supervisory authority of these laws. PTS ensures that communication providers maintain the security and integrity of their networks and services. Its scope includes supervision of communication providers.
- The Accounting Act: The Swedish Accounting Standards Board (BFN) is the supervisory authority, focusing on the secure handling and storage of financial data. Although primarily concerned with accounting practices, BFN’s role includes ensuring that financial data is protected against unauthorised access.
- The Camera Surveillance Act: The Swedish Authority for Privacy Protection (IMY) is the

supervisory authority under this act, balancing security needs with privacy rights. The supervision shall ensure that surveillance systems are secure against unauthorised access, protecting individuals’ privacy while allowing for necessary security measures.

- The Protective Security Act and the Protective Security Regulation: The supervisory mandate is divided up according to the sector in which the supervised entity (referred to as “the operator”) is active, and the following authorities are sharing the mandate: the Swedish Security Service, the Swedish Armed Forces, the Authority for Swedish Transmission System, the Swedish Transport Agency, PTS, the Swedish Defence Materiel Administration, the Swedish Financial Supervisory Authority, the Swedish Energy Agency, the Swedish Radiation Safety Authority, and the County Administrative Boards in Stockholm, Skåne, Västra Götaland and Norrbotten. The supervision shall ensure that the operators fulfil the obligations imposed and focus on protection of security sensitive activities from cyber threats. Their role is critical in safeguarding national security and ensuring the protection of critical infrastructure.
- The Information Security for Essential and Digital Services Act and the Information Security for Essential and Digital Services Regulation: The Swedish Civil Contingencies Agency (MSB) is the primary regulator, acting as a co-ordinator among sector-specific regulators and a national contact point in the EU co-operation regarding NIS. See **2 Critical Infrastructure Cybersecurity**.
- GDPR and the Data Protection Act: The Swedish Authority for Privacy Protection has the supervision mandate in Sweden. The Swedish Authority for Privacy Protection ensures that organisations implement robust security measures to protect personal data.

Their authority covers all personal data processing activities within Sweden.

- The Patient Data Act and the Patient Data Regulation: The Swedish Authority for Privacy Protection is the supervisory authority that supervises the application of data protection rules by healthcare providers, which means, for example, checking that healthcare providers take security measures to protect patient data.
- DORA: The Swedish Financial Supervisory Authority is the supervisory authority that ensures that financial entities comply with DORA.
- The Cybersecurity Act: The ENISA is the key regulator for this regulation. ENISA develops cybersecurity certification frameworks to enhance trust and security in the digital market. Their authority covers ICT products and services across the EU, promoting a common approach to cybersecurity certification.
- The AI Act: The European Commission also oversees this regulation, establishing rules for artificial intelligence systems. The AI Act includes security requirements to ensure AI systems are safe and trustworthy, which are integral to cybersecurity. Its scope covers AI systems and applications throughout the EU.
- The eIDAS Regulation: In Sweden, the Swedish Agency for Digital Government is responsible for implementing this regulation. The Swedish Agency for Digital Government oversees electronic identification and trust services, ensuring secure electronic transactions.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

Note that when Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2) is transposed into Swedish law, it will replace the current regulations.

Scope of Application

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS) was implemented in Sweden through the Act on Information Security for Critical and Digital Services and the Regulation on Information Security for Critical and Digital Services. The legislation entered into force on 1 August 2018. The purpose of the legislation is to enhance the security level of network and information systems for digital services and essential services within certain sectors. Operators covered by the regulatory framework are categorised into:

- operators of essential services, and
- digital service providers.

Operators of Essential Services

Operators of essential services exist in both private and public sectors. An operator of essential services is defined as an entity that:

- provides a service crucial for maintaining critical societal or economic activities within one of the seven sectors listed below:
 - (a) energy;

- (b) transport;
- (c) banking;
- (d) financial market infrastructure;
- (e) healthcare;
- (f) drinking water supply and distribution; or
- (g) digital infrastructure;
- the provision of such service depends on network and information systems; and
- an incident would cause a significant disruption in the provision of the service.

Digital Service Providers

Digital service providers exist in both private and public sectors. A digital service provider is defined as an entity that:

- has its main establishment in Sweden;
- has an annual turnover exceeding EUR10 million; and
- has 50 or more employees.

2.2 Critical Infrastructure Cybersecurity Requirements

Obligations for Operators of Essential Services

An operator of essential services shall:

- conduct systematic and risk-based information security work concerning the network and information systems used to deliver the essential services;
- conduct a risk analysis that will serve as the basis for selecting security measures;
- implement appropriate and proportionate technical and organisational measures to manage risks threatening the security of the network and information systems used to provide the essential services; and
- take appropriate measures to prevent and minimise the impact of incidents affecting the network and information systems used to provide the essential services.

Obligations for Providers of Digital Services

A provider of digital services shall:

- implement the technical and organisational measures considered appropriate and proportionate to address risks threatening the security of the networks and information systems used in the provision of digital services within the European Union; such measures should ensure a level of security in the network and information systems that is appropriate to the risk; and
- take measures to prevent and minimise the impact of incidents affecting the network and information systems used; these measures should aim at ensuring the continuity of services.

2.3 Incident Response and Notification Obligations

Notification Requirements

Operators of essential services and providers of digital services are required to report any incidents that occur. This contributes to creating a comprehensive view of the incident situation, enables warnings to others, and facilitates any necessary co-ordinated efforts.

Reports are submitted to the Swedish Civil Contingencies Agency, which has a co-ordinating role for the Information Security for Critical and Digital Services Act, which forwards the reports to the respective supervisory authority. The Swedish Civil Contingencies Agency has announced regulations and general advice on incident reporting for providers of essential services.

The Swedish Post and Telecom Authority is the supervisory authority for providers of digital services.

The following authorities are, for the specified sectors, the supervisory authority for operators of essential services:

- Swedish Energy Agency: energy;
- Swedish Transport Agency: transport;
- Swedish Financial Supervisory Authority: banking;
- Swedish Financial Supervisory Authority: financial market infrastructure;
- Health and Social Care Inspectorate: health-care;
- Swedish Food Agency: drinking water supply and distribution; and
- Swedish Post and Telecom Authority: digital infrastructure.

2.4 State Responsibilities and Obligations

CERT-SE is Sweden's national CSIRT (Computer Security Incident Response Team) tasked with supporting society in managing and preventing IT incidents. CERT-SE is part of the Swedish Civil Contingencies Agency, which helps integrate their efforts into the broader national security framework.

CERT-SE's responsibilities include providing assistance and guidance to the public sector, private companies, and organisations in handling cybersecurity threats and incidents. They aim to enhance the overall cybersecurity posture by offering expertise, co-ordinating responses to incidents, and promoting best practices for IT security.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

In Sweden, the scope of financial sector operational resilience regulation is primarily governed by DORA. This regulation applies to a wide range of financial entities, including (but not limited to) banks, credit institutions, payment institutions, insurance companies, and alternative investment fund managers. DORA aims to enhance digital operational resilience by setting uniform requirements across the EU, and it is directly applicable in Sweden, requiring national legislation to complement it. The regulation excludes certain small entities and those covered by specific exemptions.

3.2 ICT Service Provider Contractual Requirements

Contractual Requirements

Under the framework of DORA, contractual requirements for ICT service providers include clear terms on service levels, security measures, data protection, incident management, and termination rights. Contracts must also include provisions for audit rights and access to information necessary for the financial institution to comply with its regulatory obligations under DORA.

ICT Service Providers

In Sweden, under the framework of DORA, "ICT service providers" are defined broadly to encompass entities that offer information and communication technology services to financial institutions. These include a wide range of services such as cloud computing, data analytics, software development, and cybersecurity services. The definition is intended to cover any third-party service that could impact the operational resilience of financial entities.

Critical ICT Services

Not all ICT services are classified as critical. The classification of an ICT service as critical depends on several factors, such as the systemic impact of a failure in providing the ICT services, the reliance of financial entities, the degree of substitutability and other relevant factors. While the definition of ICT service providers in Sweden is broad, the classification of services as critical is specific and based on the potential impact on financial operations and stability.

Cloud Service Providers

Not every cloud service provider will automatically be classified as critical. The criticality of a cloud service provider is assessed based on the same criteria mentioned above. For instance:

- If a cloud service provider supports a significant portion of a financial entity's operations or hosts critical applications, it may be classified as critical.
- Cloud service providers offering infrastructure as a service (IaaS) or platform as a service (PaaS) that are integral to the financial entity's operations are more likely to be considered critical compared to those offering less essential services.

3.3 Key Operational Resilience Obligations

Objectives

The Swedish implementation of DORA is designed to ensure that financial entities can withstand, respond to, and recover from ICT-related disruptions, thereby enhancing their resilience. It also seeks to establish a unified framework for managing ICT risks across the financial sector, standardising risk management practices. By improving incident response, the regulation ensures that financial entities can respond to ICT incidents in a timely and effective manner, minimising their impact. Additionally, the regulation facilitates supervision by enabling effective oversight by regulatory authorities to ensure compliance and resilience.

Key Obligations

Financial entities are required to implement comprehensive ICT risk management frameworks, which include regular risk assessments and mitigation strategies. They must also manage risks associated with ICT service providers, ensuring that contracts include necessary provisions for resilience and security. Regular testing and monitoring of digital operational resilience are required, including threat-led penetration testing for critical entities. Furthermore, clear governance structures for ICT risk management must be established, with defined roles and responsibilities.

Incident and Reporting Obligations

Financial entities must classify ICT-related incidents based on their impact and severity. Significant incidents must be reported to the Swedish Financial Supervisory Authority within a specified timeframe, typically within 24 to 72 hours, depending on the severity. Reports should include details such as the nature of the incident, its impact, and the measures taken to address it. Entities are also required to conduct a post-incident analysis to identify root causes and implement measures to prevent recurrence. In certain cases, entities may be required to disclose incidents to the public, especially if they have a significant impact on customers or the financial system. It should be noted that entities that carry out operations covered by both DORA and the Protective Security Act must adhere to both in case of incidents, and that the incident reporting under DORA needs to take the obligations under the Protective Security Act into

consideration (which may curb the ability of an entity to report certain information under DORA).

3.4 Operational Resilience Enforcement Enforcement in Regard to Critical ICT Service Providers

The supervision of critical ICT service providers is to be carried out at Union level by the Lead Overseer. One of the three European Supervisory Authorities (European Banking Authority, European Securities and Markets Authority or European Insurance and Occupational Pensions Authority) is to be designated as Lead Overseer for each of the critical third-party service providers. In order to fulfil its tasks under DORA, the Lead Overseer may, inter alia, conduct general investigations and inspections. Within three months of the conclusion of an investigation or an inspection, the Lead Overseer shall adopt recommendations addressed to the critical third-party provider.

The Lead Overseer can impose a periodic penalty payment on the critical ICT service providers. Decisions on periodic penalty payments taken by the Lead Overseer should therefore be enforceable under the Swedish Enforcement Code (*Utsökningsbalken (1981:774)*) in the same way as a Swedish judgment that has acquired legal force. The Swedish Enforcement Authority (*Kronofogden*) is the Swedish authority that will be responsible for the practical enforcement and its decisions can be appealed to the Swedish court.

Enforcement in Regard to Financial Entities

In regard to financial entities, the enforcement of operational resilience obligations is carried out by the Swedish Financial Supervisory Authority. The authority has the power to conduct inspections, request information, and impose sanctions or corrective measures on financial institutions

and critical ICT service providers that fail to comply with operational resilience requirements. This includes fines, orders to cease certain activities, or other regulatory actions to ensure compliance.

3.5 International Data Transfers

There is no applicable information in this jurisdiction.

3.6 Threat-Led Penetration Testing

In Sweden, DORA mandates threat-led penetration testing (TLPT) for financial entities. These tests must be conducted every three years, or more frequently if required by the competent authority. The tests simulate cyber-attacks to identify vulnerabilities in an organisation's ICT infrastructure.

The tests must be executed by an external party every third time, while internal testers can be used but require specific approval and must meet conflict-of-interest requirements. The Swedish authorities, primarily the Swedish Financial Supervisory Authority and the Swedish Central Bank, share responsibilities for the TLPT process. The Swedish Financial Supervisory Authority determines which entities must undergo testing and the frequency of tests, while the Swedish Central Bank co-ordinates and monitors the tests, ensuring compliance and certifying that the tests meet the required standards. After completing the tests, entities must submit results, corrective action plans, and receive certification. This certification facilitates mutual recognition of tests across EU member states.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

The EU Cyber Resilience Act

On 10 December 2024, Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (“Cyber Resilience Act”) entered into force.

Implementation Timeline

Although the Cyber Resilience Act took effect on 10 December 2024, its full implementation is phased across three key dates: The main obligations introduced by the Cyber Resilience Act will apply from 11 December 2027, with the exception of Article 14 which will apply from 11 September 2026 and Chapter IV (Articles 35-51) which will apply from 11 June 2026.

The Inquiry Stage

On 28 November 2024, the Swedish government appointed an inquiry chair who will analyse the need for and propose measures and supplementary legislative provisions necessary to adapt Swedish law to the Cyber Resilience Act.

The work consists, inter alia, of identifying which provisions in Swedish legislation are affected by the Cyber Resilience Act and analysing whether they need to be repealed or amended, or if new provisions are needed as a result of the Cyber Resilience Act.

The investigator will, in particular:

- propose which existing authority or authorities should be designated as the national market surveillance authority;
- propose which existing authority should be designated as the notifying authority respon-

sible for, among other things, establishing and implementing the procedures necessary for the assessment, designation, and notification of conformity assessment bodies; and

- make any other proposals, including legislative proposals, that are necessary or otherwise deemed appropriate to complement the Cyber Resilience Act.

The inquiry chair has to present its proposals in a report no later than 15 December 2025.

4.2 Key Obligations Under Legislation

Scope of Application

The Cyber Resilience Act applies to “products with digital elements” whose purpose or use involves a logical or physical data connection to a device or network.

The Cyber Resilience Act covers a wide range of software and hardware products that connect, either directly or indirectly, to other devices or networks. This includes smart home devices, wearable technology, internet-connected toys, and industrial Internet of Things (IoT) devices. Non-commercial open-source software products are not covered by the Cyber Resilience Act. The Cyber Resilience Act targets manufacturers, producers, and importers, requiring them to ensure that their products are safe to use, resilient to cyber threats, and that their security features are properly disclosed.

Objectives

The Cyber Resilience Act establishes compulsory cybersecurity standards for products with digital components available in the EU market.

Its primary objectives are to:

- improve the cybersecurity of digital products, from the design and development phase and throughout the whole life cycle;
- protect consumers and businesses against the risks posed by inadequate cybersecurity measures;
- encourage manufacturers to incorporate security by design throughout the digital product life cycle; and
- supplement existing cybersecurity regulations, including the NIS2 and DORA.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

The Cybersecurity Act

The Cybersecurity Act entered into force on 27 June 2019. The primary goal of the Cybersecurity Act is to enhance protection against cybersecurity threats across the EU. The Cybersecurity Act also enables manufacturers and service providers to use one mutually recognised certificate throughout the EU.

Main Elements

The regulation has two main functions and purposes:

- to give the EU Agency for Network and Information Security a permanent mandate, more resources and new tasks; and
- to create a framework for certifying cybersecurity products and services; this framework sets up a system to govern the issuance of European cybersecurity certificates and declarations of conformity with security standards for ICT products, services, and pro-

cesses, and the purpose of the certification is to guarantee that users are provided with adequate information regarding the relevant cybersecurity features.

National Cybersecurity Certification Authority

In Sweden, the Swedish Defence Materiel Administration acts as the national cybersecurity certification authority. It is the cybersecurity and certification department at the Swedish Defence Materiel Administration that is responsible for matters related to cybersecurity certification, supervision, collaboration, and external monitoring. The department consists of the Swedish Certification Body for IT Security and the Swedish Cyber Security Certification Authority.

Furthermore, the Swedish Defence Materiel Administration is tasked with overseeing and coordinating certification activities at the national level and collaborating with EU entities such as the EU Agency for Network and Information Security and the European Commission. It also serves as Sweden's representative in the European Cybersecurity Certification Group.

Additionally, the Swedish Defence Materiel Administration is responsible for notifying the EU about accredited bodies and those authorised under the Cybersecurity Act.

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection GDPR and Swedish Supplementation

The GDPR aims to protect natural persons when processing personal data. In Sweden, the GDPR is supplemented by the Data Protection Act, which contains supplementary provisions to the GDPR.

Controller Responsibilities and Data Processing Agreements

A legal entity that determines the purposes and means of processing personal data is a controller under the GDPR. While a controller can appoint a processor to process data on its behalf, the ultimate responsibility for compliance remains with the controller. To ensure the processor adheres to GDPR requirements, the parties must enter into a data processing agreement that governs the processing activities and outlines both parties' obligations and rights.

Protective Measures and Data Subject's Rights

The GDPR requires controllers to implement appropriate technical and organisational measures to protect the processed personal data from unauthorised access. The appropriate measures should be determined based on the risk of the processing. This may include:

- pseudonymisation and encryption of personal data;
- ensuring ongoing confidentiality, integrity, availability, and resilience;
- ensuring data restoration; and
- regularly testing, assessing, and evaluating measures.

The controller must also inform data subjects about the processing of their personal data and of their rights. The data subject's rights include:

- right to access personal data and information;
- right to rectification;
- right to erasure;
- right to restriction of processing;
- right to data portability; and
- right to object.

Data Breach

Entities processing personal data must adhere to the GDPR's specific provisions regarding personal data breaches. A personal data breach involves a security incident resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.

If a breach risks individuals' rights and freedoms, the controller must notify the Swedish Authority for Privacy Protection within 72 hours of awareness.

The notification shall at least include a description of:

- the nature of the breach;
- the likely consequences of the breach;
- the measures taken or proposed to mitigate the consequences of the breach; and
- contact information for further inquiries.

If a breach likely poses a high risk to individuals' rights and freedoms, the data subject should generally be informed. All breaches must be documented by the controller, regardless of risk level.

However, it should be noted that the Data Protection Act stipulates that if an incident that constitutes a personal data breach is to be notified under the Protective Security Act, the notification and information obligations under Articles 33 and 34 of the GDPR shall not be applicable.

6.2 Cybersecurity and AI

The Swedish government has launched an inquiry to evaluate the need for national adjustments in response to the AI Act. The inquiry will recommend necessary legal changes and

measures for transparency and oversight, with the final report due by 30 September 2025.

The AI Act, effective from 1 August 2024, establishes a unified framework for AI development and use within the EU. It categorises AI systems based on risk levels, imposing stricter requirements on high-risk applications, such as those in critical infrastructure, healthcare, and law enforcement. For Sweden, this means adapting national regulations to comply with EU standards, ensuring AI systems are human-centred, reliable, and aligned with fundamental rights. This includes mechanisms for oversight and enforcement to maintain high protection levels for health, safety, and fundamental rights.

The AI Act imposes obligations primarily on AI providers, developers, and commercial users to ensure compliance with its standards. Such obligations include:

- classifying AI systems by risk levels, with stricter requirements for high-risk applications;
- ensuring AI systems are transparent and understandable to users;
- implementing mechanisms for oversight and accountability;
- meeting safety standards; and
- ensuring high-quality data management and protection.

6.3 Cybersecurity in the Healthcare Sector

The Patient Data Act and the Patient Data Regulation

The healthcare sector must systematically address the security of healthcare information management. Cybersecurity in healthcare focuses on safeguarding electronic information and assets against unauthorised access, use, and disclosure.

The Patient Data Act contains explicit provisions to prevent unauthorised dissemination by electronic means of data relating to patients undergoing treatment. It contains the provisions specifically needed for the processing of patient data by healthcare providers in relation to other personal data processing. Otherwise, the provisions of the GDPR apply to the processing of patient data and other personal data by healthcare providers. The Patient Data Act governs several aspects, including:

- the ability of healthcare personnel involved in a patient's care to access necessary medical records, even if those records were created by a different healthcare organisation;
- the regulations determining which individuals are permitted to access patient data as part of their duties within the healthcare system; and
- the patient's right to restrict access to information in their medical records within an electronic records system.

Trends and Developments

Contributed by:

Anders Bergsten and Victoria Nordenberg
Mannheimer Swartling

Mannheimer Swartling is the largest law firm in the Nordics and is a leading adviser in the premium segment for business law in Sweden. Its full-service practice is unique for Sweden in that the lawyers have a high degree of specialisation. The firm can therefore cover all the specialist advice needs of its clients – of any size or complexity – in-house. The corporate commercial team consists of 75 lawyers based in Stockholm, Gothenburg and Malmö. The team regularly acts on large IT procurements and out-

sourcings where complex cybersecurity issues arise. Cybersecurity matters within digitalisation projects, online currencies and collaboration agreements are also frequently handled by the team. Another strength is data protection mandates ranging from GDPR compliance to data breaches. Clients also benefit from the team's close collaboration with the M&A department to assist with technology-related set-ups. Clients from the healthcare, automotive and technology sectors mandate Mannheimer Swartling.

Authors



Anders Bergsten is a member of Mannheimer Swartling's corporate, tech and IP practice group, and is based in Stockholm. He advises clients on a wide range of national and

international commercial matters, focused on the IT and technology area. Anders' practice consists mainly of advising on complex delivery, outsourcing and procurement projects, together with advising on cybersecurity, protective security, digital compliance and personal data matters. Anders joined the firm in 2006 and is a member of the Swedish Bar Association. He has an LL.M degree from the University of Uppsala and has studied law at the University of Sydney.



Victoria Nordenberg is a member of Mannheimer Swartling's corporate, tech and IP practice group. She advises Swedish and international clients across a wide range of

industries, with a particular focus on societal functions and critical infrastructure. Victoria has extensive experience in drafting and negotiating IT contracts, outsourcing agreements and other complex commercial agreements. In addition, Victoria has significant experience working with cybersecurity and digital communications regulation. Victoria joined the firm in 2016 and is a member of the Swedish Bar Association. She holds an LL.M degree from the University of Uppsala.

Mannheimer Swartling Advokatbyrå AB

Norrlandsgatan 21
111 43
Stockholm
Sweden

Tel: +46 859 506 000
Fax: +46 859 506 001
Email: felicity.trocme@msa.se
Web: www.mannheimerswartling.se



**MANNHEIMER
SWARTLING**

Digitalisation and Cyber-Attacks

Sweden is a leading nation in the research and development of new technologies, with digitalisation at the heart of its progress. However, the deteriorating global security landscape has increased the risk of cyber-attacks, which makes highly digitised countries extra vulnerable. Like in many other countries, both public and private entities in Sweden are repeatedly targeted by cyber-attacks from foreign powers (either state actors or threat actors acting with the tacit acceptance from host nations). Consequently, the ability to effectively manage these cyber threats is crucial for Swedish organisations, leading to an increased need for robust protection against such attacks. This has led to an increased need for robust protection against cyber-attacks.

In Sweden, cyber threats manifest themselves in various forms, including intelligence threats from foreign powers and criminal activities targeting companies. These threats often involve tactics such as phishing, password attacks, malware and attacks on mobile devices and email systems. As cyber-attacks continue to evolve and become more sophisticated, it is imperative for

every organisation to regularly ensure that its defences remain robust and effective. Protection against cyber-attacks is particularly important for organisations that provide essential societal functions and manage critical IT systems. The direct and indirect costs of cyber-attacks on such operations are estimated to be in the billions of Swedish kronor yearly.

It should be noted that the Swedish regulatory environment concerning cybersecurity has not entirely kept pace with the swift deterioration in the global security landscape, together with the adoption of many EU initiatives. To a certain extent, this has led to a somewhat fragmented regulatory picture – eg, in relation to supervisory authorities and notification obligations in case of incidents caused by cyber-attacks.

Extended Applicability

In the past, the legal obligations to meet certain cybersecurity requirements have been directed at public authorities, whereas now the regulatory framework will require substantial security measures from a much broader group of organisations, including private companies. In 2019, the applicability of the Protective Secu-

rity Act (*Säkerhetsskyddslagen* (2018:585)) was extended from public entities to all types of entities whose operations are of importance to Sweden's security. Similarly, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2) and Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER), which will be transposed into Swedish law later this year, will apply to both private and public entities and will require extensive cybersecurity measures to be taken.

Increased Sanctions

With the increased focus on cybersecurity and security measures, one of the tools that legislators are using to enforce the importance of cybersecurity is to increase sanctions. This tool has been used in relation to both NIS2 and CER, where an operator that fails to comply with NIS2 or CER can be fined up to the higher of 2% of its total worldwide annual turnover in the preceding financial year or EUR10,000,000.

In order to create a common basis and applicability, the Swedish government's official report on the transposition of CER into Swedish law, SOU 2024:64, proposes that a failure to comply with the Protective Security Act is prohibited in a similar manner, and the proposal is to increase the sanction to the greater of SEK120,000,000 (approximately EUR12,000,000) or 2% of the operator's total annual global turnover from the previous financial year.

National Cybersecurity Centre

Due to the increased focus on cybersecurity in Sweden, the Swedish Armed Forces, the National Defence Radio Establishment, the Swedish Civil Contingencies Agency and the Swedish Security Service, launched the National Cybersecurity Centre in December 2020 with the mission to strengthen Sweden's overall ability to prevent, detect and manage cyber threats. From November 2024, the National Cybersecurity Centre is part of the National Defence Radio Establishment, which coincides with the government raising its ambitions for the centre.

The NCSC is responsible for strengthening Sweden's cybersecurity and is now expected to expand its responsibilities. These new responsibilities include acting as a central body to co-ordinate and support national cybersecurity efforts. This involves monitoring and analysing cyber threats, providing advice and support to both public and private organisations, and promoting information sharing and collaboration among various cybersecurity stakeholders. The NCSC will also improve the ability to analyse and assess cyberthreats, vulnerabilities and other risks regarding information- and cybersecurity.

Common Level of Security Measures Within the Union

Sweden is not the only EU member state that has an increased focus on cybersecurity. The EU is adopting several robust regulatory frameworks that require comprehensive security measures, some of which are expected to be transposed to binding Swedish law during 2025 and some of which Swedish entities should monitor during the year.

NIS2

The NIS2 directive was adopted by the EU in December 2022, repealing and replacing Direc-

tive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

The directive aims to harmonise and strengthen cybersecurity in the Union. It sets out requirements for technical, operational and organisational measures to manage risks that threaten the security of network and information systems. These measures should include risk analysis, business continuity measures, supply chain security measures and personnel security measures. The measures should be based on an overall risk perspective and risk analysis and be proportionate to the risk. They should be evaluated and include specific elements, including supply chain security. Supply chain security covers security aspects relating to the links between each operator and its direct suppliers or service providers. This means that each operator must take risk management measures in relation to its suppliers and is therefore responsible for its direct suppliers.

In addition, NIS2 requires policies and procedures to assess the effectiveness of cybersecurity risk management measures and to address any deficiencies. NIS2 also requires senior management to monitor the implementation of risk management measures.

In the event of an incident that has a significant impact on an entity's ability to provide its services, the directive requires the entity to notify the competent authority of the incident. If deemed appropriate, service recipients should also be informed of the incident. An incident is considered significant if it causes, or has the potential to cause, severe operational disruption to services, results in financial losses for the entity, or

has, or could have, an impact on other natural or legal persons by causing considerable damage.

As proposed in the Swedish government's official report 2024:18, NIS2 will be implemented in Sweden through the Swedish Cybersecurity Act (*cybersäkerhetslagen*) (the "Swedish Cybersecurity Act") and the Swedish Cybersecurity Regulation (*förordning om cybersäkerhet*), which will replace the current Act on Information Security for Critical and Digital Services (*lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster*) and the Regulation on Information Security for Critical and Digital Services (*förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster*). The government has not yet proposed a bill, but it is expected to do so in the spring of 2025. As NIS2 should have been implemented in the member states by 18 October 2024, and Sweden is already behind, it is expected that the time between the bill being passed and it coming into force will be short.

Once the Act comes into force, clarifying regulations will be issued by the designated authorities and only then will the detailed requirements for affected entities be clear. It has not yet been decided which authorities will be responsible for the regulations.

CER

To enhance the EU's resilience in critical infrastructure, the EU has adopted a directive aimed at ensuring that essential services can effectively prevent, withstand, and manage disruptions or interruptions in their operations. The CER is proposed to be transposed in Sweden through the Critical Operators Resilience Act (*lag om motståndskraft hos kritiska verksamhetsutövare*) and the Critical Operators Resilience Regulation (*förordning om motståndskraft hos kritiska*

verksamhetsutöväre) as described in the Swedish government's official report 2024:64. The government has not yet proposed a bill, but it is expected to do so in the spring of 2025.

Once transposed, there will be an increase in cybersecurity requirements, and other related measures, for critical entities in Sweden as the Directive replaces the previous Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, which was more limited in scope.

The CER applies to critical entities providing services in the following sectors:

- energy;
- transport;
- banking;
- financial market infrastructure;
- health;
- drinking water;
- waste water;
- digital infrastructure;
- public administration;
- space; and
- production, processing and distribution of food.

Each EU member state must list all essential services within each sector and conduct a risk assessment based on the list. Following the risk assessment, each EU member state will determine which entities are considered critical entities within each sector.

For an entity to be considered a critical entity in Sweden, the following is required:

- the entity must provide an essential service;

- the entity must operate in Sweden and have its critical infrastructure in Sweden; and
- an incident affecting the entity must significantly disrupt its ability to deliver its essential services or impact other essential services within the sectors covered by the law.

Once identified, a critical entity must perform a critical entity risk assessment. The assessment aims to identify any relevant risks associated with the delivery of the essential service and consider interdependencies with other sectors covered by the law. Based on the risk assessment, the critical entities must implement appropriate and proportionate technical, security and organisational measures to ensure resilience. These measures include preventing incidents, ensuring physical protection, mitigating the consequences of incidents, and recovering from them. Further, a critical entity must also report incidents that have or may have significant disruption to the competent authority without undue delay.

CRA Act

The Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (CRA) was adopted in the EU on 10 December 2024 and will enter into full force on 11 December 2027. However, certain parts of the CRA will enter into force during 2026.

The objective of the CRA is to strengthen EU cybersecurity and ensure cyber resilience by establishing a legal framework for essential cybersecurity requirements for digital elements in the EU. This will be implemented through restrictions on the development of secure products with digital elements to ensure that prod-

ucts in the EU are less vulnerable and more secure throughout their life cycle. The CRA also aims to improve transparency regarding the support period for products.

The CRA does not require transposition into Swedish law and will be directly applicable in Sweden when it enters into force, but additional provisions and adjustments to existing provisions may be necessary. These possible provisional additions and adjustments are currently being examined.

AI Act

As Europe becomes more digitised, the use of artificial intelligence is becoming more widespread. As a result, the EU has adopted Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (“AI Act”).

The AI Act entered into force on 1 August 2024 and will be fully applicable two years later, on 2 August 2026, with certain exceptions including prohibitions and obligations relating to AI competencies that entered into force on 2 February 2025 and governance rules and obligations for general-purpose AI models that will apply from 2 August 2025.

The AI Act aims to create a coherent framework for the development and use of AI systems across the Union. It promotes human-centred and trustworthy AI while ensuring a high level of protection for health, safety and fundamental rights. The AI Act prohibits certain uses of AI, while other uses are restricted depending on the risk level of the AI application. If an AI system is classified as high risk, it must have an appropriate level of accuracy, robustness and cybersecurity.

The AI Act constitutes Swedish law but requires complementary national provisions. These complementary provisions are currently under review and are expected to include proposed provisions for the following:

- the establishment of a system for market surveillance, market monitoring, compliance management; and
- other necessary national adaptations resulting from the AI Act.

SWITZERLAND



Law and Practice

Contributed by:

Hugh Reeves, Jürg Schneider and David Vasella
Walder Wyss Ltd

Contents

1. General Overview of Laws and Regulators p.275

- 1.1 Cybersecurity Regulation Strategy p.275
- 1.2 Cybersecurity Laws p.275
- 1.3 Cybersecurity Regulators p.277

2. Critical Infrastructure Cybersecurity p.279

- 2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.279
- 2.2 Critical Infrastructure Cybersecurity Requirements p.279
- 2.3 Incident Response and Notification Obligations p.279
- 2.4 State Responsibilities and Obligations p.279

3. Financial Sector Operational Resilience Regulation p.279

- 3.1 Scope of Financial Sector Operational Resilience Regulation p.279
- 3.2 ICT Service Provider Contractual Requirements p.280
- 3.3 Key Operational Resilience Obligations p.280
- 3.4 Operational Resilience Enforcement p.281
- 3.5 International Data Transfers p.281
- 3.6 Threat-Led Penetration Testing p.282

4. Cyber-Resilience p.283

- 4.1 Cyber-Resilience Legislation p.283
- 4.2 Key Obligations Under Legislation p.283

5. Security Certification for ICT Products, Services and Processes p.283

- 5.1 Key Cybersecurity Certification Legislation p.283

6. Cybersecurity in Other Regulations p.283

- 6.1 Cybersecurity and Data Protection p.283
- 6.2 Cybersecurity and AI p.284
- 6.3 Cybersecurity in the Healthcare Sector p.285

Walder Wyss Ltd was established in Zurich in 1972 and has since grown at record speed. Today, the firm has about 300 legal experts and approximately 150 support staff in six offices in Switzerland's economic centres. It is an agile firm that is approachable, adapts to clients quickly and does not hide behind formality. Because it is fully integrated, partners bring in those people who have the greatest expertise

and are best-suited for a particular task. This helps avoid silos and ensures that work is carried out efficiently. Walder Wyss was the first large Swiss firm to strongly focus on tech, including data protection. The firm has one of the largest and most experienced teams in this area and advises clients in all sectors on Swiss data law, including technology, privacy, AI and IT.

Authors



Hugh Reeves is a partner in the regulated markets, competition, tech and IP team at Walder Wyss. He advises clients on technology transactions, commercial contracts,

telecommunications, intellectual property and digitalisation. Hugh is active in the areas of data protection and e-commerce and assists clients with their entry or expansion into the Swiss market.



Jürg Schneider is a partner in the regulated markets, competition, tech and IP team at Walder Wyss. His practice areas include information technology, data protection and outsourcing.

Jürg has deep and extensive experience in the fields of data protection, information security and e-commerce, with a particular focus on transborder and international contexts. His competencies regarding data protection include drawing up data protection concepts and strategies for companies, leading and assisting compliance projects regarding implementation of privacy legislation for Swiss and international companies, and advising clients in regulated sectors (banking, insurance, healthcare, etc) on data protection requirements as well as cybersecurity.



David Vasella is a partner in the information technology, intellectual property and competition team. He advises Swiss and international companies and authorities on

questions concerning data and technology law.

David specialises in data use, data and technology-related contracts, data security matters, cloud projects, data protection compliance and artificial intelligence. He regularly gives talks and writes publications, for example on datenrecht.ch, a Swiss platform on data law. He is a certified information privacy professional and manager (CIPP/E, CIPM), fellow of information privacy (FIP) and AI governance professional (AIGP).

Walder Wyss Ltd

Seefeldstrasse 123
8008 Zurich
Switzerland

Tel: +41 586 585 858
Fax: +41 586 585 959
Email: reception@walderwyss.com
Web: www.walderwyss.com

walderwyss attorneys at law

1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

Switzerland is a federation comprising 26 federated states (cantons) as well as a federal government. This leads to a layered body of laws as well as, at times, a decentralised official cybersecurity approach. Cybersecurity in Switzerland remains closely tied to the area of data protection. Cybersecurity is frequently perceived as an off-shoot – or even a synonym – of data security, which, as the name suggests, targets the security and resilience of data processing and storage activities.

A further manifestation of the government's interest in cybersecurity is another governmental venture, the Digital Switzerland Strategy. The Digital Switzerland Strategy sets guidelines for Switzerland's digital transformation, and is updated annually by the Swiss Federal Council, each time with three focus topics. It is binding on the federal administration and provides guidance for other stakeholders involved in digitalisation. The first Digital Switzerland Strategy was published in 2016, and updates arrived in 2018, 2020 and 2023. On 13 December 2024, the Swiss Federal Council adopted the updated Digital Switzerland Strategy for 2025, with a focus on cybersecurity, the Swiss approach to the regulation of AI systems and the use of AI systems in the federal administration.

In 2023, the Swiss Federal Council approved the new Digital Administration Switzerland Strategy 2024–27, which defines the fields of action to be prioritised in order for the Confederation, the cantons, and cities and municipalities to jointly determine how the digital transformation of administrations is to be driven forward. A second strategy approved by the Swiss Federal Council

is the Digital Federal Administration Strategy, which creates a framework for digital transformation projects in the federal administration.

1.2 Cybersecurity Laws

On a federal level, the Swiss Constitution of 18 April 1999 protects the right to privacy, in particular the right to be protected against misuse of personal data (Article 13). The collection and use of personal data by private bodies are regulated at the federal level and are mainly governed by the Swiss Data Protection Act (the Federal Act on Data Protection; FADP) and its ordinances, including the Data Protection Ordinance (DPO).

Data processing by public bodies is governed by the FADP for federal bodies, which includes private organisations performing public tasks such as health insurance providers, pension funds and many others, and by cantonal (for example, the Information and Data Protection Act of the Canton of Zurich) and communal laws for cantonal and communal bodies.

The FADP was revised in order to implement the revised Council of Europe's Convention 108, and to more closely align with the EU General Data Protection Regulation (GDPR). The revised FADP and DPO entered into force on 1 September 2023.

While the FADP and the GDPR are similar in their approach and purpose, there are notable differences. For example, there is a data breach notification obligation under the FADP, similar to that under the GDPR, but the trigger for notifying a personal data breach to the Swiss data protection authority, the Federal Data Protection and Information Commissioner (FDPIC), is "high risk", whereas, under the GDPR, any relevant risk requires notification. On 6 February 2025, the FDPIC published non-binding guidance on

breach notification obligations under the FADP. Another key difference is the level of activity by the relevant authorities: while many supervisory authorities within the European Economic Area (EEA) are more active, providing guidance and/or enforcing the GDPR, the FDPIC is generally reluctant to take a decisive stance and rarely provides guidance for private actors. However, the FDPIC has initiated several investigations under the revised FADP.

The FADP and the DPO provide for a general requirement to ensure an appropriate level of data security in relation to personally identifiable information. The revised FADP calls for state-of-the-art data security measures, without specifying specific technical standards. However, a specific security requirement is the obligation to keep logs to ensure that data operations are logged by federal authorities and private actors that process sensitive data on a large scale or carry out “high-risk profiling”, a form of profiling that leads to personality profiles. These logs must be relatively granular and must be kept for at least one year, separately from the productive environment. In addition, the revised legislation imposes on controllers and processors, under certain conditions, a duty to notify data security breaches to the FDPIC, and potentially to data subjects. Additional compliance and documentation measures, such as data protection impact assessments and records of processing activities, as well as an obligation to maintain processing regulations, have also been introduced.

The Information Security Act (ISA) of 18 December 2020, which entered into force on 1 January 2024, governs information security practices within the federal government and its administrative bodies. Under the ISA, several ordinances further specify and implement information security requirements and also repeal (inter alia) the

Ordinance on the Protection against Cyber Risks in the Federal Administration (CyRV). Importantly, a significant feature of the ISA is the introduction of a reporting obligation for cyber-attacks for public authorities such as universities; federal, cantonal and municipal agencies; inter-cantonal, cantonal and intercommunal organisations; and providers of critical infrastructures, for example in the energy, finance, healthcare, insurance, transport, communication and IT sectors. In-scope organisations must report cyber-attacks to the National Cyber Security Centre (NCSC) within 24 hours, where the relevant thresholds and definitions are met. This obligation will come into force on 1 April 2025.

Apart from the ISA, cybersecurity remains mostly regulated by a patchwork of various acts and regulatory guidance, which deal explicitly or implicitly with cybersecurity in the private sector. These laws include:

- the Budapest Convention on Cybercrime (CCC), which entered into force in Switzerland on 1 January 2012 and imposes a harmonisation of Switzerland's criminal legislation as well as speedy international co-operation mechanisms;
- the FADP;
- the Federal Telecommunications Act (TCA) of 30 April 1997, including its ordinances, which – as of 1 January 2023 – contain specific information security and network threat resilience requirements; and
- the Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (FinMia) of 19 June 2015 – the banking and financial markets legislation also led the financial markets regulator, namely the Swiss Financial Market Supervisory Authority (FINMA), to issue various circulars and regulatory notices.

However, the Swiss government has given cybersecurity increasing attention in the past few years, and the absence of an overarching ad hoc law on cybersecurity may appear misleading given the importance and national relevance of this topic. Nonetheless, this conclusion is unlikely to lead the Swiss legislator (Parliament) to issue any additional topical legislation on cybersecurity in the near future. On the contrary, the federal government has been following the National Strategy for the Protection of Switzerland against Cyber Risks (NCS).

The NCS was last updated in April 2023. The strategy sets out the objectives and measures with which the federal government and the cantons, together with the business community and universities, intend to counter cyberthreats. A steering committee has been established to plan and co-ordinate the implementation of the strategy. The revised NCS builds on the previous strategies, adding content and precision. It defines 17 measures, each contributing to five strategic objectives, namely:

- self-empowerment (Switzerland is to expand its position as one of the world's leading knowledge, education and innovation locations in cybersecurity);
- securing digital services and infrastructures (Switzerland is to implement measures to strengthen cyber-resilience);
- ensuring effective detection, prevention, management and defence against cyber-incidents (Switzerland is to ensure the capacities and organisational structures needed to quickly identify cyberthreats and incidents, and minimise damage, are in place);
- combating and prosecuting cybercrime effectively (Switzerland is to expand its ability to identify and prosecute threat actors); and

- maintaining a leading role in international co-operation (Switzerland is to foster an open, free and secure cyberspace and compliance with international law in the digital space).

However, the NCS does not foresee the implementation of a dedicated cybersecurity legislation, instead focusing on modernising various pre-existing laws. The updated NCS is testament to the continued growth in relevance of cybersecurity in Switzerland, as well as perhaps the increased global threat posed by cyber-risks.

1.3 Cybersecurity Regulators

The FDPIC is a body established at the federal level under the FADP. The FDPIC supervises compliance with the FADP and other federal data protection legislation by federal bodies and advises private bodies. On its own initiative, or at the request of a third party, the FDPIC may carry out investigations into data processing by private bodies. In addition, each canton has its own data protection authority, which is generally competent to supervise cantonal and communal bodies (but not private parties, which are subject to the FDPIC's authority). Other regulators – for example, FINMA – may play a role in the enforcement of data protection (see the following).

It is also worth mentioning here that the key official actor in the cybersecurity area is the NCSC, which is now integrated into the new Federal Office for Cybersecurity (BACS) within the Federal Department of Defence, Civil Protection and Sport (DDPS). Indeed, in an effort to centralise the administrative activities in this area, other actors such as the Reporting and Analysis Centre for Information Assurance (MELANI), GovCert and the Cybercrime Coordination Unit (CYCO) became an integral part of the NCSC and now BACS. Tasks include raising public awareness, receiving reports on cyber-incidents and sup-

porting operators of critical infrastructures in managing these incidents. Protection of the federal administration against cyber-attacks is now a key task of a new specialist unit within the new State Secretariat for Security Policy (Sepos), also within the DDPS.

The FADP does not provide an official role for NGOs and self-regulatory organisations (SROs). Such organisations would not, for example, have a right to bring a civil claim against a company perceived to be in breach of privacy laws. However, there are a number of organisations that promote privacy, including several consumer protection organisations, although they do not perform these tasks on the basis of a legal mandate.

The NCSC – now part of BACS – is the key official actor in the cybersecurity area. GovCERT.ch, whose parent organisation is the NCSC, is the computer emergency response team (CERT) for Switzerland. Its tasks include supporting the critical IT infrastructure in Switzerland in dealing with cyberthreats. It maintains close relationships with other CERT organisations, thereby seeking to promote the exchange of cyberthreat-related information. Furthermore, the FDPIC retains strong prerogatives given the absence of standalone cybersecurity legislation.

Given the federal system in Switzerland, it should also be borne in mind that other cantonal and inter-cantonal bodies serve the purpose of information sharing. This is notably the case for the inter-cantonal Swiss Criminality Prevention Service (the SKP and PSC under its German or French and Italian acronyms, respectively). This service seeks to facilitate inter-cantonal police co-ordination as well as crime prevention measures.

FINMA is the competent authority in the banking and financial sectors. As part of its statutory mission, and in the course of supervising regulated financial entities, FINMA may also request compliance with applicable data protection and data security regulations.

The Federal Office of Communications (OFCOM) is the federal office responsible for the proper implementation of the legal and technical requirements in the communications realm and plays a particularly important role in the area of telecommunications. In the area of unfair competition, the State Secretariat for Economic Affairs (SECO) acts for the Swiss Confederation in civil and criminal proceedings if matters of public interest are at stake.

In addition, the following authorities may also be competent, albeit indirectly, in the cybersecurity area:

- the Federal Office of Civil Aviation (in case of safety-related data breaches in the aviation sector);
- the Federal Nuclear Safety Inspectorate (in case of sector-related data breaches);
- the Federal Department of the Environment, Transport, Energy and Communications (DETEC), especially in regard to the national railway industry; and
- Swissmedic, which receives notifications of serious incidents that can include incidents relating to software as a medical device.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

A breach notification obligation in cases of cybersecurity incidents affecting critical infrastructures will come into force on 1 April 2025. Moreover, the Federal Office for National Economic Supply (FONES) published a minimum information and communication technology (ICT) standard document as well as an ICT self-assessment tool directed at operators of critical infrastructures. This document rests, in part, on the requirements of the relatively ubiquitous National Institute of Standards and Technology (NIST) framework to which it refers.

2.2 Critical Infrastructure Cybersecurity Requirements

Concerning critical infrastructure cybersecurity requirements, see **2.1 Scope of Critical Infrastructure Cybersecurity Regulation**.

2.3 Incident Response and Notification Obligations

Concerning incident response and notification obligations, see **2.1 Scope of Critical Infrastructure Cybersecurity Regulation**.

2.4 State Responsibilities and Obligations

Concerning state responsibilities and obligations, see **2.1 Scope of Critical Infrastructure Cybersecurity Regulation**.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

FINMA, as the financial market supervisory authority, frequently adopts and adapts various circulars and notices. In particular, FINMA Circular 2008/21 and its recent replacement (entering into effect on 1 January 2024), Circular 2023/01 Operational Risks and Resilience – Banks, are central to all banks' cybersecurity practices laying out principles and guidelines on proper risk management in relation to client-identifying data (CID). FINMA Circular 2018/3 on Outsourcing by Banks and Insurers is another essential text as it contains rules on the security of data in an outsourcing context.

In the banking and financial markets sector, the regulator, FINMA, supervises the relevant actors (namely banks, insurance companies, financial institutions, collective investment schemes and fund management companies) and plays a role in the cybersecurity realm. Indeed, given the importance of the financial industry in Switzerland, data security and cybersecurity are core concerns. FINMA publishes an annual risk monitor as an overview of risks seen as particularly significant, and the 2023 version highlights that cyber-risks remain one of the biggest operational risks and notes a trend towards malware attacks targeting external service providers.

FINMA has also revised its circular, with the updated version, Circular 2023/1 Operational Risks and Resilience – Banks, coming into force on 1 January 2024. It requires banks and investment firms to report certain cyber-attacks within 24 hours of becoming aware of them and to submit a full report within 72 hours.

In case of a breach of the sectoral rules, FINMA has a varied toolbox of enforcement measures. These include the revocation of licences to practice, fines or even custodial sentences. FINMA also occasionally, and for preventative purposes, relies on a “naming and shaming” strategy, meaning that the perpetrator of any offence against the regulatory rules is publicly named.

3.2 ICT Service Provider Contractual Requirements

As mentioned in **2.1 Scope of Critical Infrastructure Cybersecurity Regulation**, a breach notification obligation in cases of cybersecurity incidents affecting critical infrastructures will come into force on 1 April 2025. Moreover, FONES published a minimum ICT standard document as well as an ICT self-assessment tool directed at operators of critical infrastructures. This document rests, in part, on the requirements of the relatively ubiquitous NIST framework to which it refers.

3.3 Key Operational Resilience Obligations

Concerning key operational resilience obligations, see also **1.1 Cybersecurity Regulation Strategy** and **1.2 Cybersecurity Laws**. On 7 June 2024, FINMA published supervisory guidance 03/2024 on cyber-risks, which includes:

- findings from FINMA’s cyber-risk supervision, including deep dives at banks;
- information on scenario-based cyber-exercises in accordance with Circular 2023/1 Operational Risks and Resilience; and
- clarifications of FINMA Guidance 05/2020 on the reporting requirement for cyber-attacks.

The clarifications relate to the reporting obligation under Article 29(2) of the Financial Market Supervision Act, which requires supervised

institutions to report certain material incidents to FINMA. It builds on earlier FINMA guidance, Guidance 03/24 and Guidance 05/2020. FINMA clarifies its expectations as follows.

Deadline for Reporting

FINMA confirms that the relevant institution has 24 hours from the moment a cyber-attack is discovered to report to FINMA (see the following for information about the commencement of this window). Within these initial 24 hours, the institution must carry out an initial assessment of the criticality, with the aim of assessing whether the cyber-attack requires a report to FINMA. The “actual” report must then be made within 72 hours via FINMA’s survey and application platform (EHP).

Expectations for the Initial Report

FINMA states that timeliness is of the essence for the initial report. There are no specific expectations in terms of form or content, and initial reports can also be withdrawn later.

The initial report may be made informally, for example by e-mail or telephone. The aim is to reflect the then-known facts on the basis of the initial assessment. It may, of course, be the case that further clarifications show that the initial report would not have been mandatory. Institutions can therefore withdraw their initial reports at any time, giving them an incentive to err on the side of caution.

If an institution is also subject to the reporting requirement under the ISA, as revised (with the relevant parts coming into force on 1 April 2025), the initial report can be submitted through the relevant authority, the BACS. To the extent known, the BACS will forward the report to FINMA – if the reporting institution chooses this option – automatically and without filtering, so

presumably immediately. The actual report must then continue to be submitted via the EHP.

Expectations for the Actual Report

FINMA Guidance 05/2020 requires a final root cause report for reports of cyber-attacks with a severity level of “medium” or more, which at a minimum contains the internal or external investigation or forensic report (further requirements can be found in FINMA [Guidance 05/2020](#)). As FINMA has now clarified, the root cause report should include the following aspects for the “high” and “serious” severity levels:

- the reason for the success of the cyber-attack;
- the impact of the attack on compliance with regulatory requirements, the institution’s operations and its clients; and
- the mitigating measures introduced to address the effects of the attack.

For cyber-attacks categorised as “serious”, evidence and analyses of the crisis organisation’s ability to function must be included in the submission.

Calculation of Deadlines

FINMA has confirmed its existing practice: where an attack is detected by an outsourcing provider to the institution, the 24-hour window starts when the provider becomes aware of the attack, shortening the time left for the institution, in order to treat institutions that have not outsourced any functions equally to others.

When calculating the deadlines for the initial report and follow-up reports, only official banking days count. An exception applies to attacks with the “serious” severity level. In this case, the deadline for the initial report also applies outside of banking days. FINMA must be interpreted

here as meaning that this does not apply to the deadline for the follow-up report.

It should be noted that FINMA did not formally align its guidance with the EU Digital Operational Resilience Act (DORA) or its level II and level III legislation, although they are similar in several regards.

3.4 Operational Resilience Enforcement

Concerning operational resilience enforcement, see **1.1 Cybersecurity Regulation Strategy** and **1.2 Cybersecurity Laws**.

3.5 International Data Transfers

The FADP aims to protect the personality rights and fundamental rights of natural persons whose personal data is processed. As a consequence, the FADP contains provisions on how this protection is to be guaranteed when data is transferred abroad, for instance to a state that does not offer the same level of data protection as Switzerland.

Controllers or processors may transfer personal data abroad if the Swiss Federal Council has determined that the legislation of the relevant state or international body guarantees an adequate level of protection. Therefore, the Swiss Federal Council determines, in a binding manner, to which countries the export of data is permitted.

On the other hand, in the absence of such a decision by the Swiss Federal Council, personal data may be disclosed abroad only if appropriate protection is guaranteed. Thus, at least one of the following conditions must be fulfilled:

- an international treaty;
- data protection provisions of a contract between the controller or the processor and

its contracting partner, which were communicated beforehand to the FDPIC;

- specific safeguards prepared by the competent federal body and communicated beforehand to the FDPIC;
- standard data protection clauses previously approved, established or recognised by the FDPIC; and
- binding corporate rules (BCRs) on data protection that were previously approved by the FDPIC, or by a foreign authority that is responsible for data protection and belongs to a state that guarantees adequate protection.

Mechanisms or Derogations That Apply to International Data Transfers

The FADP provides that personal data may not be disclosed abroad if this would seriously endanger the personality of the data subjects. Such a serious threat to the personality rights of the data subjects may arise if the exporting state does not have legislation that guarantees an adequate level of data protection. However, a transfer of data to such a state may be permitted if one of the foregoing conditions is fulfilled.

Regarding the standard contractual clauses (SCCs) published by the EU Commission, the FDPIC formally recognised the SCCs for international transfers from Switzerland to third states, but only if certain changes are agreed to account for Swiss law (and the fact that Switzerland is not an EEA member state).

For data transfers subject to the GDPR only, the non-amended SCCs may be used. Therefore, the parties should determine whether only the FADP or both the FADP and the GDPR apply to the transfer in question.

The EU SCCs require a “transfer impact assessment” (TIA). This also applies to Swiss companies if they use the EU SCCs (under the GDPR as well as under the FADP). As part of a TIA, the Swiss data exporter must check in each specific case whether the laws of the recipient country regarding official access in the recipient country (eg, for the purpose of national security or criminal prosecution) and the rights of the data subjects are compatible with Swiss data protection law and Swiss constitutional principles.

In addition, Switzerland has recently implemented the Swiss-US Data Protection Framework (DPF). It remains to be seen if the DPF will stand, and for now, many companies opt to use the SCCs in addition to relying on the DPF.

Finally, the FDPIC has pointed out that internal company data protection regulations – ie, BCRs, cannot be a substitute for the conclusion of a SCC if transfers are made outside of a group of companies subject to the BCRs.

3.6 Threat-Led Penetration Testing

Swiss legislation does not currently provide for threat-led penetration testing (TLPT) requirements, except that FINMA expects banks and securities dealers to carry out regular penetration testing (per its Circular 2023/1 Operational Risks). In addition, Swiss financial entities may be subject to DORA requirements if they operate within the EU or have connections with EU-based financial institutions or their clients. Likewise, Swiss companies affiliated with EU financial entities that provide intra-group ICT services to their EU counterparts are also covered by DORA for these activities. Furthermore, DORA applies to Swiss ICT service providers as soon as they plan to offer their services to relevant financial entities within the EU. Finally, although Swiss data protection legislation does

not expressly call for penetration testing, it can be mandatory to the extent it is a minimum security requirement in specific circumstances.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

Concerning cyber-resilience legislation, see **1.1 Cybersecurity Regulation Strategy** and **1.2 Cybersecurity Laws**.

4.2 Key Obligations Under Legislation

Concerning key obligations under legislation, see **1.1 Cybersecurity Regulation Strategy** and **1.2 Cybersecurity Laws**.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

The FADP regulates the issue of certification in Article 13. Software and system suppliers, as well as data controllers and their subcontractors, can have their products validated by an independent, accredited body. These certifications attest to their compliance with the requirements of the FADP.

In addition to ensuring compliance with data protection standards, these certifications offer a number of advantages. According to Article 22(5) of the FADP, a data controller who adheres to a code of conduct or holds a certification may be exempted from carrying out an otherwise-required data protection impact assessment. These certifications can also be used as a basis for authorising data transfers abroad, even when the recipient country does not offer a level of data protection deemed adequate (Article 12 of

the DPO). However, certification mechanisms have so far been little used in Swiss law.

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

Concerning cybersecurity and data protection, see also **1.1 Laws**. The only truly overarching body of laws is the federal legislation on data protection, namely the FADP and its implementing ordinances, in particular the DPO. The FADP and the DPO contain provisions on data security, but the Swiss legislator relies on a technologically neutral approach, with the result that these rules on data security remain rather abstract and do not refer to any specific technology, or any specific standard or technical requirement, except for the obligation to keep logs of certain higher-risk processing activities. Under the FADP, an intentional failure to implement certain minimum technical and organisational measures may incur liability for a criminal fine against the responsible individuals of up to CHF250,000, although there is a debate as to whether there are any binding minimum measures.

The ISA of 18 December 2020, which entered into force on 1 January 2024, governs information security practices within the federal government and its administrative bodies. Under the ISA, several ordinances further specify and implement information security requirements and also repeal (inter alia) the CyRV. Importantly, a significant feature of the ISA is the introduction of a reporting obligation for cyber-attacks for public authorities such as universities; federal, cantonal and municipal agencies; inter-cantonal, cantonal and intercommunal organisations; and providers of critical infrastructures, for example in the energy, finance, healthcare, insurance,

transport, communication and IT sectors. In-scope organisations must report cyber-attacks to the NCSC within 24 hours, where the relevant thresholds and definitions are met. This obligation will come into force on 1 April 2025.

As a more general consideration, the policy discussions in Switzerland in recent years have shown that cybersecurity is progressively evolving from what once was a purely technical consideration into a mainstream legal topic. Cybersecurity is now not only part of the legal discussions surrounding data protection and data security (in various areas, such as finance and telecommunications), but is also a focus of other branches of the law, such as insurance law.

Moreover, the policy discussions at the federal level are not expected to lead, in the short term, to any overarching cybersecurity law. However, the topic remains highly dynamic and strongly dependent on international developments. Given Switzerland's size and geographical location, prompt legal developments in the area of cybersecurity are a real possibility.

6.2 Cybersecurity and AI

Concerning cybersecurity and AI, see also **6.1 Cybersecurity and Data Protection**. In Switzerland, there is currently no overarching regulation on the use of AI.

The FDPIC has published statements and non-binding guidelines on how to address data protection matters in these areas. For example, the FDPIC pointed out that the FADP is directly applicable to AI-based data processing, and the FDPIC expects manufacturers, providers and users of AI systems to ensure transparency concerning the purpose, functionality, and data sources of AI-based processing.

Further, sector-specific regulations address particular data protection issues. For example, the Swiss government has also created a general frame of reference for the use of AI within the federal administration, and FINMA issued binding guidelines on outsourcing and data security for the financial and insurance sector.

The following FADP safeguards can be applied to AI systems.

- **Privacy by design/privacy by default:** The data controller is obliged to implement technical and organisational measures to ensure that processing complies with data protection requirements right from the outset.
- **Obligation to carry out an impact assessment:** Where the planned processing is likely to pose a high risk to data subjects or their fundamental rights, the data controller must first carry out a data protection impact analysis. A high risk exists in particular in the case of large-scale processing of sensitive data or systematic surveillance of large parts of the public domain.
- **Transparency obligation for automated decisions:** The data controller must inform the data subject of any decision taken exclusively on the basis of automated personal data processing that has legal effects on the data subject or significantly affects him or her. The data subject also has the right to express his or her point of view and to demand that the decision be reviewed by a natural person. These measures do not apply where the data subject has expressly consented to the decision being taken by automated means, or where the decision is directly related to the conclusion or performance of a contract and the data subject's request is met. If the automated decision is made by a federal body, such body must qualify it as such. The

right of the data subject to express his or her point of view and to demand that the decision be reviewed by a natural person does not apply when the data subject does not have to be heard before the decision is made. When exercising his or her right of access, the data subject receives, in particular, information concerning the existence of an automated decision and the logic on which the decision is based.

- Requirement for a formal legal basis: Federal bodies are only entitled to process personal data if a legal basis is given. The legal basis must be laid down in a law in the formal sense in three cases, namely (i) the processing of sensitive data (for example biometric and genetic data); (ii) profiling (as defined by the FADP); and (iii) when the purpose or method of processing is likely to cause serious harm to the fundamental rights of the data subject. The use of AI may therefore require a formal legal basis, even in the absence of sensitive data or profiling, if the processing method (eg, automated decision) is likely to seriously affect the fundamental rights of the data subject.

Finally, on 12 February 2025, DETEC and the Federal Department of Foreign Affairs (FDFA) presented an overview to the Swiss Federal Council of possible regulatory approaches to AI. On the basis of this overview, the Swiss Federal Council has decided on a Swiss regulatory approach for AI based on three objectives: strengthening Switzerland's location for innovation; safeguarding the protection of fundamental rights, including economic freedom; and increasing public trust in AI. To achieve these objectives, the Swiss Federal Council has set the following key steps for the future: incorporation of the Council of Europe's AI Convention into Swiss law; sector-specific legislation as far as required (cross-sector regulation, to be limited to central areas relevant to fundamental rights); and non-binding measures.

6.3 Cybersecurity in the Healthcare Sector

Concerning cybersecurity in the healthcare sector, see **6.1 Cybersecurity and Data Protection**.

Trends and Developments

Contributed by:

Hugh Reeves, Jürg Schneider and David Vasella
Walder Wyss Ltd

Walder Wyss Ltd was established in Zurich in 1972 and has since grown at record speed. Today, the firm has about 300 legal experts and approximately 150 support staff in six offices in Switzerland's economic centres. It is an agile firm that is approachable, adapts to clients quickly and does not hide behind formality. Because it is fully integrated, partners bring in those people who have the greatest expertise

and are best-suited for a particular task. This helps avoid silos and ensures that work is carried out efficiently. Walder Wyss was the first large Swiss firm to strongly focus on tech, including data protection. The firm has one of the largest and most experienced teams in this area and advises clients in all sectors on Swiss data law, including technology, privacy, AI and IT.

Authors



Hugh Reeves is a partner in the regulated markets, competition, tech and IP team at Walder Wyss. He advises clients on technology transactions, commercial contracts,

telecommunications, intellectual property and digitalisation. Hugh is active in the areas of data protection and e-commerce and assists clients with their entry or expansion into the Swiss market.



Jürg Schneider is a partner in the regulated markets, competition, tech and IP team at Walder Wyss. His practice areas include information technology, data protection and outsourcing.

Jürg has deep and extensive experience in the fields of data protection, information security and e-commerce, with a particular focus on transborder and international contexts. His competencies regarding data protection include drawing up data protection concepts and strategies for companies, leading and assisting compliance projects regarding implementation of privacy legislation for Swiss and international companies, and advising clients in regulated sectors (banking, insurance, healthcare, etc) on data protection requirements as well as cybersecurity.

Contributed by: Hugh Reeves, Jürg Schneider and David Vasella, **Walder Wyss Ltd**



David Vasella is a partner in the information technology, intellectual property and competition team. He advises Swiss and international companies and authorities on

questions concerning data and technology law.

David specialises in data use, data and technology-related contracts, data security matters, cloud projects, data protection compliance and artificial intelligence. He regularly gives talks and writes publications, for example on datenrecht.ch, a Swiss platform on data law. He is a certified information privacy professional and manager (CIPP/E, CIPM), fellow of information privacy (FIP) and AI governance professional (AIGP).

Walder Wyss Ltd

Seefeldstrasse 123
8008 Zurich
Switzerland

Tel: +41 586 585 858
Fax: +41 586 585 959
Email: reception@walderwyss.com
Web: www.walderwyss.com

walderwyss attorneys at law

Current Trends and Challenges

Cyberthreats are rapidly evolving, becoming ever more sophisticated and harder to detect. One ongoing but no less concerning trend is the increase of ransomware attacks, which have affected numerous companies and other organisations in Switzerland. Moreover, the Federal Office for Cybersecurity (BACS) reported a significant increase in phishing cases. This highlights the ongoing threat of phishing attacks, which often target individuals to gain access to sensitive information or systems.

Recent attacks include an attempt to infiltrate the IT systems of SBB, Switzerland's national railway, via email malware. This attack was partially successful, but no customer data was stolen. Another notable incident was a ransom attack on media companies, when a ransomware group breached the IT infrastructure of *Neue Zürcher Zeitung* and *CH Media*, two leading media outlets, stealing confidential data and encrypted files and extorting the companies. No ransom was paid, apparently, but sensitive employee and customer data later surfaced on the dark web. A hacker attack on a guardianship authority in the town of Saxon was successful, with sensitive client information stolen and published, affecting some 6,000 residents. Other notable incidents include an attack on the sewing machine manufacturer *Bernina*, which, according to media reports, paid a ransom; an attack on an education network used by the city of *Basel-Stadt*, leading to the theft of personal data of more than 750 persons; and a distributed denial-of-service (DDoS) attack during Ukrainian President Zelenskyy's video address to the Swiss Parliament. Other attacks targeted the city of *Baden* and the Canton of *Schwyz*.

The most widely publicised attack, however, was when a ransomware group attacked secu-

rity software provider *Xplain*, which supplies numerous Swiss government agencies. The attackers claimed to have stolen over 900 GB of sensitive data, including information linked to the Swiss Army, customs, and police. An investigation report commissioned by the Confederation was issued on 28 March 2024. Noting the joint responsibility of *Xplain* and the Confederation in connection with this cyber-attack, the report pointed to the Confederation's failure in its duties to select, instruct and supervise the personal data subcontractor, in this case the company *Xplain*. In particular, the investigation report showed that no data processing contract had been concluded between the relevant federal administration units and *Xplain*. In an *Xplain* repeat, hackers hit *Concevis*, another major software vendor for the federal and cantonal governments.

These attacks illustrate that a key threat is the rise of sophisticated, hard-to-detect ransomware attacks, including on critical infrastructure providers, and that even advanced countries like Switzerland are vulnerable to potentially crippling cyber-attacks.

Recent Regulatory Updates

While the increase in reported attacks highlights the urgency of robust cybersecurity, the issue is hardly new. Switzerland has responded to these challenges in recent months and years by adapting its cybersecurity framework on a number of levels.

The revised FADP and Data Protection Ordinance

The revised Swiss Data Protection Act (the Federal Act on Data Protection; FADP), which entered into force on 1 September 2023, introduced improved enforcement powers for the Swiss data protection authority, the Federal

Data Protection and Information Commissioner (FDPIC). The FADP also introduced new requirements around data breach reporting, requiring controllers to inform the FDPIC as soon as possible regarding data security breaches that lead to a high risk and, where necessary, to communicate the breach to the affected data subjects. The reporting obligation is similar to that under the GDPR, but the threshold is higher (high risk under the FADP, and any relevant risk under the GDPR).

In addition, the FADP and the Federal Data Protection Ordinance (DPO) provide for a general requirement to ensure an appropriate level of data security in relation to personal data. The FADP calls for state-of-the-art data security measures, without specifying specific technical standards. This is a deliberate approach from the legislator, who chose to maintain a future-proof, technologically neutral philosophy. However, a specific security requirement is the obligation to ensure that data operations are logged by federal authorities, and by private actors that process sensitive personal data on a large scale or carry out “high-risk profiling”, a form of profiling that leads to personality profiles. The FDPIC has provided guidance for implementing these logging obligations. As Switzerland is not a member of the European Economic Area (EEA), incident notifications in the EEA under the GDPR do not exempt companies from notification obligations towards the FDPIC under the FADP, if applicable, and vice versa.

The FADP provides that individuals (not legal entities, in contrast to the GDPR) who breached data security provisions and thereby failed to comply with the minimum requirements in that respect will face criminal fines of up to CHF250,000. It remains unclear at this time if a general failure to implement a sufficiently robust level of data

security can lead to a fine, but given the potential risks for business managers who may have a personal exposure, these fines are expected to work as an incentive for businesses to ensure state-of-the-art cybersecurity practices.

The new Information Security Act

While the FADP applies to personal data only and, as noted, is fairly high-level, the Swiss Federal Council enacted the Information Security Act (ISA) and four implementing ordinances on 8 November 2023, effective as of 1 January 2024. The ISA is a response to the increasing number of cyber-attacks on public authorities and private individuals, and places high demands on information security. For example, it requires authorities to maintain an information security management system and to ensure that the third parties and providers they work with take necessary security measures. The ISA has also centralised cybersecurity activities under the National Cyber Security Centre (NCSC; now part of the BACS as discussed hereunder) within the Federal Department of Defence, Civil Protection and Sport (DDPS).

A significant feature of the ISA is the introduction of a reporting obligation for cyber-attacks for public authorities such as universities and federal, cantonal and municipal agencies; inter-cantonal, cantonal and intercommunal organisations; and providers of critical infrastructures, for example in the energy, finance, healthcare, insurance, transport and communication and IT sectors. In-scope organisations must report cyber-attacks to the NCSC within 24 hours, where the relevant thresholds and definitions are met. This obligation will come into force on 1 April 2025. This notification obligation is in addition to other incident notifications, such as the obligation to report personal data security breaches to the FDPIC.

Updated government organisation at a federal level

The ISA and ensuing legislation have also reworked the government's security organisation. BACS, within the DDPS, now serves as the centre of competence for cybersecurity, acting as the primary contact for the economy, administration, educational institutions and the public on cyber-related issues. Its tasks include raising public awareness, receiving reports on cyber-incidents and supporting operators of critical infrastructures in managing these incidents. BACS has absorbed the former NCSC, and protection of the federal administration against cyber-attacks is now a key task of a new specialist unit within the new State Secretariat for Security Policy (SEPOS), also within the DDPS.

Other regulatory activity

Other authorities have an increased focus on cybersecurity as well, within the scope of their supervisory activities. A key example is the Swiss Financial Market Supervisory Authority (FINMA), which oversees compliance with – inter alia – data security regulations in the financial sector. It publishes an annual risk monitor as an overview of risks that FINMA sees as particularly significant. The 2024 version highlights that cyber-risks remain one of the biggest operational risks and observes a trend towards malware attacks targeting external service providers and a need for financial institutions to improve their responsibilities and control activities with regard to service providers. Outsourcing contributes to cyber-risks and is a focus for FINMA.

One of FINMA's main supervisory tools is issuing guidance and circulars, which set out its expectations for regulated institutions. These include FINMA Circular 2023/1 Operational Risks and Resilience – Banks, which entered into force on 1 January 2024. It applies to banks and

investment firms, requiring them to report certain cyber-attacks within 24 hours of becoming aware of them and to submit a full report within 72 hours. Again, this obligation is in addition to any other incident notification obligations. There is ongoing discussion in the market in relation to ensuring that the 24-hour requirement is met even where an institution has outsourced IT operations to a provider, such as a cloud services provider. On 7 June 2024, FINMA published FINMA Guidance 03/2024 – Findings from FINMA's cyber risk supervision, clarification of FINMA Guidance 05/2020 and scenario-based cyber risk exercises (see **3.3 Key Operational Resilience Obligations** in the [Swiss Law & Practice chapter](#) in this guide).

Initiatives at a cantonal level

The cantons have also recently increased their efforts to prevent cyberthreats. For example, Switzerland's largest canton by population, the Canton of Zurich, operates a Cantonal Cyber Security Centre (CCSC) as a knowledge hub for the canton, acting as a point of contact for cyber-issues for the cantonal administration, public authorities, critical infrastructure providers, cities, municipalities, cantonal organisations, business and industry, as well as the population. The CCSC is also responsible for implementing the cantonal cybersecurity strategy.

In addition, cantonal data protection legislation – applicable to public entities acting under cantonal laws, which may include private actors carrying out public tasks – requires notification of personal data security breaches to the cantonal data protection authorities.

The Artificial Intelligence Regulation, AI Regulation, AI Act or AIA

Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence and amend-

ing Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (the Artificial Intelligence Regulation, AI Regulation, AI Act or AIA) came into force on 1 August 2024. Its provisions will take effect in stages until August 2027 (Article 113 of the AI Act).

The AI Act is the comprehensive regulatory framework by which the EU (or the EEA, the AIA is of EEA relevance) regulates the use of AI systems (AI systems, AIS). Despite its name, the AI Act is not a comprehensive regulation of AI or market behaviour law, but rather a product safety law. It is based on the established principles of product regulation in the European single market.

The AI Act is initially applicable in the EU. However, it will be incorporated into EEA law and will then also apply to Norway, Iceland and Liechtenstein. The AI Act is currently at the EEA review stage; it will only be formally incorporated into EEA law after a decision by the Draft Joint Committee. Moreover, a Swiss company may therefore be subject to the AI Act if it sells an AIS to or in the EU (as a developer, importer or distributor); sells another product in the EU that uses an AIS as a component; or generates output that is used in the EU.

Unlike the GDPR, the AI Act itself does not contain any provisions for fines, but in Article 99 it requires member states to introduce provisions for fines, as well as other enforcement measures. Fines can be imposed on all actors – ie, on all entities involved in the value chain. Depending on the type of violation, the fines can reach up to EUR35 million or 7% of the turnover.

In Switzerland, however, there is currently no overarching regulation on the use of AI (see 6.2 **Cybersecurity and AI** in the [Swiss Law & Practice chapter](#) in this guide). At the end of 2023, the Federal Council commissioned the Federal Department of the Environment, Transport, Energy and Communications (DETEC) to explore possible approaches for regulation within the framework of the Interdepartmental Coordination Group on EU Digital Policy, by the end of 2024, and a report was published on 11 February 2025.

As a result, AI is currently governed in Switzerland by general laws, depending on the legal object affected by the use of AI, such as:

- the data protection law (if personal data is processed during training or use);
- the secrecy protection law (if secret information is used for training or as input);
- the employment contract law (if the personal data of applicants and employees is processed and if AI affects the employer's duty of care);
- public labour law (eg, when duties to cooperate take effect or when monitoring behaviour is discussed);
- personal rights (eg, when conversations or team calls are recorded);
- unfair competition law (when AI-generated content can be misleading);
- copyright law (eg, when AI is trained with works or uses works as input, and when the protection of output is under discussion);
- criminal law (when recording non-public conversations or when using AI for punishable behaviour in general);
- product liability and other liability laws; and
- other areas of law.

Private actors have also issued rules for themselves in the meantime. On 18 December 2024, FINMA published its Guidance 08/2024 – Governance and risk management when using AI, and numerous private companies have also issued or are in the process of issuing guidelines, codes and instructions, some of which are public and some of which are not.

At the end of 2023, the Federal Council commissioned DETEC to explore possible approaches for regulation within the framework of the Interdepartmental Coordination Group on EU Digital Policy, by the end of 2024. Based on this mandate, on 12 February 2025, DETEC and the Federal Department of Foreign Affairs (FDFA) pre-

sented an overview to the Swiss Federal Council of possible regulatory approaches to AI. On the basis of this overview, the Swiss Federal Council has decided on a Swiss regulatory approach for AI based on three objectives: strengthening Switzerland's location for innovation; safeguarding the protection of fundamental rights, including economic freedom; and increasing public trust in AI. To achieve these objectives, the Swiss Federal Council has set the following key steps for the future: incorporation of the Council of Europe's AI Convention into Swiss law; sector-specific legislation as far as required (cross-sector regulation, to be limited to central areas relevant to fundamental rights); and non-binding measures.



Law and Practice

Contributed by:

Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş
and Yağmur Yaren Özdebakoglu
YAZICIOGLU Legal

Contents

1. General Overview of Laws and Regulators p.295

- 1.1 Cybersecurity Regulation Strategy p.295
- 1.2 Cybersecurity Laws p.296
- 1.3 Cybersecurity Regulators p.300

2. Critical Infrastructure Cybersecurity p.302

- 2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.302
- 2.2 Critical Infrastructure Cybersecurity Requirements p.304
- 2.3 Incident Response and Notification Obligations p.306
- 2.4 State Responsibilities and Obligations p.307

3. Financial Sector Operational Resilience Regulation p.307

- 3.1 Scope of Financial Sector Operational Resilience Regulation p.307
- 3.2 ICT Service Provider Contractual Requirements p.308
- 3.3 Key Operational Resilience Obligations p.309
- 3.4 Operational Resilience Enforcement p.309
- 3.5 International Data Transfers p.310
- 3.6 Threat-Led Penetration Testing p.312

4. Cyber-Resilience p.312

- 4.1 Cyber-Resilience Legislation p.312
- 4.2 Key Obligations Under Legislation p.313

5. Security Certification for ICT Products, Services and Processes p.313

- 5.1 Key Cybersecurity Certification Legislation p.313

6. Cybersecurity in Other Regulations p.314

- 6.1 Cybersecurity and Data Protection p.314
- 6.2 Cybersecurity and AI p.315
- 6.3 Cybersecurity in the Healthcare Sector p.316

Contributed by: Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Özdebakoğlu, YAZICIOGLU Legal

YAZICIOGLU Legal is an Istanbul-based boutique technology law firm. The firm focuses on legal matters related to technology, media & telecommunications and data protection/cybersecurity. It also has solid expertise in cross-border transactions, corporate and commercial matters, intellectual property, regulatory compliance, e-commerce, consumer protection and dispute resolution. YAZICIOGLU Legal has a dedicated team of 16 lawyers working on data protection and cybersecurity. The majority of the firm's workload involves data protection-re-

lated matters. In particular, the firm is known for successfully representing its clients on investigations and data breaches before the Turkish Data Protection Authority. It also provides assistance to several clients, both local and international, including, but not limited to, Acer, Reddit, and Workday, in ensuring compliance with data protection legislation, particularly in cross-border data transfers. The firm is ranked in several legal directories for TMT and is also a Bronze Corporate Member of the International Association of Privacy Professionals (IAPP).

Authors



Bora Yazıcıoğlu is the managing partner at YAZICIOGLU Legal. He has significant experience in advising national and international clients on several aspects of data protection,

cybersecurity, and e-commerce law. Bora has represented several major clients on data breaches and investigations before the Turkish Data Protection Authority. He is one of the founding members and the current President of the Data Protection Association of Türkiye. Bora acts as the data controller representative for Zoom, Acer, Cerus, and Ookla in Türkiye.



Kübra İslamoğlu Bayer is a senior managing associate at YAZICIOGLU Legal. She advises clients on data protection, e-commerce, and cybersecurity laws. She is an active member

of the Istanbul Bar Association's IT Law Commission: Artificial Intelligence Study Group and the Data Protection Commission. Kübra gives speeches on data protection on several platforms. She holds a CIPP/E certificate from the International Association of Privacy Professionals.



Aslı Rabia Savaş is a senior associate at YAZICIOGLU Legal. She primarily focuses on data protection law, cybersecurity, e-commerce, and contracts law.

Aslı holds an advanced master's degree specialising in data law, and a CIPP/E certificate from the International Association of Privacy Professionals.



Yağmur Yaren Özdebakoğlu is an associate at YAZICIOGLU Legal. She focuses on various areas of law, including data protection, cybersecurity, e-commerce, contracts law and consumer protection law.

Contributed by: Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Öz dabakoğlu,
YAZICIOGLU Legal

YAZICIOGLU Legal

NidaKule – Goztepe
Merdivenköy Mahallesi Bora Sokak No: 1
Kat: 7 34732 Kadıköy
İstanbul
Türkiye

Tel: +90 216 468 8850
Fax: +90 216 468 8801
Email: info@yazicioglulegal.com
Web: www.yazicioglulegal.com

YAZICIOGLU
— LEGAL —

1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

Cybersecurity has been at the forefront of Türkiye's strategic policies since the last decade as an integral part of its national security. The results are showcased in the Global Cybersecurity Index 2024 published by the International Telecommunication Union, which ranked Türkiye as a Tier-1 Role-modelling country in Europe and awarded a full score in all five areas of strength (eg, legal, technical, organisation, capacity development, and co-operation measures).

The National Cybersecurity Strategy for 2024–2028 (the “NCS 2024”)

Since 2012, the Ministry of Transport and Infrastructure (the MTI) has published four mid-term strategic plans for cybersecurity, the most recent being the NCS 2024. According to the NCS 2024, Türkiye's cybersecurity strategy for the next four years is based on six objectives:

- cyber-resilience;
- proactive cyber-defence and deterrence;
- human-centred cybersecurity approach;

- secure use of technology and its contribution to cybersecurity;
- use of domestic and national technologies for combating cyber threats; and
- international reputation.

The 12th Development Program (2024–2028)

The 12th Development Program sets out the following general policy goals for information technologies, as well as sector-specific policies (eg, financial markets, education and health):

- strategic, regulatory, and technological efforts to ensure national cybersecurity and strengthen institutional structures;
- updating the National Cyber Security Strategy and Action Plan in the context of new-generation cyber-threats and technological developments;
- enacting regulations in line with the EU's “NIS2 Directive” and the best international practices;
- administrative structuring for high-level co-ordination of national cybersecurity activities;
- strengthening cybersecurity threat intelligence through the development of AI and big data analytics applications;

Contributed by: Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Özdebakoglu, YAZICIOGLU Legal

- strengthening the national cybersecurity infrastructure;
- enacting and implementing procedures and principles on the establishment of an information security system in critical infrastructures;
- introducing cybersecurity standards in the required fields;
- improving the domestic cybersecurity ecosystem, spreading national solutions, and boosting competitiveness on an international scale;
- supporting the global competitiveness of domestic solutions;
- developing test infrastructures for cybersecurity;
- increasing the use of domestic cybersecurity products, primarily in public institutions;
- raising cybersecurity awareness and training a competent workforce and making new business models for maintaining the same;
- building programmes aimed at cybersecurity training and bettering career opportunities; and
- improving the content, quality, and environment for training personnel fit for the sectoral needs.

The Medium-Term Program (2025–2027)

Medium-Term Program provides the following policy objectives:

- utilising digital technologies to the fullest extent to strengthen nationwide cybersecurity through comprehensive policies, enhance the efficiency of public administration, and develop public services;
- enacting dedicated legislation on cybersecurity and the necessary secondary regulations in compliance with the EU *acquis* (the collection of common rights and obligations that constitute the body of EU law, incorporated

- into the legal systems of EU member states – according to the official website of the EU);
- implementing public–university–private sector co-operation programmes to train qualified personnel in strategic fields, including cybersecurity; and
- taking measures to increase the level of resilience in payment and electronic institutions’ cybersecurity.

The Presidency Program for 2025

Lastly, the Presidency Program for 2025 sets out more specific plans that are based upon the six objectives set out in the NCS 2024, including:

- legislative works in line with the EU legal framework (eg, the EU’s NIS2 Directive and the EU Cyber Resilience Act);
- review of critical infrastructure sectors;
- awareness-raising activities for the public; and
- cybersecurity training for public servants.

1.2 Cybersecurity Laws

There have been significant developments in cybersecurity legislation of Türkiye recently. On 19 March 2025, the Cybersecurity Act was published in the official gazette and entered into force. According to the Cybersecurity Act, secondary regulations will be made within one year. Until then, current regulations that are not contrary to the Cybersecurity Act will continue to be in force.

General Regulations

The Constitution of the Turkish Republic (the “Constitution”)

The Constitution does not directly set out any provision on cybersecurity. However, as cybersecurity is an umbrella term also covering data protection – whether it is personal or non-personal data – it can be considered that cyberse-

Contributed by: Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Öz dabakoğlu, YAZICIOGLU Legal

curity is partly and indirectly covered by Article 20(3) of the Constitution, which provides for the right to protection of personal data. Furthermore, Article 22 recognises freedom of communication as an individual right to any person.

The Cybersecurity Act

The Cybersecurity Act provides a dedicated legal framework for the responsibilities of institutions and persons who operate in cyberspace and the powers and duties of the recently established Cybersecurity Directorate (“*Directorate*”). It also establishes the Cybersecurity Board and determines its duties.

Additionally, certain actions are now criminalised, such as:

- failure to provide information, documents and data to the Directorate’s audit personnel;
- distributing, sharing or selling leaked data; and
- creating and disseminating false content regarding data breaches in cyberspace, with the intent to incite anxiety, fear and panic among the public or to target institutions or individuals.

There are also specific requirements for companies producing cybersecurity products and services.

For more information on the Cybersecurity Act, see **1.3 Cybersecurity Regulators**, **2.1 Scope of Critical Infrastructure Cybersecurity Regulation**, **2.2 Critical Infrastructure Cybersecurity Requirements**, **4.1 Cyber-Resilience Legislation**, **4.2 Key Obligations Under Legislation**, and **5.1 Key Cybersecurity Certification Legislation**.

The Law on Regulation of Publications via the Internet and Combating Crimes Committed by Means of Such Publications No 5651 (the “Internet Law”)

The Internet Law aims to regulate the obligations and responsibilities of content providers, hosting providers, internet service providers, social network providers, and access providers to combat crimes committed via the internet.

The Internet Law directs the Turkish Information and Communication Technologies Authority (the ICTA) to establish co-ordination between the relevant public institutions, law enforcement agencies, above-mentioned providers and other related institutions and organisations to ensure the safe use of the internet, raise public awareness, and carry out necessary activities (eg, taking necessary measures within the scope of national cybersecurity policies). However, according to the Cybersecurity Act, the ICTA will no longer be able to carry out these duties when the Directorate’s organisation is completed.

The Law on Electronic Communication No 5809 (the “E-Communication Law”)

Information security is among the basic principles in the E-Communication Law, which provides the main framework for network security, the confidentiality of communication, and personal data protection. Detailed provisions concerning each may be found under several secondary pieces of legislation enacted based thereon.

While the ICTA is the authorised regulatory body in the e-communications sector, its authority in cybersecurity measures has now been transferred to the Directorate. However, the ICTA will continue to exercise these powers until the latter becomes operational.

Contributed by: Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Özdebakoglu, YAZICIOGLU Legal

The Council of Ministers Decision on Carrying Out, Managing and Co-ordinating National Cybersecurity Activities, dated 11 June 2012 (the “Council of Ministers Decision on Cybersecurity”)

This decision is one of the landmarks of Türkiye’s cybersecurity legislation. It defines national cybersecurity as: “security of all services, transactions, and data provided via information and communications technologies as well as systems used for the provision thereof”.

The Cybersecurity Act transfers the MTI’s cybersecurity-related duties and powers to the Directorate; however, it does not explicitly annul this decision.

The Presidential Decree No 177 on the Cybersecurity Directorate

On 8 January 2025, the Presidential Decree No 177 on the Cybersecurity Directorate established the Directorate as a public legal entity affiliated with the Presidency with financial autonomy. The decree grants the Directorate general regulatory power on cybersecurity matters. Refer to **1.3 Cybersecurity Regulators** for further explanations on the duties of the Directorate.

The Communiqué on Procedures and Principles of the Establishment, Duties and Activities of Cyber-Incidents Response Teams (CERTs) (the “Communiqué on CERTs”)

The purpose and scope of this *communiqué* are to ensure CERTs carry out their services effectively and efficiently by determining the procedures and principles of their establishment, duties and work.

The Guideline for Establishment and Management of Institutional CERTs (the “Institutional CERT Guideline”) and the Guideline for Establishment and Management of Sectoral CERTs (the “Sectoral CERT Guideline”)

These guidelines, published by the National Cyber Incidents Response Centre (TR-CERT), provide guidance on:

- establishing and managing institutional CERTs and sectoral CERTs in relevant organisations;
- their relationship with each other and the TR-CERT;
- capacity planning;
- qualifications of the personnel (education level and experience);
- mandatory training; and
- the steps that personnel must take before, during and after a cybersecurity incident.

They also include the principles for communication with internal/external stakeholders and establishing institutional and sectoral CERTs.

The Decree No 2019/12 on Information and Communication Security Measures issued by the Presidency of Türkiye (the “Presidency Decree”)

The Presidency Decree sets specific measures deemed appropriate to diminish and neutralise security risks – in particular, ensuring the security of critical data that may jeopardise national security or deteriorate public order when its confidentiality, integrity, or accessibility is compromised. It provides an obligation to securely store critical data (eg, population, health and communication records, genetic and biometric data) within Türkiye.

Contributed by: Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Özdebakoglu, YAZICIOGLU Legal

The Presidency Decree applies to public institutions and organisations as well as businesses providing critical infrastructure services (ie, energy, electronic communications, banking and finance, critical public services, water management, and transportation). See **2.1 Scope of Critical Infrastructure Cybersecurity Regulation** for further details.

The Turkish Data Protection Law No 6698 (the “DP Law”) and its secondary legislation

The DP Law covers all personal data-processing activities in Türkiye. From a cybersecurity perspective, it also regulates the security of personal data and full or partly automated and non-automated data-processing systems. According to the DP Law, controllers are obliged to take all necessary technical and organisational measures to provide a sufficient level of security to:

- prevent unlawful processing and accessing of personal data; and
- ensure the safekeeping of personal data.

See **6.1 Cybersecurity and Data Protection** for further information.

The Turkish Criminal Code (the TCrC) No 5237

The TCrC criminalises several actions in connection to cybersecurity and sets out criminal sanctions of imprisonment between six months and eight years for these actions. Some are as follows:

- unlawful access to a cyber-system;
- blocking or bricking the cyber-system or destroying, modifying, or making inaccessible the data within a cyber-system;
- misuse of debit or credit cards;
- manufacturing, importing, dispatching, transporting, storing, accepting, selling, offering for

sale, purchasing, giving to others or keeping forbidden devices and software that are used to break a computer program’s password or a code as such in order to commit a crime described in the bullet points above;

- committing theft or fraud via cyber-systems;
- unlawful recording of personal data;
- unlawful transfer, publication or acquisition of personal data; and
- failure to destroy personal data after the retention period set forth in the applicable laws.

The Law on Intellectual and Artistic Works No 5846

The Law on Intellectual and Artistic Works (focusing on the protection of copyright) also criminalises the following actions with sanctions of imprisonment between six months and two years:

- circumventing technological measures such as access control or encryption;
- breach of the protected rights of the database manufacturer; and
- continuous violation of copyrights and related rights by service and information content providers via transmission tools for signs, sounds and/or images, including digital transmission.

The Communiqué on the Procedures and Principles for Connecting to and Auditing the KamuNet Network (The “Communiqué on KamuNet”)

KamuNet (loosely translated as PublicNet) is a closed-circuit, virtual network infrastructure isolated from the private network and internet environment and utilised by public institutions and organisations in their service, transaction, and data traffic transfers. Hence, it is more secure against physical and cyber-attacks. Per the Prime Ministry Decree No 2016/28 on Inte-

Contributed by: Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Özdebakoglu, YAZICIOGLU Legal

grating Public Institutions and Organisations into KamuNet, all public institutions and organisations must utilise the KamuNet network.

The *Communiqué* on KamuNet sets the requirements for public institutions and organisations integrated into KamuNet, such as having a TS ISO/IEC 27001 certificate for their information security management systems. In addition, it authorises the MTI to determine the public institutions and organisations to be integrated into KamuNet and assess their suitability before the integration.

1.3 Cybersecurity Regulators

Regulators

The Cybersecurity Directorate

The Directorate has been designated as a general authority on cybersecurity matters. The main duties and powers of the Directorate are as follows:

- conducting operations to increase cyber-resilience (eg, by penetration tests or risk analysis);
- determining critical infrastructures;
- ensuring keeping of the asset inventory for public institutions and critical infrastructures;
- establishing and auditing CERTs;
- determining the procedures and principles to be followed by those operating in the field of cybersecurity;
- establishing and operating the necessary infrastructure for the cybersecurity of public institutions and critical services, providing secure hosting services, and defining the procedures and principles thereof;
- determining the standards for the cybersecurity field;
- carrying out testing and certification procedures for the cybersecurity field;

- conducting cybersecurity audits and imposing sanctions; and
- determining the technical criteria for the cybersecurity products and services to be used in public institutions and critical infrastructures.

However, the Directorate's duties will continue to be performed by the existing relevant public institutions and organisations until the relevant units within the Directorate are established and become operational.

The Ministry of Transport and Infrastructure (the MTI)

The Council of Ministers Decision on Cybersecurity authorises the MTI for the implementation, administration and co-ordination of national cybersecurity actions and preparation and co-ordination of policy, strategy and action plans regarding the governance of national cybersecurity.

MTI oversees and conducts cybersecurity activities at the strategic level through the TR-CERT.

The Cybersecurity Act delegates MTI's cybersecurity-related responsibilities to the Directory.

The Cybersecurity Board

The Cybersecurity Board, presided by the President of the Republic of Türkiye, is tasked with:

- adopting resolutions regarding cybersecurity policies, strategies, action plans, and other regulatory measures;
- adopting resolutions for the implementation of the cybersecurity technology roadmap prepared by the Directorate;
- identifying priority areas for incentives in cybersecurity;

Contributed by: Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Özdebakoglu, YAZICIOGLU Legal

- adopting resolutions for the development of human resources in the cybersecurity field;
- determining critical infrastructure sectors; and
- resolving the disputes between the Directorate and public institutions.

The Information and Communication Technologies Authority (the ICTA)

ICTA is an independent administrative institution and has administrative and financial autonomy.

In addition to its regulatory role in telecommunications, ICTA closely monitors cybersecurity incidents through publicly available and private forums and mediums. ICTA also audits and warns private companies concerning specific cybersecurity threats and technical vulnerabilities.

The Cybersecurity Act annuls the provisions granting the ICTA general cybersecurity-related powers and limits its duties to the data systems within its own competency. However, ICTA will continue carrying out its duties for the time being. According to the Cybersecurity Act, when the Directorate's organisation becomes fully operational, ICTA will transfer to the Directorate all its assets that are exclusively used for national cybersecurity activities.

The Digital Transformation Office (the DTO)

The DTO has played an active role in cybersecurity, big data, artificial intelligence, and digital transformation since its establishment in 2018.

The DTO was abolished with a Presidency Decree on 28 March 2025 and its cybersecurity-related duties and assets have been transferred to the Directorate.

National Cyber Incidents Response Centre (the TR-CERT)

In 2013, the TR-CERT was established under ICTA to identify emerging threats, take measures to reduce and eliminate the effects of possible attacks and incidents on national cyberspace and share them with the relevant actors.

TR-CERT oversees the management of response to cybersecurity incidents from the beginning until the resolution. It co-ordinates with CERTs who are required to report cybersecurity events to the TR-CERT.

TR-CERT also carries out awareness-raising and guidance activities to increase the awareness of public institutions and organisations against cyber-attacks.

Cyber Incidents Response Teams (CERTs) Sectoral CERTs

Sectoral CERTs are established under:

- the regulatory and supervisory bodies; or
- the relevant ministries of critical sectors, which are:
 - (a) the Ministry of Interior;
 - (b) the Ministry of Justice;
 - (c) the Ministry of Treasury and Finance;
 - (d) the Ministry of Environment, Urbanisation and Climate Change;
 - (e) the Ministry of Labour and Social Security;
 - (f) the Ministry of Agriculture and Forestry; and
 - (g) the Ministry of Health.

Sectoral CERTs are responsible for co-ordination, regulation and supervision of cybersecurity in their respective critical sectors. They act in

Contributed by: Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Özdebakoglu, YAZICIOGLU Legal

co-ordination with the TR-CERT and institutional CERTs operating in the sectors concerned.

Institutional CERTs

Institutional CERTs are established within public and private organisations.

All organisations operating in the critical infrastructure sectors must establish an institutional CERT thereunder and ICTA has the authority to order a public or private organisation to establish and maintain a CERT, even if that organisation does not operate in critical infrastructure sectors.

Institutional CERTs also act in co-ordination with the TR-CERT and sectoral CERTs operating in the relevant sector, as applicable.

The Personal Data Protection Authority (the DPA)

The primary supervisory and regulatory authority for data protection matters is the DPA. It is an independent administrative institution that has administrative and financial autonomy.

The DPA is authorised to regulate data protection activities and to take measures to protect the rights of data subjects. The DPA is competent to receive data breach notices according to the DP Law.

The National Intelligence Agency

The National Intelligence Agency is entitled to collect, record, and analyse information, documents, news, and data by using any technical intelligence and human intelligence method, tool and system regarding foreign intelligence, national defence, counterterrorism, international crimes and cybersecurity, and to deliver the produced intelligence to the necessary institutions.

The Turkish National Police Department of Cybercrime Prevention

Established in 2011, this department provides support in investigating crimes committed using information technology. It gathers forensic data to fight cybercrime effectively and efficiently.

The Ministry of National Defence, the Presidency of Defence Industries, and the Turkish Armed Forces Cyber Defence Command

These entities ensure cybersecurity from the perspective of military and national defence.

The Ministry of Interior Disaster and Emergency Management Presidency

The Ministry of Interior Disaster and Emergency Management Presidency is responsible for crisis co-ordination and management to protect critical infrastructures in the event of a disaster.

Others

Apart from the above, sector-specific administrative institutions such as the Banking Regulation and Supervision of Agency (the BRSA), the Capital Markets Board (the CMB), the Turkish Republic Central Bank (the TRCB), the Energy Market Regulatory Authority (the EMRA), the General Directorate of Civil Aviation (the GDCA), and the Nuclear Regulatory Authority are entitled to regulate cybersecurity-related issues in their respective sectors.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

General

There is no framework legislation on critical infrastructure cybersecurity like the EU's NIS2

Contributed by: Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Özdebakoğlu, YAZICIOGLU Legal

or the USA's Cyber Incident Reporting for Critical Infrastructure Act. However, enacting regulations in line with the EU's "*NIS2 Directive*" is a policy goal identified by the 12th Development Program.

The Cybersecurity Act delegates to the Directorate and the Cybersecurity Board the duty to determine critical infrastructures and the organisations and locations to which they belong. Currently, there is no precise scope for critical infrastructure cybersecurity regulation, and the relevant sectoral legislation must be consulted. The applicable legal texts are policy documents published by authorised institutions and sector-specific by-laws.

The DTO's Information and Communication Security Guide (the "ICS Guide")

The ICS Guide published by DTO defines "*critical infrastructure*" as "*infrastructures that incorporate information technologies which may cause loss of life, economic harm of large-scale, national security gaps and public disorder when the confidentiality, integrity and availability of data/information therein are disrupted*".

The ICS Guide applies to public institutions, organisations and businesses providing critical infrastructure services. It sets out general security measures and those specific to the energy and e-communication sectors. The ICS Guide defines, among other things, the asset groups (eg, network and systems, apps, devices, physical places, and personnel), their criticality level, measures, the application process, and their respective compliance plan.

Guidance of the MTI

The MTI is tasked with identifying critical infrastructures along with the institutions they belong to and their locations. (However, this duty will be

transferred to the Directorate when it is operational.) There are six critical infrastructure sectors:

- e-communications;
- energy;
- finance;
- transport;
- water management; and
- critical public services.

The Sectoral CERT Guideline published by the MTI defines critical public services as services provided by critical systems with which citizens frequently interact, and mentions the following:

- civil registration;
- land registration;
- taxation;
- commerce;
- social security;
- health (emergency services, medical services, blood and organ donation and public health);
- food;
- security (police, *gendarmerie*, – a police force that is part of the armed forces in Türkiye that is affiliated to the Ministry of Interior and carries out duties related to safety, public order and security assigned to it by certain laws and regulations – and coast guard);
- roads and bridges;
- dams; and
- services provided via critical systems where salary and judicial transactions are performed and their records are kept.

The MTI also published: "*Document for Minimum Security Measures for Critical Information System Infrastructure*" and "*Minimum Information Security Criteria for Public Institutions to Comply*".

E-Communications

The By-Law on NIS in the E-Communications Sector is the main regulation for the e-communications sector, with the purpose to provide the procedures and principles of operators to ensure network and information security. It applies to the operators within the scope of the E-Communications Law.

Energy

The main regulation on cybersecurity in the energy sector is the By-Law on Cybersecurity Competency Model in the Energy Sector. It aims to improve cybersecurity and define the minimum acceptable level of security of industrial control systems used in the energy sector, and establish the procedures and principles related to the cyber-resilience, proficiency, and maturity thereof.

The By-Law covers industrial control systems owned by legal entities with the following licences: electricity transmission licence, electricity distribution licence, electricity generation facility licence, natural gas transmission licence for pipeline transmission, natural gas distribution licence, natural gas storage licence (LNG, underground), crude oil transmission licence, and refinery licence.

Banking and Finance

By-Law on Information Systems of Banks and Electronic Banking Services aims to manage information systems used by banks in the performance of their operations and set forth the minimum procedures and principles to be applied in the offer of electronic banking services and management of risks related thereto. It covers the entities falling within the scope of the Banking Law (eg, deposit and participation banks, branches of foreign institutions within Türkiye, etc).

2.2 Critical Infrastructure Cybersecurity Requirements

General

According to the Cybersecurity Act, one of the duties of the Directorate is to determine technical criteria for cybersecurity products and services to be used in public institutions and critical infrastructures. However, these criteria are not determined yet as the Directorate has not become fully operational.

The Presidency Decree provides the following security measures for critical infrastructure security of public institutions and organisations:

- conducting security clearances for personnel of critical importance; and
- requiring communication service providers to establish internet exchange points in Türkiye.

For comprehensive measures, the Presidency Decree refers to the ICS Guide, which provides the following for critical infrastructure security in public institutions and organisations and businesses providing critical infrastructure services:

- network and system security measures (eg, protection against malware, penetration tests, and cybersecurity management);
- application and data security measures (eg, secure software development, error handling and log management, and database and record management);
- portable device and media security measures (eg, securing smartphones and tablets, portable computers and portable media);
- IoT devices security measures (eg, internal data storage, authentication and authorisation, and API and connectivity security);
- personnel security measures (eg, training and awareness programmes, and suppliers' relationship security); and

Contributed by: Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Özdebakoglu, YAZICIOGLU Legal

- physical environment security measures (eg, protection of server room/data centre, and protection against electromagnetic information leakage (TEMPEST)).

The ICS Guide also sets out sector-specific security measures for e-communications and energy sectors. Additionally, there are other sector-specific regulations setting the requirements for critical infrastructure cybersecurity. Refer to the details of the sector-specific regulations below.

E-Communications Sector

Security measures to be taken by the actors in the e-communications sector in accordance with the ICS Guide are as follows:

- service security and continuity;
- infrastructure services security;
- fraud detection and prevention;
- signalling traffic security;
- establishing trusted communication;
- hardening activities;
- monitoring equipment failures;
- ensuring equipment security;
- threat intelligence management;
- communication with authorities;
- prevention of caller ID manipulation; and
- ensuring that domestic communication traffic remains within the country.

The By-Law on NIS in the E-Communications Sector requires that a report on NIS must be prepared by the operator every year – until the end of March – and kept for five years to be sent to ICTA upon request and/or submitted during the inspections made by ICTA. The report includes information such as:

- risk assessment and processing methods, and details of transactions made according to these methods;
- business continuity plans; and
- details on information security breach incidents that have occurred.

Per the By-Law, operators cannot allow unlicensed software and software going against Information Security Management Systems Policy rules and must take measures to protect information and software against harmful codes and identify security measures for downloading files or software via external networks.

Operators are also obligated to define and document rules related to the transfer of software from the development environment to the production environment.

Energy Sector

The actors in the energy sector must take the following security measures per the ICS Guide:

- device configurations;
- network access control;
- authentication;
- access management;
- physical access security;
- ensuring system continuity;
- prevention of data manipulation;
- user access management;
- SSL/TLS protected communication;
- security of GPS communication and synchronisation;
- ensuring equipment security;
- threat intelligence management;
- communication with authorities; and
- using safe methods for data transmission.

The competency model under the By-Law on Cybersecurity Competency Model in the Energy

Sector sets out three basic competency levels. The applicable competency level will be identified with sectoral criticality degrees determined by the EMRA. The obligated organisations must implement the competency model after EMRA determines the respective criticality degrees and notifies them.

Banking and Finance Sector

Banks and other financial institutions under the authority of the BRSA must take the measures outlined in the By-Law on Information Systems of Banks and Electronic Banking Services.

Moreover, personal data specific to banking relationships are also considered customer secrets under the Banking Law. For specific requirements and restrictions thereto, see **3. Financial Sector Operational Resilience Regulation**.

Health Sector

See **6.3 Cybersecurity in the Healthcare Sector**.

Civil Aviation Sector

The Cybersecurity Directive for Civil Aviation Enterprises (the “*Directive*”) outlines the following measures to be taken by civil aviation enterprises against cyber threats:

- effective oversight of use of information systems;
- regular cybersecurity risk and threat assessments for operational assets;
- implementation of policies, procedures, and process documents;
- mechanisms to detect, prevent, and respond to potential cybersecurity breaches;
- testing, auditing, and monitoring cybersecurity controls and structures, and reporting the results; and
- developing a continuity management process and continuity plan for IT systems to ensure

critical cybersecurity processes remain operational.

2.3 Incident Response and Notification Obligations

General Notification Duties

One of the main obligations provided under the Presidency Decree for public institutions is adopting the necessary measures regarding cyber threat notifications.

“*cybersecurity event*” is defined in the *Communiqué* on CERTs as “*breach or attempted breach of confidentiality, integrity, or accessibility of industrial control or information systems or data processed thereby*”. If an organisation is required to establish a CERT, in principle, its CERT must report any cybersecurity event to the TR-CERT and the relevant sectoral CERT (if applicable). See **1.3 Cybersecurity Regulators** for more details.

Conversely, an organisation that is not required to establish a CERT, is not under obligation to report (although, voluntary reporting is allowed).

In addition, when the Directorate becomes operational, institutions and persons using information systems will be required to notify the Directorate of any vulnerability or cyber incidents that they detect in their service area. Also, those who fail to fulfil their duties and responsibilities by not reporting cyber incidents and vulnerabilities to the Directorate will be subject to an administrative fine between TRY1 million and TRY10 million.

Personal Data Breach Notification to the DPA

Controllers must report to the DPA within 72 hours and notify the relevant data subjects within the shortest time possible if third parties unlawfully acquire personal data (regardless of

the likelihood or lack thereof to result in a risk to the rights and freedoms of natural persons).

Sectoral Notification Duties

- In the e-communications sector, the By-Law on NIS in the E-Communication Sector requires the operator to notify ICTA regarding network and information security breaches that affect more than 5% of its subscribers and the circumstances that interrupt the continuity of the business. The notification must include, as a minimum, the time, nature, impact and duration of the breach, as well as the measures taken.
- In the banking sector, the By-Law on Information Systems of Banks and Electronic Banking Services (the “By-Law ISBEBS”) requires banks to report cyber-events to the BRSA.
- A cyber-attack affecting a public company must be disclosed to the public as per the *Communiqué* on Material Events Disclosure.
- In the healthcare sector, as per the Directive on the Information Security Policies of the Ministry of Health, all information security breach incidents related to the Ministry of Health must be submitted to the central breach notification system thereof.

2.4 State Responsibilities and Obligations

For the allocation of duties and the details thereof, see 1.3 Cybersecurity Regulators. See also 2.1 Scope of Critical Infrastructure Cybersecurity Regulation and 2.2 Critical Infrastructure Cybersecurity Requirements for obligations provided for public institutions under the ICS Guide.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

There is no general legislation covering the Turkish financial sector’s operational resilience. Rather, relevant regulations of the BRSA, TRCB and CMB set the rules on the management of information systems for banks, payment and electronic money institutions, and capital market institutions respectively.

- The information systems of banks are regulated by By-Law ISBEBS. It applies to deposit banks, participation banks, development and investment banks established in Türkiye and the Turkish branches of such foreign banks.
- The information systems of payment institutions and electronic money institutions are regulated by the *Communiqué* on Data-Sharing Services in the Payment Services Area of Payment and Electronic Money Institutions’ Information Systems and Payment Service Providers (the “*Communiqué* on Payment Services”). The *Communiqué* covers payment institutions and electronic money institutions, which consist of an exhaustive list of institutions that are authorised by the TRCB in accordance with the Law on Payment and Securities Settlement Systems, Payment Services, and Electronic Money Institutions.
- The CMB has a *Communiqué* on Information Systems Management (The “*CMB Communiqué*”). This *Communiqué* concerns stock exchanges and market operators and other organised marketplaces, publicly held corporations, and capital market institutions (eg, investment firms, collective investment schemes, portfolio management companies, and cryptocurrency service providers), among others. This *Communiqué* was superseded

by another *Communiqué* (The “*New CMB-Communiqué*”) that will take effect on 30 June 2025. The new *Communiqué* will cover crypto-asset service providers as well.

3.2 ICT Service Provider Contractual Requirements

There is no legal definition for ICT service providers or cloud service providers. However, several sectoral regulations indicate different service providers for ICT services. Since they are regulated sectorally, there is no general classification of critical ICT services either.

The By-Law ISBEBS, the *Communiqué* on Payment Services, and the CMB *Communiqué* (collectively, the “*Financial NIS*”) The Financial NIS regulates the outsourcing of ICT services by the institutions it covers. Thus, it includes provisions concerning the financial sector institutions’ outsourced information systems services.

The Financial NIS aims to guarantee that financial sector institutions retain their control over even the outsourced information systems and for them to remain accountable to the relevant parties (eg, their customers). For the scope of Financial NIS, see 3.1 **Scope of Financial Sector Operation Resilience Regulation**.

The By-Law ISBEBS defines “*outsourcing*” as support services that banks acquire from external sources, which may potentially affect the confidentiality, integrity, and availability of banking data, continuity of banking services, and services involving access to or sharing of banking data.

Banks must also follow the conditions set under the By-Law on Support Services for Banks,

which covers the banks’ outsourcing of any type of support services.

Outsourcing contracts must include certain clauses, including:

- the scope of the contract and the responsibilities of the parties;
- the liability of the external outsourcing provider with regard to information security;
- the liability of the sub-contractors of the outsourcing provider, which must be equivalent to thereof; and
- terms for changes and termination.

Classification of ICT Services

The Financial NIS does not define any ICT services as “*critical*”.

The By-Law ISBEBS and the *Communiqué* on Payment Services mention additional requirements for “*critical information systems*” without providing any definition. However, the By-Law on Remote Identity Verification Methods to be Used by Banks and the Establishment of Contractual Relationships in Electronic Environment classifies the systems used in the context of remote identity verification as critical information systems in terms of the By-Law ISBEBS.

The New CMB *Communiqué* (taking effect on 30 June 2025) does not define “*critical information systems*” either. However, it defines “*criticality*” as “*the quality of the information asset that indicates its importance or necessity in achieving the business objectives of the institution, organisation or company*”. It also sets additional requirements for critical information systems, such as establishing mechanisms to instantly monitor unauthorised access attempts.

3.3 Key Operational Resilience Obligations

As outlined above, there is no overarching digital operation resilience regulation, and the applicable legal requirements are fragmented across several legislative pieces.

The Financial NIS imposes several obligations on the institutions of their respective areas to increase the resilience of financial sector institutions' information systems. Financial NIS aims to establish the standards for strengthening these systems. It provides measures to be taken for information security as well as the management of cyber incidents.

Localisation Obligations

The following entities must keep their primary and secondary information systems in Türkiye:

- banks;
- payment institutions and electronic money institutions;
- insurance and private pension companies (except for services such as email, teleconference or videoconference);
- certain public companies, as well as certain capital markets institutions; and
- financial lease, factoring and finance companies.

For outsourced products or services, the *Communiqué* on Payment Services requires use of local products, or the manufacturers thereof to have R&D centres and response centres in Türkiye.

Risk Management Obligations

Financial sector institutions are required to prepare a plan and policy for the detection, analysis, and management of risks related to information systems. They also impose internal control

mechanisms for the same (eg, approval of senior staff).

Cyber Incident Management and Reporting Obligations

The measures to be taken in the event of a cyber incident include keeping a detailed record thereof, preventing the recurrence of a similar incident, establishing internal mechanisms for cyber incident management, and identifying the root causes of cyber incidents.

Certain details of cyber incidents must be reported to the internal senior staff as well as the relevant institutions (eg, the BRSA, TRCB and Institutional CERTs). Additionally, since the financial sector is one of the critical infrastructure sectors, financial sector institutions must also follow the notification obligations mentioned in 2.3 Incident Response and Notification Obligations.

Other Obligations

For other crucial obligations see 3.2 ICT Service Provider Contractual Requirements, 3.5 International Data Transfers and 3.6 Threat-Led Penetration Testing.

3.4 Operational Resilience Enforcement

The enforcement of the operational resilience obligations outlined above is shared by the BRSA, TRCB, and CMB.

The Banking Regulation and Supervision of Agency (the BRSA)

The BRSA is authorised to carry out examination of all books, records, and documents, and conduct on-site audits and ex officio inspections concerning the support service organisations.

The By-Law ISBEBS also authorises BSRA to carry out inspections concerning the ICT providers of banks and requires them to provide the

necessary information and documents requested and to keep and operate all kinds of records in a readable format.

Moreover, BSRA is authorised to impose administrative fines in case of non-compliance with its regulations in accordance with the Banking Law.

The Turkish Republic Central Bank (the TRCB)

The TRCB is authorised to audit banks, payment institutions, electronic money institutions, and their branches, representatives or outsourced service providers of the Post and Telegraph Organisation A.Ş.

The TRCB may request the payment institution and electronic money institution to take the necessary measures in relation to the issues identified. In case of failure to take these measures in a reasonable time, TRCB may revoke the operating licence.

Depending on the case, TRCB may impose a wide range of administrative fines for non-compliance with the regulations on payment services and electronic money institutions.

The Capital Markets Board (the CMB)

The CMB has the authority to audit the activities concerning capital markets of all institutions and organisations under the scope of the Capital Markets Law and other relevant real or legal persons. The auditing personnel may request relevant documents and information. The failure to provide these and obscuring the audit are criminalised under the Capital Markets Law.

Depending on the case, CMB may impose a wide range of administrative fines on persons who fail to comply with the Capital Markets Law and its secondary legislation.

3.5 International Data Transfers

Banking Law and Its Secondary Legislation

Refer to the localisation obligation under 3.3 Key Operational Resilience Obligations.

Additionally, customer secrets under the Banking Law cannot be disclosed or transferred to foreign (or domestic) third parties without receiving the customer's request or explicit instruction. There are two exceptions.

- Customer secrets can be transferred to authorities that are authorised by Turkish laws.
- Information and documents may be shared to the parent company located abroad, provided that its capital share equals to or exceeds ten percent, and a non-disclosure agreement is signed with the parent company. Even then, only the following information may be shared – preparation of consolidated financial statements, risk management, and internal audit practices.

The By-Law on the Sharing of Secret Information, which applies to bank secrets and customer secrets collectively, also provides exceptions to the prohibition to share secret information. Accordingly, the following transfers are allowed.

- Per a BoD decision to be adopted by the bank, sharing with third parties bank secrets that only contain classified information belonging to the bank.
- The disclosures made to the foreign judicial and alternative dispute resolution authorities or to the parties representing the bank in such disputes, where the disclosure is necessary for the proof of the claim or defence.

Contributed by: Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Özdebakoglu, YAZICIOGLU Legal

The Communiqué on Payment Services

In cases where one of the parties of the payment transaction is located abroad, the institution may share the required data with the relevant third parties abroad. However, the following conditions must be satisfied:

- data must be stored domestically;
- data must be limited to the extent necessary for the performance; and
- the principle of proportionality must be respected.

General DP Law Regime on International Personal Data Transfers

If data transferred is personal data, the DP Law also applies.

Provisions on international personal data transfers under the DP Law have been significantly amended on 12 March 2024, effective from 1 September 2024. The purpose of the amendment was to align the DP Law with the General Data Protection Regulation.

The new regime allows personal data to be transferred abroad or to international organisations under the following conditions.

- Existence of one of the applicable legal bases under the DP Law and an adequacy decision for the country, international organisation or the sectors therein to which the data will be transferred (note that, as of the date of this publication, the DPA has not issued any adequacy decision yet).
- In the absence of an adequacy decision – the existence of one of the applicable legal bases under the DP Law and enforceable data subject rights and effective legal remedies for data subjects and provision of one of the following appropriate safeguards:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules;

(c) standard contractual clauses; or

(d) a written letter of commitment, together with the approval of the transfer by the Board.

- In the absence of an adequacy decision and where appropriate safeguards cannot be provided – the existence of derogations for specific situations outlined in the DP Law, where the transfer is “occasional”.

Although the DPA published the By-Law on Procedures for the Transfer of Personal Data Abroad and a guideline, there are many ongoing discussions on interpreting the provisions therein.

Besides the amendments, there is an unaltered provision under the DP Law, which provides a reservation for provisions under other laws applying to personal data transfers abroad. In the Banking Sector Best Practices Guide on the Protection of Personal Data, the DPA states that where such a specific provision is applicable, it will override the transfer regime under the DP Law.

The provisions explicitly mentioned in the Banking Guide are those on “consumer secrets” under the Banking Law and related secondary regulations. Although not explicitly mentioned, Article 24 under the By-Law on Measures for Preventing Money Laundering and Financing of Terrorism, which provides the minimum information to be included in an international e-transfer, will also apply in a preceding manner.

International Treaties

International treaties to which Türkiye is a party may allow or require banks to transfer data

abroad under some conditions (eg, the Agreement Between the Government of the Republic of Türkiye and the Government of the United States of America to Improve International Tax Compliance requires Turkish financial institutions to report US citizens and residents' data for tax compliance purposes). In these cases, the treaties will have precedence over the local laws according to Article 90(3) of the Constitution. If the transferred data is personal data, the reservation under the DP Law may also be applicable.

3.6 Threat-Led Penetration Testing

The Financial NIS imposes penetration testing obligations for their respective financial sector institutions as detailed below.

The By-Law ISBEBS

Banks must have penetration tests performed at least once a year by independent teams that are not involved in the design, development, implementation or execution of the services provided through information systems.

The Institutional CERTs of banks are also required to conduct routine penetration tests on IT assets, routinely monitor trace records and check for correlations that may lead to meaningful results.

The Communiqué on Payment Services

The *Communiqué* provides the following penetration testing requirements for payment and electronic money institutions.

- They must have regular penetration tests performed at least once a year for scenarios covering possible internal and external threats. The procedure to be followed for penetration testing is provided under the Annex 5 therein.
- They must submit a report to TRCB at least annually, detailing security breaches, penetra-

tion test results, and critical vulnerabilities identified, measures taken to eliminate them and the results thereof.

The CMB Communiqué

The information systems of the related institutions and organisations must have penetration tests performed at least once a year. The procedure to be followed for penetration testing is provided under the Annex 1 therein.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

There is no general legislative instrument on cyber resilience in Türkiye.

Currently, the main regulations on managing cyber incidents are the *Communiqué* on the Procedures and Principles Regarding the Establishment, Duties and Activities of CERTs and MTI's guidelines on establishing institutional and sectoral CERTs. For further information on CERTs, see 1.3 Cybersecurity Regulators.

However, the Presidency Program for 2025 includes a plan to enact legislative regulations in line with the EU's Cyber Resilience Act (CRA). It is possible to expect a cyber resilience regulation in the following years, since cyber resilience is listed as one of the six main objectives of the NCS 2024. In this regard, "*establishing principles to mitigate the possible impacts of cyber incidents*" objective of the Cybersecurity Act indicates at cyber resilience.

According to the Cybersecurity Act, cybersecurity "*encompasses a set of activities aimed at protecting from attacks the information systems that constitute cyberspace, ensuring the confidentiality, integrity, and availability of data processed*

therein, detecting attacks and cyber incidents, activating response and alert mechanisms, and restoring the situation to its state prior to the cyber incident". The last part of this definition seems to include cyber resilience thereunder.

4.2 Key Obligations Under Legislation

The Cybersecurity Act delegates a specific duty to the Cybersecurity Directorate for *"increasing the cyber resilience of critical infrastructures and information systems through vulnerability and penetration tests and risk analysis, cyber-threat intelligence, and malware inspection operations"*.

Currently, the Institutional CERTs are subject to the following resilience-related obligations during and after a cyber incident:

- carrying out their activities to prevent cyber incidents or mitigate damages in co-ordination with their sectoral CERTs, if any;
- notifying the TR-CERT of the situation without delay;
- reporting cyber incidents to their institutions, notifying the TR-CERT and their sectoral CERTs without delay;
- primarily trying to eliminate a cyber incident with their own means and capabilities, and requesting assistance from the TR-CERT and their sectoral CERT, as applicable;
- reporting to the competent authorities and the TR-CERT without delay, if there is doubt that a crime has been committed during the intervention of a cyber incident;
- having 24/7-accessible contact information and notifying their sectoral CERTs and the TR-CERT thereof;
- identifying and keeping record of the vulnerability that led to the incident immediately;
- measuring and monitoring the types, quantities and costs of cyber incidents; and

- submitting to the management of the institution for corrective/preventive actions that can be taken in relation to the incident.

The Sectoral CERTs, on the other hand, have the following obligations:

- carrying out activities for preventing cyber incidents or mitigating their damages in co-ordination with the TR-CERT;
- notifying the TR-CERT of cyber incidents experienced by their CERTs without delay;
- having 24/7-accessible contact information and notifying their CERTs and the TR-CERT thereof;
- supporting their CERTs in cyber incidents; and
- reporting to the competent authorities and the TR-CERT without delay, if there is doubt that a crime has been committed during the intervention of a cyber incident.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

Currently, there is no general legal framework for certification requirements of ICT products and services. However, there are sector-specific legislation with certification requirements.

The Cybersecurity Act provides certain certification requirements. According to the Cybersecurity Act, cybersecurity products, systems and services to be used in public institutions and organisations and critical infrastructures have to be procured from cybersecurity experts and companies who will be certified by the Cybersecurity Directorate. Procurement from uncertified experts or companies will be subject to an

administrative fine between TRY1 million and TRY10 million.

TS ISO/IEC 27001 Certificate

In the e-communications and energy sector, and for e-invoice service providers, obtaining a TS ISO/IEC 27001 certificate is a de jure standard. However, many other organisations also choose to voluntarily comply with this standard as a good practice to improve cybersecurity.

The Financial Sector

- The BRSA requires all banks to meet Control Objectives for Information and Related Technologies (COBIT) standards. COBIT process management is used not only in banks but also in the finance and production sectors.
- The By-Law on Banking Cards and Credit Cards require organisations entering into merchant agreements with banks to comply with the Payment Card Industry Data Security Standards (PCI DSS) standards.
- According to the CMB's *Communiqué* on Independence Audit of Information Systems, auditors who audit publicly held companies must have a Certified Information System Auditor (CISA) certificate.

The Healthcare Sector

The By-Law on Health Information Management Systems requires health information systems' service providers to have following certificates:

- TS ISO/IEC 27001;
- TS ISO/IEC 15504 Software Process Improvement and Capability Determination (SPICE) certificate at a minimum of the second level, which is obtained from institutions and organisations with TS ISO/IEC 17065 accreditation and include SPICE lead auditor; or

- CMMI certificate at a minimum of the third level, which is obtained from institutions or companies with CMMI lead auditor.

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

Data controllers are obliged to provide an appropriate level of security for the personal data they process. Hence, data controllers must ensure that their processors provide a level of security for personal data that is, at minimum, equivalent to their own. Data controllers are also held liable for the security measures taken by data processors. They may conduct or commission the necessary audits on their processors' systems containing personal data, review the results, and inspect the data processor on-site.

The DPA issued the Guideline on Personal Data Protection (Technical and Organisational Measures) (the "*Measures Guideline*") in 2018, which lists and details the technical and administrative measures to be taken by data controllers. The guideline suggests the following cybersecurity-related measures:

- using a firewall and internet gateway;
- patch management;
- software updates;
- limiting access to systems containing personal data;
- using strong passwords for such systems;
- creating an access control matrix;
- using brute force algorithm (BFA);
- using antivirus, antispam and similar products that regularly scan the information system network and detect potential threats; and

Contributed by: Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Özdebakoglu, YAZICIOGLU Legal

- using SSL or more secure methods for data collection from different websites and/or mobile application channels.

There are stricter requirements for the processing of special categories of data per the DPA Decision No 2018/10. The DPA may also specify case-specific measures in its published decisions.

Administrative fines for failure to take necessary technical and organisational measures (interpreted very broadly, including unlawful data transfer abroad and violation of fundamental principles) range between TRY204,285 and TRY13,620,402 for 2025.

Also refer to the data breach notification duty explained under **2.3 Incident Response and Notification Obligations**, where failing to comply with this obligation results in a data breach.

6.2 Cybersecurity and AI

Currently, there is no legislation in Türkiye regulating AI or providing obligations regarding AI.

However, on 5 October 2024, the Turkish Parliament published a decision on the establishment of a parliamentary research commission to determine the steps to be taken toward the achievements of AI, to establish a legal infrastructure in this field and to determine measures to prevent the risks of the use of AI. Members of this commission were elected recently. However, there is no public information on the progress of the commission's work.

In addition, a proposal for an AI Act was submitted to parliament on 25 June 2024. The proposal included provisions on risk management in production and use of AI and auditing AI operators. Although its approval is unlikely, it marks a sig-

nificant milestone as the first legislative initiative in this field.

The DTO's National Artificial Intelligence Strategy for 2021–2025

The strategy is a framework document outlining strategic priorities, goals and measures. The strategic priorities are as follows:

- training AI experts and increasing employment in the field of AI;
- supporting research, entrepreneurship and innovation;
- broadening access opportunities to quality data and technical infrastructure;
- taking regulatory actions to expedite socio-economic compliance;
- strengthening co-operation at the international level; and
- expediting structural and workforce transformation.

The Action Plan of National Artificial Intelligence Strategy for 2024–2025 includes the following:

- improving the data governance regulations in the AI ecosystem;
- enacting a national regulation on the development and use of AI systems and the market supply of systems containing AI, which follows international norms;
- preparing a Legal Evaluation Guide for AI Applications; and
- developing an AI Values and Principles Impact Analysis Framework.

There are recommended security measures concerning AI under the following documents:

Contributed by: Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Özdebakoğlu, YAZICIOGLU Legal

The DTO's Report on Chatbot Applications and the Case of ChatGPT

The report provides information on security risks and methods to reduce them. These methods include:

- authentication and authorisation;
- end-to-end encryption;
- self-deleting messages;
- configuration of user control and access rights; and
- proper storage of chat history.

Recommendations by the DPA

The DPA's informational document on chatbots highlights:

- the importance of transparency in AI chatbot applications;
- the potential risks, such as over-sharing of personal data by the data subjects and cyber incidents; and
- the need for special protection for minors.

The following measures are suggested to be taken while developing a chatbot application:

- complying with internationally recognised standards, having certificates, and ensuring privacy by default at every stage in the development process thereof; and
- in data communication, preferring secure methods for transmitting inputs such as text, voice, speech and images to the hosting environments.

Finally, the DPA's *"Recommendations on Data Protection in the Context of Artificial Intelligence"* consists of data protection-related recommendations for developers, producers, service providers, and decision-makers vis-à-vis AI systems.

6.3 Cybersecurity in the Healthcare Sector

The Directive on the Information Security Policies of the Ministry of Health ("MoH InfoSec Directive") and the Guideline for Information Security Policies ("MoH InfoSec Guideline")

The MoH InfoSec Directive and MoH InfoSec Guideline were published by Health Information Systems General Directorate (HISGD) under the Ministry of Health, which was established to regulate information systems and communication technologies that are used in the healthcare sector.

MoH InfoSec Directive establishes the Information Security Management Commission and sub-commissions that are responsible for information security and cyber incident management across all central and provincial organisations of the Ministry of Health.

It also establishes the sectoral CERT for the healthcare sector and requires the appointment of an information security officer. Moreover, the MoH InfoSec Directive tasks HISGD with the management of information security breaches and auditing information security.

For details of the certification obligation for service providers of health information systems, see **5.1 Key Cybersecurity Certification Legislation.**

The By-Law on Personal Health Data

In addition to the provisions under the DP Law pertaining to special categories of personal data, the By-Law on Personal Health Data provides the specific procedure to be followed by health-care providers while processing health data.

It covers accessing, securing, rectifying, destroying, and transferring health data. It emphasises

the data security measures required by the DP Law and requires taking the information security measures under the MoH InfoSec Directive. In addition, using KamuNet to transfer health data – where technical infrastructure allows – is required.

The Guide on Protection of Personal Data in Pharmacovigilance Activities

Health data is also protected in the context of the R&D process of medicines. In this regard, the Turkish Medicines and Medical Devices Agency published the Guide on Protection of Personal Data in Pharmacovigilance Activities. It specifies the technical and organisational measures for the security of the data processed in pharmacovigilance activities, such as:

- personnel training for the first intervention regarding cybersecurity;
- setting up a firewall;
- using an internet gateway;
- using antivirus and antispam software;
- removing software with vulnerabilities and unused software;
- patch management and software updates;
- limiting access to systems containing personal data;
- checking which software and services are running on information networks;
- determining whether there is penetration or unexpected movements in information networks;
- keeping a regular record of all users' activity (such as log records);
- establishing an official reporting procedure for security issues;
- reporting security issues to the data controller as quickly as possible;
- collecting and storing evidence in case of cyber incidents;
- preferring to use internationally recognised encryption programs;
- ensuring security of environments containing personal data; and
- taking measures such as 2FA and encrypting with cryptographic methods in case of storing in a cloud.



Law and Practice

Contributed by:

William Long, Francesca Blythe, Eleanor Dodding and Anila Rayani
Sidley Austin LLP

Contents

1. General Overview of Laws and Regulators p.321

- 1.1 Cybersecurity Regulation Strategy p.321
- 1.2 Cybersecurity Laws p.321
- 1.3 Cybersecurity Regulators p.323

2. Critical Infrastructure Cybersecurity p.324

- 2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.324
- 2.2 Critical Infrastructure Cybersecurity Requirements p.325
- 2.3 Incident Response and Notification Obligations p.325
- 2.4 State Responsibilities and Obligations p.326

3. Financial Sector Operational Resilience Regulation p.326

- 3.1 Scope of Financial Sector Operational Resilience Regulation p.326
- 3.2 ICT Service Provider Contractual Requirements p.327
- 3.3 Key Operational Resilience Obligations p.327
- 3.4 Operational Resilience Enforcement p.328
- 3.5 International Data Transfers p.328
- 3.6 Threat-Led Penetration Testing p.329

4. Cyber-Resilience p.329

- 4.1 Cyber-Resilience Legislation p.329
- 4.2 Key Obligations Under Legislation p.329

5. Security Certification for ICT Products, Services and Processes p.332

- 5.1 Key Cybersecurity Certification Legislation p.332

6. Cybersecurity in Other Regulations p.332

- 6.1 Cybersecurity and Data Protection p.332
- 6.2 Cybersecurity and AI p.334
- 6.3 Cybersecurity in the Healthcare Sector p.334

Sidley Austin LLP is a premier global law firm with a practice highly attuned to the ever-changing international landscape. The firm advises clients around the globe and has more than 2,300 lawyers in 21 offices worldwide. Sidley Austin maintains a commitment to providing quality legal services and offering advice on litigation, transactional and regulatory matters spanning virtually every area of law. The firm's lawyers have wide-reaching legal backgrounds and are dedicated to teamwork, collaboration, and superior client service. The team helps a

range of businesses address some of the most challenging matters concerning data protection, privacy, information security and incident response, data commercialisation, internet and computer law, IP, information management and records retention, e-commerce, consumer protection, and cybercrime. Sidley Austin advises clients with extensive operations in Europe – as well as in the USA, Asia and elsewhere – on developing and implementing global data protection programmes.

Authors



William Long is a partner at Sidley Austin LLP, where he leads the EU and UK data protection practice and is global co-leader of the firm's highly ranked privacy and

cybersecurity practice. William advises international clients on a wide variety of AI, cyber, and digital data laws, as well as data protection, privacy, information security, social media, e-commerce and other regulatory matters. He has been a member of the International Association of Privacy Professionals (IAPP)'s European Advisory Board and on the DataGuidance panel of data protection lawyers. William has also been on the editorial board of "e-Health Law & Policy" and assists with dplegal, a network for privacy professionals.



Francesca Blythe is a partner at Sidley Austin LLP and advises international clients on a wide range of privacy, cybersecurity, and emerging technology issues, including on privacy and

cybersecurity compliance strategies. She has also counselled clients in preparing for, and responding to, data breaches of varying sizes. Francesca co-leads Sidley Austin's benchmarking group for in-house data privacy professionals (dplegal) in the life sciences sector and was previously in-house counsel at the largest international health and beauty retailer in Asia and Europe. While there, she regularly gave advice on compliance and strategies relating to data protection laws and assisted in the planning and delivery of a global privacy compliance project.

Contributed by: William Long, Francesca Blythe, Eleanor Dodding and Anila Rayani, **Sidley Austin LLP**



Eleanor Dodding is a senior managing associate at Sidley Austin LLP. She provides practical and strategic advice to international clients regarding the EU and UK General Data

Protection Regulation, e-privacy laws, international data transfers (including with regard to the Schrems II decision), and sector-specific privacy and cybersecurity laws. Eleanor also has experience in assisting clients with preparing for, and responding to, cybersecurity incidents.



Anila Rayani is an associate at Sidley Austin LLP. She advises international clients on various data protection, privacy, and cybersecurity matters, including the EU and UK General Data

Protection Regulation, e-privacy laws, and emerging AI and cyber frameworks. Anila also has experience investigating and responding to complex cross-border cybersecurity incidents and personal data breaches, as well as dealing with regulatory inquiries.

Sidley Austin LLP

70 St Mary Axe
London
EC3A 8BE
UK

Tel: +44 020 7360 3600
Fax: +44 020 7626 7937
Web: www.sidley.com

SIDLEY

1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

The UK cybersecurity legal system is well developed and is similar to the legal systems across the European Economic Area (EEA), rather than the USA – although post-Brexit, divergence in approach to cybersecurity regulation by the EU and the UK are starting to emerge. Since the GDPR came into force in 2018, the enforcement of cybersecurity rules in the UK continues to be a focus, particularly by the UK data protection regulator, the Information Commissioner's Office (ICO). In 2025, the UK looks set to introduce new legislation to address the changing cyberthreat landscape and more closely align UK law with developments in the EU (such as the Network and Information Systems Directive 2 (the "NIS 2 Directive")) – see **2. Critical Infrastructure Cybersecurity** for further detail.

The UK government has also signalled an overhaul of its ability to assist and promote cybersecurity through its national cyber strategy for 2022 (the "National Cyber Strategy"), as well as through its government-specific Government Cyber Security Strategy for 2022–30. The National Cyber Strategy takes a "whole of society" approach, with the aim of shifting the burden of cybersecurity from individual citizens to the organisations and professionals best placed to manage cyber-risks. The National Cyber Strategy is comprised of five pillars, which it is working to achieve by 2025:

- strengthening the UK cyber ecosystem – by investing in people and skills, and deepening the partnership between government, academia and industry;
- building a resilient and prosperous digital UK – by reducing cyber-risks so that businesses

can maximise the economic benefits of digital technology and provide more security for UK citizens online;

- taking the lead in technologies vital to cyber power – by building industrial capacity and developing frameworks to secure future technologies;
- advancing UK global leadership and influence for a more secure, prosperous and open international order – by working with government and industry partners and sharing the expertise that underpins UK cyber power; and
- detecting, disrupting and deterring adversaries to enhance UK security in and through cyberspace – by making more integrated, creative and routine use of the UK's full spectrum of levers.

The National Cyber Strategy also proposes a number of regulatory reforms, including but not limited to increasing the scope of the Network and Information Systems Regulations (the "NIS Regulations") (see **2. Critical Infrastructure Cybersecurity** for further detail).

1.2 Cybersecurity Laws

The UK has a well-developed – and growing – network of civil and criminal laws relating to cybersecurity, contained in UK legislation, companion rules made under such legislation, decisions of UK courts, and a steady stream of regulatory guidance from UK regulators.

Key cybersecurity requirements imposed on organisations in the UK, or on organisations that are established outside the UK but are processing personal data of individuals located in the UK, are derived from the UK General Data Protection Regulation (the "UK GDPR"), as supplemented by the UK Data Protection Act 2018 (DPA).

The UK GDPR applies to the security of “personal data” (ie, any information relating to an identified or identifiable individual who can be identified – directly or indirectly – by reference to an identifier such as a name, an identification number, location data or an online identifier). As such, only those cybersecurity incidents impacting personal data will be regulated by the UK GDPR (see also **6.1 Cybersecurity and Data Protection**). The UK GDPR requires organisations to maintain “appropriate” technical and organisational security measures and to comply with certain notification obligations when “personal data breaches” occur. The DPA also allows for criminal prosecutions to be brought for certain cybersecurity-related breaches.

Secondly, the NIS Regulations currently apply to two categories of key infrastructure operators – namely, “operators of essential services” (OESs) and “relevant digital service providers” (RDSPs). Like the UK GDPR, the NIS Regulations require organisations that are subject to them to implement certain cybersecurity measures and to report certain cybersecurity incidents that affect such organisations. On 17 July 2024, the UK government announced the Cybersecurity and Resilience Bill (the “CS&R Bill”), which would expand the remit of the NIS Regulations to protect more digital services and supply chains. Please see **2.1 Scope of Critical Infrastructure Cybersecurity Regulation** for additional information on the proposed updates to the NIS Regulations via the CS&R Bill.

Thirdly, the Product Security and Telecommunications Infrastructure Act 2022 (the “PSTI Act”), which came into force on 29 April 2024, requires manufacturers, importers and distributors of UK consumer-connected products to meet certain cybersecurity standards. This includes more stringent security requirements (eg, default

password requirements and minimum support periods for providing security updates) and requirements to investigate any compliance failures and take remediation action, as well as notify relevant authorities and other third parties about such compliance failures (see **4.2 Key Obligations Under Legislation**).

Fourthly, the Computer Misuse Act 1990 (CMA) is the UK’s primary legislation with regard to criminalising unauthorised access to computers and other IT systems. It contains a number of cybersecurity-related offences. A key offence under the CMA (Section 1) is where a defendant obtains “unauthorised access” to a computer – ie, the defendant causes a computer “to perform any function with intent to secure access to any program or data held in any computer” or “to enable such access to be secured” where such access is “unauthorised” and this is known to the defendant at the relevant time.

Fifthly, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the “PECR”), the EU Notification Regulations 611/2013 (the “Notification Regulation”), and the Communications Act 2003 (the “CA 2003”) contain cybersecurity obligations applicable primarily to electronic communications networks and service operations (such as telecommunications systems operators).

There are also sector-specific laws that contain cybersecurity obligations – for example, Financial Conduct Authority (FCA) rules (applicable to FCA-regulated firms), the Payment Services Regulations 2017 (PSRs) (which transposed the Second EU Payment Services Directive into English law and apply to payment service providers), and the Official Secrets Act 1989 (OSA) (which is applicable to certain official government information). Similarly, the Investigatory Powers Act

2016 (IPA) and the Regulation of Investigatory Powers Act 2000 (RIPA) regulate electronic surveillance and interception in the UK and contain associated safeguards.

These laws are increasingly being enforced by UK governmental authorities – including the ICO and sector-specific regulators such as the FCA – and private individuals and organisations. Regulators are also increasingly collaborating on cybersecurity enforcement; examples include the ICO teaming up with the Competition and Markets Authority, the Office of Communications (Ofcom) and the FCA to form the Digital Regulation Co-operation Forum (DRCF).

In addition to legislation, English “common law” contains rules that are relevant to cybersecurity. There is a legal and ethical duty of confidence where information is shared in confidence and must not be disclosed without legal authority. The duty applies to information not already in the public domain and is subject to a number of exceptions, including where disclosure:

- has been consented to by the discloser; or
- is required by law.

The FCA rules, the PSRs, the OSA, the IPA, the RIPA and other sector-specific or specialised laws or the common-law duty of confidence are not further considered in this guide.

1.3 Cybersecurity Regulators

There are different UK regulators for each of the key UK cybersecurity legislations under consideration.

UK GDPR and DPA

In the UK, the ICO is responsible for monitoring the application of the UK GDPR and the DPA and taking enforcement action against organisa-

tions for non-compliance with such legislation, including investigating personal data breaches and inadequate security measures. The ICO may initiate an investigation of its own accord or on the basis of a complaint submitted by, for example, a private individual or organisation. The ICO also has the power to conduct both off-site and on-site audits. Please note that prosecutions under the DPA can only be brought by the ICO or by (or with the consent of) the Director of Public Prosecutions (DPP).

NIS Regulations

With regard to the NIS Regulations, the “competent authority” is determined on an industry-by-industry basis through the Department for Science Innovation and Technology (DSIT), which oversees the implementation of the NIS Regulations across the UK. For OESs in the oil sector, for example, the competent authority in England, Scotland and Wales is the Secretary of State for Business, Energy and Industrial Strategy – whereas in Northern Ireland it is the Department of Finance. The ICO is the competent authority for RDSPs.

Competent authorities may be reactive or proactive in terms of the incidents they choose to investigate and they are supported by the National Cybersecurity Security Centre (NCSC), which offers technical advice (except in health-care, where this support is offered by NHS Digital). Certain organisations are also subject to regular compliance audits from their relevant competent authority – failing these audits can lead to fines of up to GBP17 million.

PECR and CA 2003

As regards the PECR, the ICO may audit the compliance of service providers pursuant to Regulation 5A of the PECR. Notifiable personal data breaches under Regulation 5A of the PECR

must be reported to the ICO. The ICO is, in turn, responsible for investigating the breach and taking any subsequent enforcement action.

However, with regard to the CA 2003 (which is a companion legislation to the PECR), Ofcom is the primary regulator. Pursuant to Section 105C of the CA 2003, Ofcom may carry out an audit of the security measures taken by a network provider or a service provider under Section 105A. Notifiable security breaches under Section 105 of CA 2003 must be reported to Ofcom, which is in turn responsible for investigating the breach and taking any subsequent enforcement action.

CMA

Although there is no regulatory authority with oversight of the CMA per se, the provisions of the CMA are enforced by the UK Crown Prosecution Service (CPS), which is the public authority responsible for prosecuting the majority of criminal cases in the UK. The CPS is notified of CMA investigations and potential offences by the police and other investigative organisations in England and Wales. See **4.2 Key Obligations Under Legislation** for more information.

PSTI

The Office for Product Safety and Standards is responsible for enforcing the PSTI Act. Non-compliance with the PSTI Act can result in fines of up to GBP10 million or 4% of a company's global turnover (whichever is greater), as well as up to GBP20,000 per day in the case of an ongoing contravention.

National Cybersecurity Security Centre

The NCSC is the key UK cybersecurity agency, co-ordinating UK cybersecurity policy and technical standards, particularly with regard to the NIS Regulations and the UK GDPR. The NCSC acts as the national computer security incident

response team (CSIRT) under the NIS Regulations and supports organisations that suffer cybersecurity incidents. It also acts as a “single point of contact” for competent authorities under the NIS Regulations. Following Brexit, the UK has forfeited its position on the EU Agency for Cybersecurity (ENISA); however, some operational co-operation continues in order to allow for improved cybersecurity across Europe.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

The regulation of cybersecurity for critical infrastructure in the UK is primarily governed by the NIS Regulations. See **1.2 Cybersecurity Laws** for a summary of the scope of the NIS Regulations.

On 17 July 2024, the UK government introduced the CS&R Bill, intended to strengthen UK defences against cyber-attacks and protect critical infrastructure. The briefing note on the CS&R Bill suggests it will update the UK's cyber regulatory framework by:

- expanding the scope of the NIS Regulations to cover “more digital services and supply chains”;
- giving further power to regulators to ensure measures are being implemented; and
- mandating increased incident reporting to provide a better picture of the threat landscape and cyber-attacks.

It is expected that the CS&R Bill will be introduced in Parliament in 2025.

2.2 Critical Infrastructure Cybersecurity Requirements

OESs and RDSPs are required under the NIS Regulations to implement appropriate and proportionate technical and organisational measures to ensure a level of security appropriate to the risk posed.

RDSPs

For RDSPs, these requirements are supplemented by the Commission Implementing Regulation (EU) 2018/151 (the “DSP Regulation”). In summary, RDSPs must take account of the following.

- The security of systems and facilities – measures in this area should cover systematic management of network and information systems, physical and environmental security measures, security of supplies and access controls to systems.
- Incident handling – measures should include incident detection processes and procedures, processes and policies on incident reporting, incident response and incident assessment. See 2.3 **Incident Response and Notification Obligations** for further detail.
- Business continuity management – this is the capability to maintain or restore the delivery of services to acceptable predefined levels following a disruptive incident.
- Monitoring, auditing and testing – measures should establish and maintain policies and processes concerning the assessment, inspection and verification of systems.
- Compliance with international standards – measures are not specified by the DSP Regulation but, instead, the NIS Regulations refer to “standards” as:
 - (a) standards adopted by an international standardisation body as specified in Regulation 1025/2012; and/or

- (b) any European, national, or internationally-accepted standards and specifications relevant to the security of networks and information systems.

The ICO notes that examples of appropriate standards may include ISO/IEC 27001 on information security management systems and ISO/IEC 22301 on business continuity management systems, as well as any other related standards.

OESs

OESs are subject to similar requirements as RDSPs in that they must also take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies, and subject to guidance from the relevant competent authority (which, as noted in 1.3 **Cybersecurity Regulations** (NIS Regulations), is on a sector-specific basis).

2.3 Incident Response and Notification Obligations

Under the NIS Regulations, different incident reporting obligations apply to OESs and RDSPs respectively.

For OESs, cybersecurity event notification is required when any incident has a “significant impact” on the continuity of the essential service that the OES provides. Determining this requires a fact-specific analysis of the number of users affected by the disruption of the service, the duration of the incident, and the geographical area affected by the incident, as well as any other relevant guidance issued by their designated “competent authority”.

For RDSPs, notification is required where there will be a “substantial impact” on the provision of

any relevant service. As from 12 January 2022, the ICO (which is the lead regulator for RDSPs) must be notified by an RDSP where there is an incident that has a substantial impact on the provision of any digital services, including online marketplaces, online search engines and cloud computing services. It should be noted that, in comparison with the UK GDPR, notifiable incidents under the NIS Regulations need not always involve personal data – that is, cybersecurity incidents that do not involve personal data (such as cyber-attacks on industrial control systems) could be notifiable under the NIS Regulations, but would not be notifiable under the UK GDPR if they do not involve personal data.

Under the NIS Regulations, as with the UK GDPR, OESs and RDSPs must notify their relevant competent authority and the ICO respectively of an incident “without undue delay” and, in any event, no later than 72 hours after the OES or RDSP (as applicable) becomes aware of the incident.

The NIS Regulations require that OESs and RDSPs adopt “appropriate and proportionate” technical and organisational security measures, as well as “appropriate” measures to prevent and minimise the impact of incidents affecting those systems (taking into account the state of the art), so as to ensure the continuity of the essential services that the OES provides. Although serious incidents must be reported under the NIS Regulations, the ICO has also explained that software vulnerabilities – ie, weaknesses in a system that can be exploited by an attacker – may also need to be reported, as per the “additional information” required in the ICO’s NIS reporting form.

2.4 State Responsibilities and Obligations

This not applicable in the UK.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

In the UK, operational resilience in the financial sector is primarily addressed by the FCA, the Prudential Regulatory Authority (PRA) and the Bank of England in their rules and guidance on requirements to strengthen operational resilience in the financial services sector – for example, the FCA’s rules on operational resilience under Chapter 15A of its Senior Management Arrangements, Systems and Controls Sourcebook and the PRA’s supervisory statement “Operational resilience: Impact tolerances for important business services” (SS1/21) (collectively, the “Operational Resilience Requirements”), which were published on 31 March 2022 and address how firms identify, map, test and enhance their important business services to withstand disruptions. The requirements for UK firms to have performed mapping and testing so that they are able to remain within impact tolerances for each important business service are required to be in place by no later than 31 March 2025. The rules are intended to align closely (albeit not entirely) with international standards and other regimes, such as the EU’s Digital and Operational Resilience Act (DORA).

In November 2024, the FCA and the PRA published a joint policy statement, “Operational resilience: Critical third parties to the UK financial sector” (PS16/24) (the “CTP Policy Statement”). This confirmed that operational resilience remains a priority for the regulators and focuses, among other things, on further defining obligations with regard to critical third parties (CTPs) (see 3.2 ICT Service Provider Contractual Requirements for further detail).

3.2 ICT Service Provider Contractual Requirements

As noted in 3.1 **Scope of Financial Sector Operation Resilience Regulation**, CTPs are a key focus of UK financial services operational resilience. The CTP Policy Statement introduces new rules that will apply to a CTP designated under the regime.

Under the applicable rules, CTPs will need to:

- meet the minimum resilience standards in respect of any material services that they are providing to financial services firms;
- comply with six “fundamental rules” that will apply to all the services a CTP provides, including having effective risk strategies and dealing with the FCA or PRA (as applicable) in a co-operative manner; and
- comply with eight “operational risk and resilience requirements” that will apply to a CTP’s material services, such as the requirement to appropriately manage incidents that may adversely affect (or may reasonably be expected to adversely affect) the delivery of a material service.

The new regime for CTPs was created under the Financial Services and Markets Act 2023, which amended the Financial Services and Markets Act 2000 (FSMA). The relevant provisions allow the UK Treasury to designate a person who provides services to regulated firms and financial market infrastructures as “critical”. CTPs will typically be service providers that provide certain outsourced and third-party services to large numbers of financial institutions and whose services are very difficult to substitute. Although the concepts in FSMA are broadly analogous to DORA, the criteria for designation and the scope of regulatory powers differ in several important respects.

3.3 Key Operational Resilience Obligations

The FCA has demonstrated a strong focus on cybersecurity in the context of the financial services industry. This is particularly relevant in the context of:

- Principle 3 (Management and Control) of the FCA Handbook’s Principles for Businesses, which states that “a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems”; and
- Principle 11 (Relations with Regulators), which requires that “a firm must deal with its regulators in an open and co-operative way, and must disclose to the FCA appropriately anything relating to the firm of which that regulator would reasonably expect notice”.

In relation to Principle 11, the FCA has confirmed that regulated firms must report material cyber-incidents. The FCA considers that an incident may be material if it:

- results in significant loss of data or the availability or control of a firm’s IT systems;
- affects a large number of customers; and
- results in unauthorised access to, or malicious software present on, a firm’s information and communication systems.

The FCA goes on to require that where such an incident is deemed to be material:

- the FCA (and the PRA for dual-regulated firms) should be notified;
- if the incident is criminal, Action Fraud (the UK’s national fraud and cybercrime reporting centre) should be contacted; and

- where the incident is also a personal data breach, organisations may need to report the incident to the ICO.

The FCA also recommends that firms refer to the NCSC guidance on reporting incidents and reports should be shared on the Cyber Security Information Sharing Partnership (CiSP) platform. The CiSP is a key information-sharing organisation in the UK. It is a joint industry and UK government initiative managed by the NCSC. The CiSP allows members to voluntarily exchange cyber-risk information in a secure environment, such that there are reductions to the impact of cyber-risks for UK businesses in general.

More generally, and as part of the FCA's goal to assist firms in becoming more resilient to cyber-attacks, it recommends that firms of all sizes should develop a "security culture" and be able to identify and prioritise information assets and constantly evolve to meet new threats.

In addition, certain categories of FCA-regulated firms have additional reporting requirements. By way of example, payment services providers are required to report major operational and security incidents pursuant to the PSRs.

For CTPs, the rules established by CTP Policy Statement introduce a phased approach to notifications in relation to incidents affecting CTP services, such as those that impact the availability, authenticity, integrity, or confidentiality of assets. This reporting will consist of:

- an initial notification, without undue delay, to the relevant parties after the CTP is aware that the relevant incident has occurred;
- one or more intermediate incident reports as needed; and
- a final incident report.

Looking forward, the Operational Resilience Requirements will require financial services firms to comply with a number of obligations around operational resilience, including:

- performing mapping and scenario testing (including for cyber-related disruptions);
- investing to enable a firm to operate within its impact tolerances and respond effectively and recover quickly when disruption does occur;
- documenting and maintaining operational resilience policies and procedures;
- assigning clear roles and responsibilities within the firm; and
- engaging with key stakeholders (eg, regulators, clients, suppliers, and CTPs).

On 13 December 2024, the PRA and FCA published further consultation papers – respectively, "Operational resilience: Operational incident and outsourcing and third-party reporting" (PRA CP17/24) and "Operational Incident and Third-Party Reporting" (FCA CP24/28). These propose a framework for reporting operational incidents and notification and reporting of material third-party arrangements. Under the proposals, the PRA and FCA will expect firms to report incidents meeting certain thresholds. The consultation papers are open for comments until 13 March 2025.

3.4 Operational Resilience Enforcement

The FCA and PRA have a broad legislative mandate and powers to enforce rules made under the CTP regime against designated CTPs. As this is a new regime, it remains to be seen how such powers will be exercised.

3.5 International Data Transfers

This is not applicable in the UK.

3.6 Threat-Led Penetration Testing

See 3.3 Key Operational Resilience Requirements for the upcoming Operational Resilience Requirements, which will include testing requirements.

In addition, the CBEST programme is a cyber-assessment tool to assist UK firms with assessing the cyber-resilience of key financial institutions through security testing performed in “live” corporate environments. On 13 December 2024, the FCA (together with the Bank of England and the PRA) published their annual CBEST thematic report (the “CBEST Report”). The CBEST Report contains cyber-resilience good practice recommendations and insight, including from the NCSC, for firms to help them maintain their operational resilience. The good practice recommendations are the result of a programme that assesses the cyber-resilience of systemic financial institutions through live testing. The report highlights the importance of building a strong foundation of cyberhygiene to prevent common cyber-incidents, including training and awareness and robust authentication.

The key areas of focus based on the 2024 CBEST Report are:

- cybersecurity risks to assets and individuals;
- cyber-risk management and impact-based approaches to the protection of key resources (people, process, technology and data);
- detection and response capabilities leveraging the latest threat intelligence; and
- cyber-incident response to eradicate threats and mitigate impacts.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

As outlined in 1.2 Cybersecurity Laws, there are a number of laws that supplement the UK’s cyber-resilience strategy alongside the NIS Regulations. Please refer to 4.2 Key Obligations Under Legislation for more information.

4.2 Key Obligations Under Legislation PSTI Act

Under this new act, manufacturers (the person responsible for manufacturing a product, designing a product or otherwise marketing the product under their own name or trade mark) of “UK consumer connectable products” are required to comply with new obligations to manage cybersecurity risk for connected products made available in the UK. Similar obligations also apply to importers and distributors. These include:

- duty to comply with security requirements as defined by the Secretary of State;
- duty to investigate and take action in relation to compliance failures – this may include preventing the product from being made available in the UK and/or remedying the compliance failure and notifying enforcement authorities, other manufacturers, importers and distributors; and
- duty to maintain records of investigations and compliance failures for a minimum of ten years – these records may be requested by the Secretary of State in the course of investigating and enforcing the legislation.

The PSTI Act provides for the power of the Secretary of State to deem compliance with security requirements. This is further elaborated in the Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023 (the

“PSTI Regulations”), which set out conditions for deemed compliance with security standards, including compliance with relevant parts of ETSI EN 303 645 or – in some cases – ISO/IEC 29147.

Schedule 1 of the PSTI Regulations includes the following security requirements for manufacturers:

- all UK consumer connected products passwords must be unique and incapable of being reset to any universal factory setting;
- manufacturers, importers and/or distributors of UK consumer-connected products must provide a public point of contact for reporting vulnerabilities and these must be acted on in a timely manner; and
- manufacturers, importers and/or distributors of UK consumer-connected products explicitly state the minimum length of time for which the device will receive security updates at the point of sale.

CMA

As mentioned in **1.2 Cybersecurity Laws**, a key offence under the CMA (Section 1) is where a defendant obtains “unauthorised access” to a computer. Although the CMA primarily applies to offences committed within the UK, it allows for prosecutions to be brought in the UK where some or all of the offending acts were committed outside the UK – reflecting the trans-border nature of many cybersecurity-related offences. By way of example, Section 1 of the CMA can apply to offending acts committed outside the UK and can – as a result – be prosecuted in the UK where there is “at least one significant link with the domestic jurisdiction”. A significant link can include where:

- the accused is in a relevant country of the UK (England, Wales, Scotland and Northern Ireland) at the time of the offence;
- the target of the CMA offence is in a relevant country of the UK; or
- the technological activity that has facilitated the offending may have passed through a server based in a relevant country of the UK.

An offence committed under the CMA is prosecuted through the UK courts by the CPS. When determining whether to bring a prosecution under the CMA, the CPS must be satisfied that there is enough evidence to provide a “realistic prospect of conviction” against each defendant and that the public interest factors tending against prosecution outweigh those tending in favour. Offences under the CMA can carry imprisonment or a fine (or both). In addition, a serious crime prevention order can be made against an individual or an organisation in relation to a breach of the CMA.

The UK government continues to progress amendments to the CMA, as for many years commentators have stated that the CMA has failed to keep pace with the cybersecurity landscape. Commentators highlight issues with the ambiguity around the meaning of “authorisation” and its subsequent impact on cybersecurity professionals, as well as issues with the current jurisdictional scope of the CMA, given the international nature of many cybersecurity incidents. In November 2023, the UK government published responses to a consultation on proposed CMA reforms, noting that work will continue on engagement with private and public sector organisations to understand further impacts and mitigations in this area before it is considered for legislation.

PECR and CA 2003

Regulation 5(1A) of the PECR requires service providers to:

- restrict access to personal data to only authorised personnel;
- protect personal data against “accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure”; and
- implement a security policy with regard to the processing of personal data.

Service providers are also required to retain a log of the personal data breaches pursuant to Regulation 5A(8) of the PECR.

Guidance on Security Requirements published by Ofcom in relation to the CA 2003 states that it is necessary to establish “clear lines of accountability, up to and including board or company director level, and sufficient technical capability to ensure that potential risks are identified and appropriately managed”. The guidance further states that “a level of internal security expertise, capacity, and appropriate accountability mechanisms, sufficient to provide proper management of (security risks)” must be maintained. The guidance also references the following:

- the importance of internal risk assessments;
- the need for sufficient oversight of networks and services to enable fast identification of significant security incidents;
- a requirement to put in place security measures that exceed those in the Cyber Essentials scheme; and
- the importance of intelligence-led vulnerability testing to manage cyber-risks.

Regulation 2(1) of the PECR defines a “personal data breach” as a breach of security leading

to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of – or access to – personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service. The security and breach notification requirements under Regulation 5 of the PECR apply to personal data.

Under Regulation 5A of the PECR, service providers are required to notify the ICO in the event of a personal data breach (as defined under Regulation 3 of the PECR). Pursuant to Article 2(2) of the Notification Regulation, such notification must be made where feasible, no later than 24 hours after the detection of the personal data breach. A notification to the ICO is not required where an organisation is responsible for delivering part of the service but does not have a direct contractual relationship with end users. In such cases, the organisation must notify the organisation that does have the contractual relationship with end users and that organisation must then notify the ICO. The service provider is also required to notify (without undue delay) the concerned subscriber or user where the breach is likely to adversely affect their personal data or privacy, unless the service provider can demonstrate to the ICO that the data was made unintelligible (eg, encrypted).

The security breach notification requirements under Section 105K(1)(a) of the CA 2003 apply to public electronic communications networks and systems: network and service providers must notify Ofcom of security breaches that have a significant impact on the operation of a public electronic communications network. Section 105(A) of the CA 2003 broadly defines a “security compromise” as including “anything that compromises the availability, performance or functionality of the network or service”. In

determining whether the effect that a security compromise has – or would have – on the operation of a network or service is “significant”, certain matters should be considered, including the length of the period during which the operation of the network or service is or would be affected, the number of affected persons, the geographical size and location affected, and the extent to which activities of persons who use the network or service are or would be affected by the effect on the operation of the network or service.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

There are numerous cybersecurity frameworks that are expressly or implicitly recognised by UK cybersecurity regulators. By way of example, the ICO recommends that organisations review the UK Cyber Essentials scheme (a UK government- and industry-backed scheme), which provides basic guidance to organisations on how to prevent and limit the impact of cyber-attacks.

Similarly, Ofcom repeatedly references the International Standard for Organization (ISO) standards in its Guidance on Security Requirements. In addition, Ofcom comments that the controls in the UK’s Cyber Essentials scheme should be implemented and exceeded; according to Ofcom, obtaining the Cyber Essentials Plus certification is “a powerful way to demonstrate this”.

Regarding the NIS Regulations, the NCSC has published 14 cybersecurity and resilience principles that provide guidance in the form of the Cyber Assessment Framework (CAF). The CAF

is particularly relevant to OESs that are subject to the NIS Regulations.

Lastly, the most used account and payments data security standard, the Payment Card Industry Data Security Standard (PCI DSS), was revised. Version 4.0 was published on 31 March 2022.

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

As mentioned in 1.2 Cybersecurity Laws, the UK GDPR and the DPA contain cybersecurity obligations in relation to the processing of personal data. The UK GDPR and the DPA apply to:

- all organisations established in the four countries of the UK (ie, England, Northern Ireland, Scotland and Wales); and
- organisations not established in the UK processing personal data of data subjects in the UK to offer them goods or services or to monitor their behaviour.

The UK GDPR requires that controllers and processors implement “appropriate” technical and organisational security measures, taking into account the state of the art, costs of implementation, and the nature, scope, context and purposes of the processing of personal data, as well as the risks of such processing to the data subject’s rights (eg, from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of – or access to – personal data transmitted, stored or otherwise processed by the organisation).

The UK GDPR itself sets out examples of “appropriate” security measures, which are:

- pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of personal data processing.

Importantly, according to the ICO, there is no “one size fits all” approach to “appropriate” security and recommends that – before taking a view on what is “appropriate” – organisations should assess the level of risk by reviewing the type of personal data held, whether it is sensitive or confidential, and the damage caused to data subjects if compromised (eg, identity fraud).

In addition, when considering which cybersecurity measures to adopt, the ICO recommends that organisations consider:

- system security – security of the organisation’s network and information systems (particularly systems that process personal data);
- data security – security of the personal data held in the organisation’s systems (eg, ensuring appropriate access controls are in place within the organisation);
- actively managing software vulnerabilities –including using in-support software and the application of software update policies (patching), as well as taking other mitigating steps where patches cannot be applied;
- online security – website and mobile application security; and

- device security – considering information security policies for bring-your-own devices, where offered by the organisation.

The UK GDPR and the DPA continue to be enforced by the ICO, including with regard to cybersecurity matters, but only to the extent that they impact personal data. The ICO is required to adhere to specific procedures before undertaking enforcement action – for example, before imposing an administrative fine on an organisation for:

- breaching the integrity and confidentiality principle;
- inadequate security measures; or
- failing to report a personal data breach to the ICO or affected data subjects.

Where applicable, the ICO is required under Section 149 of the DPA to first issue the organisation with a written “enforcement notice”, which requires the organisation to take steps specified in the notice and/or refrain from taking steps specified in the notice. If the ICO is of the view that the organisation has failed to comply with the enforcement notice, the ICO will then issue a written notice (penalty notice) imposing a monetary penalty on the organisation of up to the greater of 4% of annual worldwide turnover or GBP17.5 million. When determining the monetary penalty amount, the ICO will consider a number of aggravating or mitigating factors. These factors include the nature, gravity and duration of the infringement – for example, personal data breach or inadequate security measures – and the intentional or negligent character of the infringement.

In determining whether to undertake a criminal prosecution under the DPA, the ICO must reference the Code for Crown Prosecutors and the

ICO's own prosecution policy. Although the ICO has a number of enforcement tools available to it (including providing a caution to offending organisations), the ICO's Prosecution Policy Statement requires the ICO to consider aggravating factors in order to bring a prosecution instead of a caution. These include the accused breaching the law for financial gain, abusing a position of trust, or damage or distress being caused to data subjects.

The maximum penalty for criminal offences under the DPA is an unlimited fine. Imprisonment is not available for conviction under any of the DPA offences. Defendants are entitled to normal rights of appeal against a conviction or sentence in the legal system.

6.2 Cybersecurity and AI

On 26 November 2023, the US Cybersecurity and Infrastructure Security Agency (CISA), together with the UK's NCSC, published joint Guidelines for Secure AI System Development (the "AI Guidelines"). The AI Guidelines aim to ensure that developers take a "secure by design" approach, integrating cybersecurity into the development process from the outset and throughout. The AI Guidelines cover secure design, secure development, secure deployment, and secure operation and maintenance. Relatedly, in its annual review published on 3 December 2024, the NCSC noted the significant advances in AI that will enable and enhance existing challenges associated with cybersecurity.

Work is currently underway by the DSIT to produce a sector agnostic Code of Practice on Cyber Security of AI (the "AI COP") to establish the minimum cybersecurity standards that developers and system operators should incorporate when building and using AI solutions. The

AI COP, which is voluntary, is based on the AI Guidelines and is intended to sit alongside the UK government's 2023 White Paper "A pro-innovation approach to AI regulation", which includes "Safety, Security and Robustness" as one of the five key principles – the focus of the AI COP. The AI COP is structured around 12 principles and stakeholders to which each principle primarily applies are identified. Requirements include AI security awareness training, system design and dataset considerations, incorporating threat-modelling into the risk management process, and evaluation and testing. The consultation on the AI COP closed on 9 August 2024 and the UK government's response is anticipated – although no timeline has been set.

6.3 Cybersecurity in the Healthcare Sector

Under the NIS Regulations, NHS trusts, foundation trusts, integrated care boards, and certain other healthcare providers are designated as OESs. Consequently, these healthcare providers are required to comply with the obligations of an OES as described in 2.2 **Critical Infrastructure Cybersecurity Requirements**.

Medical devices in scope of the Medical Devices Regulations 2002 are expressly excluded from the PSTI Act. However, the UK government is expected to continue its overhaul of the UK's medical devices legislative framework following the application of the Medicines and Medical Devices Act 2021 (the "MMD Act"). The MMD Act includes powers for the Secretary of State to introduce regulations in relation to the manufacture of medical devices. In February 2024, the Department for Health and Social Care (DHSC) confirmed that it would be introducing a package of legislative reform for UK medical devices. In December 2024, the Medicines & Healthcare products Regulatory Agency (MHRA) issued a

revised roadmap for reform (the “Roadmap”), which stated that new guidance will be published on cybersecurity requirements for software included as part of a medical device.

The MHRA has produced a number of work packages in their proposed Software and AI as a Medical Device Change Programme, with Work Package WP5 dedicated to “Cyber Secure Medical Devices”. This work package focuses on ensuring that cybersecurity is adequately reflected in software as a medical device (SaMD) requirements and explains that secondary legislation will be developed to impose cybersecurity and IT requirements to guard against cybersecurity risks in medical devices and in vitro diagnostics (IVDs) that may result in device malfunction, loss or tampering with personal data, damage to the device, and ultimately injury to the patient. Guidance will be developed on cybersecurity issues in the life cycle management processes of medical devices and IVDs and on the reporting of cybersecurity vulnerabilities.

NHS Digital (the body responsible for information, data and IT systems in health and social care in the UK) has published a variety of guidance, including the Data Security and Protection Toolkit, which is an online self-assessment tool that all organisations must use if they have access to NHS patient data and systems. This includes an incident reporting tool that incorporates the notification requirements of the UK GDPR and the NIS Regulations. There is also a GDPR-focused document entitled “Respond to an NHS Cyber-Alert”, which explains the intersection between medicine, personal data, and cybersecurity.

At an EU level (albeit highly persuasive, rather than legally binding, from a UK perspective), the Medical Device Co-Ordination Group published

updated guidance in June 2020 on cybersecurity for medical devices, which is intended to assist medical device manufacturers in meeting the cybersecurity requirements in the EU’s Medical Devices Regulation and the In Vitro Diagnostic Regulation. According to the updated guidance, manufacturers must consider safety and cybersecurity throughout the life cycle of a product – that is, they must integrate security “by design”. This concept closely aligns with the requirement of privacy by design under the UK GDPR. Manufacturers must also perform increased post-market surveillance and vigilance. Such post-market surveillance should address the following:

- operation of the device in the intended environment;
- sharing and dissemination of cybersecurity information and knowledge of cybersecurity vulnerabilities and threats across multiple sectors;
- vulnerability remediation; and
- incident response.

The MHRA clearly stated in its Roadmap the regulations will move the UK towards greater alignment of the cybersecurity requirements for medical devices with the approach taken by the EU and other international regulators.

Lastly, it is worth mentioning that – rather than taking a separate approach to any AI-enabled product – the UK’s approach to regulating cybersecurity risks resulting from AI is sector-specific. In the healthcare space, the MHRA has announced in its Policy Paper “Impact of AI on the regulation of medical products” of April 2024 that it will follow a principles-based approach in order to avoid constraining innovation, including the guidance on cybersecurity for AI as expected to be published in spring 2025.

Trends and Developments

Contributed by:

William Long, Francesca Blythe, Eleanor Dodding and Anila Rayani
Sidley Austin LLP

Sidley Austin LLP is a premier global law firm with a practice highly attuned to the ever-changing international landscape. The firm advises clients around the globe and has more than 2,300 lawyers in 21 offices worldwide. Sidley Austin maintains a commitment to providing quality legal services and offering advice on litigation, transactional and regulatory matters spanning virtually every area of law. The firm's lawyers have wide-reaching legal backgrounds and are dedicated to teamwork, collaboration, and superior client service. The team helps a

range of businesses address some of the most challenging matters concerning data protection, privacy, information security and incident response, data commercialisation, internet and computer law, IP, information management and records retention, e-commerce, consumer protection, and cybercrime. Sidley Austin advises clients with extensive operations in Europe – as well as in the USA, Asia and elsewhere – on developing and implementing global data protection programmes.

Authors



William Long is a partner at Sidley Austin LLP, where he leads the EU and UK data protection practice and is global co-leader of the firm's highly ranked privacy and

cybersecurity practice. William advises international clients on a wide variety of AI, cyber, and digital data laws, as well as data protection, privacy, information security, social media, e-commerce and other regulatory matters. He has been a member of the International Association of Privacy Professionals (IAPP)'s European Advisory Board and on the DataGuidance panel of data protection lawyers. William has also been on the editorial board of "e-Health Law & Policy" and assists with dplegal, a network for privacy professionals.



Francesca Blythe is a partner at Sidley Austin LLP and advises international clients on a wide range of privacy, cybersecurity, and emerging technology issues, including on privacy and

cybersecurity compliance strategies. She has also counselled clients in preparing for, and responding to, data breaches of varying sizes. Francesca co-leads Sidley Austin's benchmarking group for in-house data privacy professionals (dplegal) in the life sciences sector and was previously in-house counsel at the largest international health and beauty retailer in Asia and Europe. While there, she regularly gave advice on compliance and strategies relating to data protection laws and assisted in the planning and delivery of a global privacy compliance project.

UK TRENDS AND DEVELOPMENTS

Contributed by: William Long, Francesca Blythe, Eleanor Dodding and Anila Rayani, **Sidley Austin LLP**



Eleanor Dodding is a senior managing associate at Sidley Austin LLP. She provides practical and strategic advice to international clients regarding the EU and UK General Data

Protection Regulation, e-privacy laws, international data transfers (including with regard to the Schrems II decision), and sector-specific privacy and cybersecurity laws. Eleanor also has experience in assisting clients with preparing for, and responding to, cybersecurity incidents.



Anila Rayani is an associate at Sidley Austin LLP. She advises international clients on various data protection, privacy, and cybersecurity matters, including the EU and UK General Data

Protection Regulation, e-privacy laws, and emerging AI and cyber frameworks. Anila also has experience investigating and responding to complex cross-border cybersecurity incidents and personal data breaches, as well as dealing with regulatory inquiries.

Sidley Austin LLP

70 St Mary Axe
City of London
London
EC3A 8BE
UK

Tel: +44 020 7360 3600
Fax: +44 020 7626 7937
Web: www.sidley.com

SIDLEY

Cyber-Resilience in the UK: An Overview

Cyber-resilience is a sector-agnostic issue that is continuing to grow in importance; a cybersecurity breach can have a significant financial impact on an organisation and cause untold damage to brand and reputation. As the world grows ever more dependent on technology such as AI, cybersecurity awareness and good cyber-hygiene become increasingly fundamental to the UK's overall resilience. Consequently, cybersecurity has been a UK government priority.

Despite a change in government in 2024, the pace of cybersecurity reform remained consistent – with the passing and proposing of a number of new laws, as well as the publication of several consultations on draft guidance. Supply chain cybersecurity resilience was a key theme and is expected to continue in 2025, likely influenced by the plethora of new EU cybersecurity laws (such as the Network and Information Security Directive 2 (“NIS2”)). Consequently, it is expected that cybersecurity legislation will remain a focus for the UK government in 2025 as the reform progresses and takes effect.

Cybersecurity threats and developments

The UK government's Cyber Security Breaches Survey (the “Survey”), published in April 2024, exposed a disconcerting cybersecurity landscape for UK businesses. Approximately 7.78 million cybercrimes were committed against UK businesses in the 12 months prior to the Survey's publication, with half of UK businesses reporting having experienced a cyber-attack or security breach. Phishing attacks emerged as the most common (affecting 84% of businesses), whereas ransomware and denial of service attacks were the least common (affecting 2% or fewer). Nonetheless, the UK's National Cyber Security Centre (NCSC) warned that ransomware posed

the most significant threat to UK critical national infrastructure (CNI).

UK businesses and institutions also faced cyberthreats from hostile state actors – including from Russia, China, Iran, and North Korea. These countries exploited the increasingly tense geopolitical situation arising from the conflicts in Ukraine and the Middle East. The NCSC's Annual Review 2024 (the “Review”) stated that China presents the most sophisticated cyberthreat to the UK, while Russia encourages non-State malicious actors to launch cyber-attacks against Western countries, alongside its own state-backed cybercampaign.

Ransomware attacks are evolving and – instead of encrypting the stolen data and demanding payment for its decryption – malicious actors are now threatening to publish sensitive personal data online, causing financial and reputational harm to victims. This was the case in the June 2024 ransomware attack on a pathological laboratory service provider to the NHS, which disrupted NHS services and leaked data online. Global ransomware payments totalled USD1 billion in 2023, according to the Review. In May 2024, the NCSC, UK Information Commissioner's Office (ICO) and insurance industry bodies issued a joint guidance, “Guidance for Organisations Considering Payment in Ransomware Incidents”, discouraging organisations from making ransom payments.

Technological developments, particularly in AI and quantum computing, also pose a challenge to the UK's cyber-resilience. The Review identified cyber-intrusion as a growing threat in the next five years, facilitated by poor regulation in certain jurisdictions and by AI technological advances that increase the effectiveness of social engineering, vulnerability identification,

and data analysis. This risk is, however, already evident; in May 2024, a deepfake scam resulted in an employee transferring USD25 million to a malicious actor.

The NCSC has warned that the commercialisation of cyber-intrusion tools has made it easier for malicious actors to access and attack systems, and harder to trace them. The NCSC is also cognisant of the impact quantum computing will have on existing cryptography methods and technology in the longer term and urged action to prepare for the emerging cyber-risks.

In 2025, the NCSC is expected to focus on key actions to enhance the UK's cyber-resilience, including:

- promoting basic cybersecurity practices among UK businesses, including a focus on the adoption of the NCSC's Cyber Essentials certification and the Cyber Assessment Framework;
- the publication of more practical guidance from the NCSC and the National Protective Security Authority;
- continued international co-operation and action against malicious cyber actors from hostile states; and
- initiatives to grow a cyberskilled workforce that is cyberliterate and can contribute to cybersecurity technological innovation.

UK cyber-regulation landscape

The UK's cybersecurity landscape underwent significant changes in 2024 and more reforms are expected in 2025.

The Product Security and Telecommunications Infrastructure (PSTI) Act and its accompanying regulations came into force on 29 April 2024. They require organisations that manufacture

"relevant connectable products" to meet certain cybersecurity standards such as minimum password requirements, reporting security issues, and minimum periods for which products will receive security updates.

The Labour government, which came to power following the UK's General Election in May 2024, has demonstrated its commitment to cybersecurity reform and progressing the UK's National Cyber Strategy. The King's Speech in July 2024 announced the introduction of two new bills into Parliament – namely, the Cyber Security and Resilience (CSR) Bill and the Data (Use and Access) (DUA) Bill.

The CSR Bill will revise the Network and Information Systems Regulations 2018 (the "NIS Regulations"), which is the only existing sector-wide cybersecurity legislation in the UK. The UK government has been under pressure to update the NIS Regulations – which was implemented pre-Brexit – to align more closely with recent EU legislative developments in this space and, in particular, to expand the scope of the NIS Regulations to include more digital services and supply chains, increase mandatory incident reporting obligations, and provide enhanced powers to regulators. According to the UK Department for Science, Innovation and Technology (DSIT), the CSR Bill will be introduced into Parliament in 2025.

The DUA Bill will amend the existing UK data protection laws. However, owing to the overlap between data protection and cybersecurity, businesses should be aware of the DUA Bill when considering their overall cyber-resilience programme. The DUA has been teased as the potential vehicle for further amendments to the Computer Misuse Act (CMA). Proposed amendments to the CMA were debated in the House

of Lords and subsequently rejected in December 2024 and again in January 2025. The proposed amendments were intended to support cybersecurity professionals that work against cybercrime, included an update to the definition of unauthorised access, and would have provided for a new defence against offences under the CMA where a person is acting to prevent or detect a crime or is otherwise acting in the public interest. The DUA Bill will continue to progress through the legislative process in 2025, most likely without CMA reform. Nevertheless, in October 2024, the UK's Security Minister stated that the Labour government remains committed to tackling cybercriminals and suggested that a review of the CMA is forthcoming.

In 2024, the DSIT consulted on three draft cybersecurity codes of practice:

- the AI Cyber Security Code of Practice (the “AI COP”);
- the Code of Practice for Software Vendors (the “Software Vendors COP”); and
- the Cyber Governance Code of Practice (the “Governance COP”).

The AI COP aims to develop a global technical standard for the security of AI systems, based on the principle of “Safety, Security and Robustness” from the UK government’s 2023 White Paper, “A pro-innovation approach to AI regulation”. The Software Vendors COP sets out four key principles for security measures that businesses that develop and/or sell software in a B2B context should follow, which are:

- secure design and development;
- build environment security;
- secure deployment and maintenance; and
- communication with customers.

The Governance COP outlines five key principles and related actions for good cybergovernance, which relate to risk management, cyberstrategy, people, incident planning and response, and assurance and oversight. The consultations closed in 2024 but the responses have not yet been published. Businesses should keep an eye out for them in 2025.

Finally, in September 2024, the UK government designated data centres as CNI – meaning that, alongside energy supply, water supply and transportation, data centres located in the UK are considered “essential for the functioning of society”. As a result, UK data centres can access more support and guidance from the government and the NCSC in the event of outages, cyber-attacks, and adverse weather events.

Supply chain cybersecurity resilience and risk management

Supply chain cybersecurity risk management was a key theme during the course of 2024, particularly in the financial services sector, and this trend is likely to continue in 2025. As businesses become more interconnected, they also become more vulnerable to cyber-attacks through their suppliers, even if they have strong cybersecurity practices themselves.

As mentioned in “UK cyber-regulation landscape”, the CSR Bill is expected to expand the scope of the NIS Regulations to (inter alia) introduce new obligations with regard to supply chain management and cyber-resilience – ie, in line with the approach taken in the EU under NIS2 where in-scope entities are required to implement supply chain security policies, supply chain due diligence and minimum supply chain security standards, among other measures. The CSR Bill will likely be scrutinised against NIS2 once published.

In the meantime, the UK has a voluntary approach to supply chain cybersecurity regulation. The Software Vendors COP and the AI COP both include principles and guidance on how to assess and manage supply chain cyber-risks throughout the product life cycle, engage trusted actors involved in the product build and life cycle, and notify vulnerabilities to other parties.

The financial services sector has also made progress in promoting the use of Cyber Essentials, the NCSC-backed scheme that helps organisations improve their cybersecurity and protect themselves from cyber-attacks. Six major UK banks have committed to making Cyber Essentials a requirement for their suppliers and encouraged other businesses to join them. The benefits of this approach include improved supplier due diligence, reduced compliance costs, and improved cyber-insurance coverage across the supply chain.

Additionally, the UK's financial regulators – the Bank of England, the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) – issued a joint policy statement (PS 16/24) on the final Critical Third Party Oversight Regime (the “Regime”), which came into effect on 1 January 2025. The Regime aims to manage the risks to the UK financial system's stability and confidence that could arise from failures or disruptions in the services that a critical third party provides to firms. The Regime consists of several policy statements and rules that apply to third parties that are designated as critical by His Majesty's Treasury. This is similar to the EU's Digital Operational Resilience Act (DORA), which also applies to financial institutions and insurance intermediaries, and which came into effect on 17 January 2025. Under DORA, certain third-party information and com-

munications technology service providers are subject to similar cybersecurity obligations.

Cybersecurity enforcement trends

As it currently stands, the majority of enforcement action concerning cybersecurity in the UK is conducted by the ICO in relation to security incidents under the General Data Protection Regulation (GDPR).

The ICO's report “Data Security Incident Trends” shows that, out of the 60,607 incidents reported to the ICO from the start of 2019 through to the third quarter of 2024, 14,993 (approximately 25%) were cyber-related. There has been a steady number of cyber-incidents reported to the ICO each year, with a slight spike in notifications in 2023 (3,318 in total). As with the findings from the NCSC, the ICO figures show that the most common cyber-incident notifications relate to phishing attacks (approximately 39%), followed by ransomware attacks (approximately 26%) and unauthorised access incidents (approximately 12%).

Despite all the evidence pointing towards a more challenging cybersecurity landscape, as well as the strong signals from the NCSC that cyber-resilience and cyber enforcement are top priorities, the nature of ICO enforcement action appears to have softened. There has been a sharp decline in the number of “investigations” the ICO has launched in response to a notification of a cyber-incident – from 1,497 in 2019 to just 39 in the first three quarters of 2024. However, during the same time period, there has been a steady increase in the “informal action taken” by the ICO. This means that the ICO is increasingly deeming it unnecessary to use its formal powers, such as issuing a fine or a reprimand, and instead provides advice to the notifying organisation.

That said, the ICO is clearly willing to issue fines to organisations that experience a cyber-incident as a result of failing to implement appropriate technical and organisational measures as required under the GDPR, with more than GBP19 million in fines having already being issued in this regard and a GBP6 million provisional fine announced in August 2024. Similarly, the ICO has recently issued reprimands in relation to a variety of cyber-incidents, including a brute-force attack resulting from a known software vulnerability, as well as multiple instances of ransomware attacks, malware attacks, and unauthorised access incidents resulting from non-compliance with GDPR security requirements. It is important to note that, according to the ICO's data protection fining guidance (updated in March 2024), pro-active notification to the NCSC – alongside the usual notification requirements to the ICO – can be considered a mitigating factor by the ICO when deciding to issue a fine.

Taking this in the round, it appears that the ICO's preferred intervention is through the provision of advice and guidance to organisations. Its formal powers seem to be reserved for the most serious failings that lead to a cyber-incident.

Practical considerations

Cyber-attacks pose a serious and growing threat to businesses and institutions in Western countries, requiring more than just compliance measures to protect their assets, data and reputation. Cybersecurity must become a core operational function, with strong leadership and support from the board and senior leaders.

Businesses should assess and address any gaps or weaknesses in their cybersecurity practices, seek accreditation from recognised cybersecurity frameworks where appropriate, and enforce cybersecurity minimum standards across their supply chains. It is critical that employees are provided with adequate cybersecurity training to protect against a successful cyber-attack and to reduce the likelihood of a cybersecurity incident caused by human error or action. Businesses should also monitor the development of new laws and guidance, as well as proactively implement best practice standards as recommended by the NCSC.



Law and Practice

Contributed by:

Beth George, Timothy Howard, Brock Dahl and Megan Kayo
Freshfields

Contents

1. General Overview of Laws and Regulators p.346

- 1.1 Cybersecurity Regulation Strategy p.346
- 1.2 Cybersecurity Laws p.346
- 1.3 Cybersecurity Regulators p.347

2. Critical Infrastructure Cybersecurity p.347

- 2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.347
- 2.2 Critical Infrastructure Cybersecurity Requirements p.348
- 2.3 Incident Response and Notification Obligations p.349
- 2.4 State Responsibilities and Obligations p.350

3. Financial Sector Operational Resilience Regulation p.351

- 3.1 Scope of Financial Sector Operational Resilience Regulation p.351
- 3.2 ICT Service Provider Contractual Requirements p.352
- 3.3 Key Operational Resilience Obligations p.353
- 3.4 Operational Resilience Enforcement p.354
- 3.5 International Data Transfers p.354
- 3.6 Threat-Led Penetration Testing p.354

4. Cyber-Resilience p.355

- 4.1 Cyber-Resilience Legislation p.355
- 4.2 Key Obligations Under Legislation p.355

5. Security Certification for ICT Products, Services and Processes p.355

- 5.1 Key Cybersecurity Certification Legislation p.355

6. Cybersecurity in Other Regulations p.355

- 6.1 Cybersecurity and Data Protection p.355
- 6.2 Cybersecurity and AI p.356
- 6.3 Cybersecurity in the Healthcare Sector p.357

Freshfields is a global market leader in handling data crises, investigations, class actions, and regulatory engagement. The firm has in-depth experience in cybersecurity – from prevention to governance to responding to incidents – and has a deep bench of cybersecurity and privacy attorneys who provide clients with global coverage from offices around the world, including in the USA, Europe, the UK, and Asia. With a

strong market-leading data and cyber practice comprising more than lawyers, Freshfields' global team of experts works seamlessly at the highest level, leveraging their expertise in crisis management and judicial proceedings to provide high-quality advice. This includes extensive know-how, honed through involvement in hundreds of international cases.

Authors



Beth George leads Freshfields' strategic risk and crisis management practice. Based in Silicon Valley, Beth regularly advises boards of private and public companies on risk

management and governance, including advising on governance related to AI, data practices and cybersecurity, content management, cybersecurity incidents, and geopolitical events. Her practice has included representing a large company facing high-profile congressional investigations and litigation regarding its data security practices, investigating alleged nation state insider threats at a leading tech company, and advising a public company in a high-profile breach that resulted in an FBI investigation and criminal charges.



Timothy Howard is Freshfields' US head of data security and is based in New York, where his practice focuses on white-collar and government regulatory investigations, with special

attention to cybersecurity, data breaches, and cryptocurrency. Tim is an accomplished trial lawyer and investigator, having managed cases across a range of disciplines, including securities fraud, tax fraud, Foreign Corrupt Practices Act violations, cyber-intrusions, and healthcare fraud. He has advised Freshfields' clients on complex cross-border data breach incidents, including managing incident response, forensic investigation and engagement with regulators, Department of Justice and SEC investigations, and advising companies on AI, cybergovernance, and other data security risks.

Contributed by: Beth George, Timothy Howard, Brock Dahl and Megan Kayo, **Freshfields**



Brock Dahl brings cutting-edge cyber experience to Freshfields from his time at the National Security Agency (NSA). As deputy general counsel in operations at the NSA, Brock

advised leadership on how to achieve mission objectives within the boundaries of state, federal and international cyber, privacy, and national security laws. He has a deep understanding of advanced technologies and the legal challenges they raise and has played a key role in the US government's response to significant global cyber-incidents in recent years.



Megan Kayo of Freshfields specialises in cybersecurity and privacy issues. Based in Silicon Valley, she has worked on hundreds of data breach incidents, including

investigations, notifications and interactions with regulators and affected individuals. Megan represents clients in regulatory investigations of their information security programmes, products (including generative AI products), and their responses to data breaches and security incidents. She also helps clients with privacy compliance and data governance, including risk assessment and management, breach mitigation, business continuity and disaster recovery planning, oversight of third-party service providers, due diligence in corporate transactions, and board of director advice and counselling.

Freshfields

3 World Trade Center
175 Greenwich St
51st Floor
New York
NY 10007
USA

Tel: +1 212 277 4000
Fax: +1 212 277 4001
Email: beth.george@freshfields.com
Web: www.freshfields.us

FRESHFIELDS

1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

The USA does not regulate cybersecurity under a single, general, nationwide regime. Instead, multiple overlapping regulatory regimes at both the federal and state level address cybersecurity in a sector- or jurisdiction-specific manner. The scope and substantive obligations imposed by each of these regulations address specific aspects of cybersecurity. These aspects can include:

- technical measures that can be implemented to mitigate the risk of unauthorised access to data;
- incident response procedures for when data breaches occur; and
- transparency and reporting requirements.

These regulations serve purposes such as protecting national security, safeguarding personal information (including specific regulations addressing sensitive financial data or health information), and promoting collaboration and innovation. For more information on sector-specific and national security-specific regulations, see **2. Critical Infrastructure Cybersecurity**, **3. Financial Sector Operational Resilience Regulation**, and **6.3 Cybersecurity in the Healthcare Sector**.

1.2 Cybersecurity Laws

At the federal level, the main laws and regulations governing cybersecurity include:

- the Gramm-Leach-Bliley Act (GLBA) of 1999, which imposes security and transparency requirements on financial institutions' handling of non-public personal information of customers (see **3.1 Scope of Financial**

Sector Operational Resilience Regulation for more detail);

- the Health Insurance Portability and Accountability Act (HIPAA), which regulates the protection of sensitive healthcare-related information (see **6.3 Cybersecurity in the Healthcare Sector** for more detail);
- the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which regulates disclosure of cyber-incidents by critical infrastructure companies (see **2.1 Scope of Critical Infrastructure Cybersecurity Regulation** for more detail);
- laws and regulations imposing cybersecurity obligations on federal government agencies and contractors, such as the Defense Federal Acquisition Regulation Supplement (DFARS) and the Federal Information Security Management Act; and
- the SEC's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure rules requiring some publicly traded companies to report certain cybersecurity incidents and make disclosures about their cybersecurity strategy, cybersecurity governance, and cybersecurity risk management in public filings.

A number of federal laws and regulations criminalise hacking and otherwise regulate the use of information technology by individuals and law enforcement entities alike. By way of example, the Computer Fraud and Abuse Act criminalises unauthorised access to computer systems, and the Stored Communications Act regulates ISPs' ability to voluntarily provide stored electronic communications and data to the government and also regulates the manner in which the government may seek compelled access to stored electronic communications and data through legal process. In addition, the Wiretap Act and the Pen Register Act criminalise the unlawful

interception of content and non-content data, respectively.

In addition to these cybersecurity-specific laws and regulations, some more general regulations have been enforced with regard to cybersecurity. By example, Section 5 of the Federal Trade Commission Act empowers the Federal Trade Commission (FTC) to regulate and enforce against unfair or deceptive trade practices in general. The FTC and federal courts have interpreted this regulation to permit the regulation and enforcement of cybersecurity where companies' security practices (and public representations concerning those practices) may qualify as unfair or deceptive.

Finally, in addition to federal regulation, many states impose cybersecurity obligations through statute or regulation. Some states require by statute that companies take reasonable measures to protect sensitive personal information of state residents, with varying levels of specificity as to what measures are required or will be deemed reasonable if employed. Other states have more developed regulatory regimes, including the California Consumer Privacy Act. For more details on cybersecurity regulations promulgated by New York State's Department of Financial Services (NYDFS), see **6.2 Cybersecurity and AI**.

1.3 Cybersecurity Regulators

At the federal level, the main cybersecurity regulators include:

- the FTC, which – as noted in **1.2 Cybersecurity Laws** – regulates cybersecurity as part of its broad authority to regulate and enforce against unfair or deceptive trade practices;
- the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and the Depart-

ment of Homeland Security (DHS), which investigate and prosecute federal criminal activity, including cyber-intrusions and cyber-enabled crime;

- the DHS, which regulates critical infrastructure and other aspects of national security;
- the Department of Health and Human Services (HHS), which enforces HIPAA regulations – including those related to data protection – over covered providers; and
- the SEC, which regulates publicly traded companies and imposes disclosure obligations following cybersecurity breaches.

Federal regulators have the authority to promulgate regulations with the force of law following a public notice-and-comment process, as well as to enforce those regulations through civil investigations (including compulsory disclosure of documents and testimony) and litigation.

At the state level, cybersecurity may be regulated by state Attorneys General or subdivisions within their offices. Some states have established cybersecurity-specific agencies, such as the Utah Cyber Center, and others have conferred authority to sector-specific regulators, such as the NYDFS. For more detail on the NYDFS, see **6.2 Cybersecurity and AI**.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

In the USA, CIRCIA requires critical infrastructure entities to report covered cyber-incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours and ransomware payments within 24 hours. The applicable rules for covered entities under CIRCIA are still under

development and it is currently estimated they will go into effect at the end of 2026. The regulation, released in draft form on 4 April 2024, purports to further define the categories of entities and incidents subject to the reporting regime.

The scope of application under CIRCIA is intentionally broad, encompassing entities across all 16 critical infrastructure sectors, as identified by the DHS. These sectors include industries vital to public safety, economic stability, and national security, such as the chemical, critical manufacturing, defence industrial base (DIB), energy, financial services, healthcare, and IT industries.

Sector-Specific Regulations

- **Energy** – the Federal Energy Regulatory Commission (FERC) enforces the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards, requiring electric utilities to secure cyber-assets, manage supply chain risks, and report incidents under Section 215 of the Federal Power Act (FPA).
- **Transportation** – the Transportation Security Administration (TSA) mandates cybersecurity for pipeline, rail and aviation operators through directives requiring incident reporting, risk mitigation, and security plans.
- **Water and waste water systems** – the Environmental Protection Agency (EPA) enforces cybersecurity requirements under America's Water Infrastructure Act (AWIA), requiring utilities serving more than 3,300 people to assess risks and enhance cybersecurity protections.
- **Nuclear** – the National Nuclear Security Administration (NNSA) and Nuclear Regulatory Commission (NRC) enforce cybersecurity for nuclear facilities and contractors handling classified data, with strict protections under Title 10, Code of Federal Regulations (CFR)

Part 73 and the Department of Energy Cybersecurity Program Plan (CSP).

- **DIB** – the Cybersecurity Maturity Model Certification (CMMC) and DFARS 252.204-7012 require defence contractors handling Controlled Unclassified Information to meet National Institute of Standards and Technology (NIST) SP 800-171 standards for cybersecurity and separate departmental requirements obligate certain entities to report identified categories of cyber-incidents.
- **Healthcare** – HIPAA mandates cybersecurity protections for electronic protected health information ("ePHI") under the HIPAA Security Rule, with breach reporting obligations under the HIPAA Breach Notification Rule. See **6.3 Cybersecurity in the Healthcare Sector** for more on HIPAA.
- **Other entities handling personal health records** – entities not regulated by HIPAA that handle personal health records (PHRs) are required to notify affected individuals under the FTC's Health Breach Notification Rule (HBNR).

2.2 Critical Infrastructure Cybersecurity Requirements

In the USA, critical infrastructure cybersecurity is governed by sector-specific regulations designed to address the unique risks faced by each industry. These requirements aim to enhance resilience against cyberthreats by mandating proactive risk management, incident reporting, and adherence to best practices.

There are a number of sector-specific cybersecurity requirements, as follows.

- **Energy sector** – the FERC's CIP Standards require cybersecurity plans, access controls, and periodic risk assessments.

- Water and waste water systems sector – the EPA mandates water utilities to incorporate cybersecurity into risk assessments and develop emergency response plans under the AWIA.
- Nuclear sector – NRC licensees must implement extensive cybersecurity safeguards, including access controls, network monitoring, supply chain risk management, and incident response protocols to prevent cyberthreats from compromising reactor operations or sensitive nuclear materials.
- Transportation sectors – TSA’s cybersecurity directives require critical infrastructure owners to implement vulnerability assessments, mitigation measures, and cybersecurity plans. Other particular requirements apply to the rail and aviation sectors.
- Healthcare sector – see **6.3 Cybersecurity in the Healthcare Sector**.
- Financial services sector – see **3. Financial Sector Operational Resilience Regulation** (in particular, **3.1 Scope of Financial Sector Operational Resilience Regulation**).
- DIB – the CMMC framework establishes tiered cybersecurity requirements for defence contractors handling controlled unclassified information (CUI), with higher levels requiring measures such as encryption, multifactor authentication, and third-party cybersecurity assessments.
- cyber-incident reporting – covered entities must report covered cyber-incidents to CISA within 72 hours of determining that a covered incident has occurred; and
- ransomware payment reporting – entities must notify CISA within 24 hours of making a ransomware payment.

These requirements aim to enable CISA to better co-ordinate incident response efforts and facilitate information sharing between government and private-sector stakeholders. Despite the comprehensive framework, several uncertainties remain, as follows.

2.3 Incident Response and Notification Obligations

In the USA, incident response and notification obligations for critical infrastructure owners and operators are primarily governed by sector-specific regulations. CIRCIA will apply in addition to, not in replacement of, these sector-specific obligations. Once the CIRCIA regulations are finalised, they will require:

- Covered entities – CISA’s forthcoming regulations will determine which organisations within each sector are subject to CIRCIA obligations. Small or ancillary entities may face ambiguity about whether they fall within the scope.
- Incident thresholds – CIRCIA has not finalised what constitutes a “covered cyber-incident”. Without CISA’s finalised guidance, entities lack clarity on reporting triggers.
- Overlapping regulations – entities operating in multiple sectors may face overlapping obligations under federal and sector-specific frameworks (eg, HIPAA versus CIRCIA).
- Liability protections – while CIRCIA provides limited liability protections for reporting entities, questions remain about their interaction with confidentiality obligations under other frameworks, such as HIPAA or NRC regulations.
- International implications – organisations operating internationally may need to reconcile compliance with US frameworks such as CIRCIA and foreign standards, including the EU’s Network and Information Security Directive 2 (“NIS2”).

As noted in **2.1 Scope of Critical Infrastructure Cybersecurity Regulation**, in addition to the forthcoming CIRCIA requirements, there have already been sector-specific notification requirements in place for quite some time. Those include the following.

- Energy sector – the NERC, under FERC oversight, requires Bulk Electric System (BES) entities to report cybersecurity incidents that could impact reliability, including operational disruptions, unauthorized access, or attempted compromises, with notification timelines based on the severity of the incident. The most severe incidents (those that successfully compromise BES Cyber Systems and impact reliability) must be reported to the Electricity Information Sharing and Analysis Center (E-ISAC) and CISA within one hour of determination.
- Water and waste water systems sector – under the AWIA, water utilities must notify local emergency planning committees of any disruptions affecting service delivery, including those caused by cybersecurity incidents.
- Nuclear sector – the NRC requires immediate notification of cyber-incidents that compromise digital systems essential to nuclear safety, security, or emergency preparedness.
- Transportation systems sector – the TSA requires pipeline, rail and aviation operators to report identified categories of cybersecurity incidents within 24 hours and conduct post-incident reviews.
- Healthcare sector – see **6.3 Cybersecurity in the Healthcare Sector**.
- Financial services sector – see **3. Financial Sector Operational Resilience Regulation** (in particular, **3.1 Scope of Financial Sector Operational Resilience Regulation**).

- DIB – contractors handling CUI must report cyber-incidents to the Department of Defense (DoD) within 72 hours of discovery.

2.4 State Responsibilities and Obligations

State governments play a critical role in enhancing resilience and identifying threats to critical infrastructure within their jurisdictions. While the federal government provides overarching guidance and regulatory frameworks, states often act as the frontline co-ordinators for implementing resilience strategies, facilitating information sharing, and supporting critical infrastructure owners and operators.

Resilience Responsibilities

State responsibilities when it comes to enhancing the cyber-resilience of critical infrastructure are as follows.

- Development of statewide cybersecurity strategies – many states have established cybersecurity offices or task forces to develop and implement strategies aimed at strengthening the resilience of public and private critical infrastructure. These strategies often align with federal initiatives, such as the NIST Cybersecurity Framework, while addressing state-specific risks and priorities.
- Incident response co-ordination – states frequently serve as co-ordinators for incident response efforts through their state fusion centres and emergency operations centres. These entities work closely with CISA, local governments, and private-sector stakeholders to respond to and recover from cyber-incidents.
- Infrastructure resilience grants and programmes – states administer federal grant programmes, such as the State and Local Cybersecurity Grant Program, to fund pro-

jects that enhance the resilience of critical infrastructure. These grants support initiatives such as system upgrades, cybersecurity training, and vulnerability assessments.

Threat Identification Responsibilities

State responsibilities when it comes to identifying cybersecurity threats to critical infrastructure are as follows.

- Threat intelligence sharing – state governments act as intermediaries between federal agencies and local entities by disseminating threat intelligence. This includes leveraging the federal Multi-State Information Sharing and Analysis Center (MS-ISAC), which provides cybersecurity threat monitoring, analysis, and early warnings tailored to state and local governments.
- sector-specific threat monitoring – many states focus on monitoring threats to key sectors, such as water utilities, energy grids, and healthcare facilities, which are often regulated at the state level. State public utility commissions and health departments often collaborate with federal agencies to identify and mitigate threats.
- Mandatory reporting and oversight – states enforce data breach reporting requirements for businesses and other entities operating within their jurisdiction. Virtually all states have enacted data breach notification laws, requiring organisations to report breaches involving personally identifiable information (PII) to affected individuals and, in many cases, the state Attorney General or other regulatory bodies. For instance:
 - (a) some states (eg, California) mandate detailed reporting on the nature of the breach and steps taken to address it; and
 - (b) some state laws also impose specific deadlines for breach notifications, typical-

ly ranging between 30–90 days, depending on the jurisdiction.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (together, the “prudential regulators”) consider cybersecurity to be a component of US financial institutions’ operational risk management framework, as described in the regulatory capital rules and elsewhere.

Title V of the GLBA was the first federal law to require that financial institutions safeguard non-public personal information (NPPI) of their customers. The statute requires each prudential regulator to establish standards for financial institutions to:

- insure the security and confidentiality of records containing NPPI;
- protect against “any anticipated threats or hazards” to such records; and
- protect against unauthorised access of such records (the “Safeguards Rule”).

The Interagency Guidelines Establishing Information Security Standards (the “Security Guidelines”) that derive from this statutory mandate require all financial institutions to have information security programmes that further the objectives of the Safeguards Rule. In 2020, the OCC and the FDIC published a Joint Statement on Heightened Cybersecurity Risk (the “Joint Statement”), which elaborated on the Security Guidelines.

Cybersecurity risks are also addressed in the Interagency Guidelines Establishing Standards for Safety and Soundness (the “Safety and Soundness Guidelines”), which set out broad safety and soundness standards against which financial institutions are evaluated. As with other components of risk management, the prudential regulators expect a financial institution to tailor its cybersecurity risk management system to be proportionate to the size and the complexity of the institution and its risk profile.

In 2020, the prudential regulators published interagency guidance on Sound Practices to Strengthen Operational Resilience (the “Sound Practices”), which brought together existing regulations, guidance, statements and common industry standards for operational resilience. Acknowledging cybersecurity risk as “one of the most important types of operational risk”, the Sound Practices include an appendix with sound practices for managing cyber-risk.

The Federal Financial Institutions Examination Council (FFIEC) – an interagency body that promotes uniformity in the supervision of financial institutions – has also published examination manuals and guidance on cybersecurity risk management, including the FFIEC IT Examination Handbook.

Taken together, these rules, statements and guidelines, as well as the FFIEC examination manuals and supplements, provide the prudential regulators’ most current standards regarding managing cybersecurity risk.

3.2 ICT Service Provider Contractual Requirements

The Bank Service Company Act grants the prudential regulators statutory authority to supervise certain third parties that provide services

to financial institutions. In the case of IT, these third-party service providers include core application processors, electronic funds transfer switches, internet banking providers, item processors, managed security service providers, and data storage service providers.

In October 2012, concurrently with the release of the Supervision of Technology Service Providers Booklet (the “TSP Booklet”) of the FFIEC’s IT Examination Handbook (described in 3.1 **Scope of Financial Sector Operational Resilience Regulation**), the prudential regulators also released the Administrative Guidelines on the Implementation of Interagency Programs for the Supervision of Technology Service Providers. The guidelines describe how technology service providers (TSPs) are assessed for risk using the Uniform Rating System for Information Technology (URSIT). The URSIT score is used to determine the priority, frequency and extensiveness of the examinations of TSPs. TSPs are considered either significant service providers (SSPs), serving a large number of banks and posing higher risk, or regional service providers (RSPs), serving fewer banks and posing less risk.

The Multi-Regional Data Processing Servicer (MDPS) programme is a programme that specifically designates for special monitoring and interagency supervision TSPs that are considered “mission-critical” (vital to the successful continuance of a core business activity) for a large number of financial institutions that are regulated by more than one prudential regulator or provide services through a number of technology service centres located in diverse geographic regions.

the prudential regulators also conduct shared application software reviews (SASRs) to review major software packages used by a significant

number of financial institutions or for higher-risk applications in larger financial institutions (such as software packages for use in wire transfer, capital markets, or securities transfer).

Contractual Requirements

Although the prudential regulators have authority to supervise TSPs, financial institutions remain primarily responsible for ensuring that TSPs' activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations, and face liability for breaches or violations by a TSP. As such, financial institutions are expected to have robust third-party risk management processes, including contract development and ongoing monitoring. As described in the TSP Booklet, contracts between financial institutions and TSPs should include the following:

- the right to audit and conduct business continuity planning (BCP) testing;
- measurable service-level agreements (SLAs) for services being provided;
- default and termination provisions;
- the need for data security and confidentiality to, at a minimum, adhere to US regulatory standards (for foreign-based service providers);
- clear definitions of data ownership and handling expectations;
- the ability to request information describing a TSP's response to relevant regulations, supervisory guidance, or other notices from federal banking agencies;
- incident response and notification responsibilities; and
- the extension of contractual terms to subcontractors.

3.3 Key Operational Resilience Obligations

Financial institutions are required to maintain risk management systems that are proportional to the size and complexity of their organisation (known as "tailoring"). Given that risk management is institution-specific, regulators have not established any processes and controls for cybersecurity risk that are required, but the regulatory guidance and FFIEC manuals described in **3.1 Scope of Financial Sector Operational Resilience Regulation** provide standards and best practices to comply with regulators' objectives. The Joint Statement, described in **3.1 Scope of Financial Sector Operational Resilience Regulation**, summarises the elements of effective cybersecurity controls as:

- "response and resilience capabilities" – review, update and test incident response and business continuity plans;
- "authentication" – protect against unauthorised access; and
- "system configuration" – securely configure systems and services.

Incident and Reporting Obligations

The prudential regulators issued a rule, effective as of April 2022, requiring financial institutions to notify their primary regulator of any computer security incidents that rise to the level of "notification incidents". The final rule defines a "notification incident" as a computer security incident that the financial institution believes could "materially disrupt, degrade, or impair":

- "the ability of the banking organi[s]ation to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business;

- any business line of a banking organi[s]ation, including associated operations, services, functions and support, [where this] would result in a material loss of revenue, profit, or franchise value; or
- operations of a banking organi[s]ation, including associated services, functions and support, as applicable – the failure or discontinuance of which would pose a threat to the financial stability of the United States”.

Financial institutions must notify their primary regulator as soon as possible and no later than 36 hours after the financial institution determines that a notification incident has occurred. Each prudential regulator has designated their own points of contact for notification, available on each prudential regulator’s website.

3.4 Operational Resilience Enforcement

Enforcement of the laws and regulations described in **3.1 Scope of Financial Sector Operational Resilience Regulation** begins with the supervisory and examination authority of the prudential regulators. For financial institutions, cybersecurity risks are assessed during the course of a full-scope, on-site examination as part of the financial institution’s routine supervisory cycle or during a specialty examination, such as an IT examination. The prudential regulators have the authority to supervise TSPs, as described in **3.2 ICT Service Provider Contractual Requirements**, and TSPs are examined based on their risk level as calculated using an URSIT rating. The examinations of TSPs focus on issues such as management of technology, integrity of data, and confidentiality of information. Financial institutions are entitled to copies of the Report of Examination (ROE) of a TSP with which they have a contract.

Cybersecurity control deficiencies are generally not subject to public enforcement actions by prudential regulators unless the financial institution is subject to a major cybersecurity breach. Instead, the prudential regulators may issue a “matter requiring attention” (MRA), a “matter requiring immediate attention” (MRIA), or – in the case of the FDIC – a “matter requiring board attention” (MRBA), which are confidential supervisory findings that require the financial institution to take corrective action. The board of directors is expected to respond to MRAs, MRIAs, and MRBAs through written responses and progress reports, and the prudential regulators will continue to monitor corrective action until resolved. If the corrective action is not satisfactory to the prudential regulators, MRAs and MRIAs could lead to further formal or informal investigation or enforcement action. Formal enforcement actions may take the form of cease-and-desist orders, civil monetary penalty orders, or other actions.

3.5 International Data Transfers

The primary US restrictions on data transfers are not specific to the financial sector but apply more broadly to a range of identified transaction categories. The restrictions were established via Executive Order 14117 (2024) and implemented via DOJ regulation at Title 28, CFR 202.101 et seq and restrict the transfer of certain categories of bulk sensitive data and government information to identified countries of concern. The executive order also identifies certain control measures for defined categories of sensitive transactions that are not outright forbidden.

3.6 Threat-Led Penetration Testing

While other jurisdictions have implemented cyber-resiliency stress testing as part of their supervisory and review process, the USA does not have an equivalent required scenario stress test. Instead, financial institutions are encour-

aged to use standardised tools that incorporate industry standards and best practices to determine their cybersecurity risk. These tools include FFIEC Cybersecurity Assessment Tool (sunsetting in August 2025), the NIST Cybersecurity Framework, the Center for Internet Security Critical Security Controls, and the Financial Services Sector Coordinating Council Cybersecurity Profile.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

Legislation around cyber-resilience continues to develop in the USA, as follows.

- The Federal Reserve, in co-ordination with the OCC and the FDIC, has issued guidance in the form of a paper on operational resilience that includes an appendix of practices for cyber-risk management.
- Some regulations impose transparency obligations related to cyber-resiliency. By way of example, the SEC requires publicly traded companies to disclose measures taken to manage certain cyber-related risks. NYDFS regulations (described in greater detail in **6.2 Cybersecurity and AI**) impose similar disclosure requirements and technical obligations regarding backup systems to promote resiliency.
- Draft legislation that would create a task force directed to report on conclusions and recommendations related to protecting critical infrastructure from foreign state-sponsored threats has passed one house of Congress.

4.2 Key Obligations Under Legislation

Draft legislation would create a task force to consider steps that critical infrastructure companies can take to strengthen resilience against

foreign state-sponsored attacks (see **4.1 Cyber-Resilience Legislation**).

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

Unlike Europe, the USA does not have any security certification requirements for information and communications (ICT) products or services. CISA co-chairs the ICT Supply Chain Risk Management Task Force, a PPP that is charged with identifying challenges and solutions for managing risks in the global ICT supply chain. That task force has issued several handbooks and resource guides to help the private sector manage supply chain risk in ICT. Separately, the Federal Communications Commission (FCC) has created a voluntary cybersecurity labelling programme for wireless consumer internet of things (IoT) products – namely, the US Cyber Trust Mark. The Cyber Trust Mark is a label designed to demonstrate to consumers that devices with the label have met robust cybersecurity standards and is expected to launch in 2025.

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection Federal Data Protection Regulation

At the federal level, the GLBA directs covered financial institutions to provide notices about their information-sharing practices and to implement appropriate safeguards to ensure the security of customer information and protect against unauthorised access to such information. The Safeguards Rule, which is one of the GLBA's implementing regulations, includes prescriptive

security requirements, including implementing a written information security programme. This written information security programme must include risk assessments, access controls, data inventories, encryption, multifactor authentication, logging of access to customer information, regular monitoring and testing, training, and assessments of third-party service providers. The Safeguards Rule also requires covered financial institutions to designate an individual with responsibility for the programme, who must report in writing to the board at least annually. The Safeguards Rule also requires financial institutions to notify the FTC of security breaches involving unauthorised acquisition of at least 500 consumers' unencrypted information, no later than 30 days after discovering such event.

HIPAA is the primary law that regulates data privacy and security for healthcare providers (see **6.3 Cybersecurity and the Healthcare Sector** for more detail).

Additionally, the SEC's Regulation S-P ("Reg S-P") requires broker-dealers, investment companies, and registered investment advisers to provide notices about privacy practices, institute written policies and procedures that safeguard customer information, securely dispose of consumer report information, and adequately oversee third-party service providers. Reg S-P was recently amended to require covered entities to implement an incident response plan and provide data breach notifications to affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorisation.

State-Level Data Protection Regulation

Many states have passed comprehensive data privacy laws that also include cybersecurity requirements. Typically, these state laws require

covered entities to implement reasonable security measures to protect consumer personal data. The California Consumer Privacy Act includes a private right of action for consumers whose unencrypted personal information is subject to a breach of security due to the failure of the business to implement reasonable security measures. Additionally, in November 2024, the California Privacy Protection Agency (CPPA) released a proposed rule that would require covered businesses to conduct annual independent cybersecurity audits, present the results of the audit to senior executives at the business, and submit a certification of the audit to the CPPA.

6.2 Cybersecurity and AI

AI regulation is still nascent, but some government entities are starting to address the cybersecurity implications of AI. Although Congress has not passed any comprehensive AI bill to date, there have been Presidential executive orders on AI and cybersecurity. During the Biden administration, President Biden issued an executive order directing federal entities to implement guidance related to safety and security in the deployment of AI. In November 2024, the DHS released a voluntary framework for how to safely and securely deploy AI in critical infrastructure. However, on his first day in office in 2025, President Trump revoked former President Biden's executive order that had established initiatives related to the safe deployment of AI. President Trump has since issued two new executive orders on AI, which do not focus on cybersecurity, safety or accountability measures.

At the state level, the NYDFS's 23 New York Codes, Rules and Regulations (NYCRR) 500 ("Part 500") includes prescriptive requirements for covered financial services companies to implement cybersecurity safeguards, such as implementing multifactor authentication. In

October 2024, the NYDFS issued guidance on how companies can address the emerging security threats from AI. It includes recommendations such as updating employee training to expand awareness of AI-powered social engineering and designing access controls to better withstand deepfakes and other AI-enhanced attacks.

6.3 Cybersecurity in the Healthcare Sector

HIPAA is the primary law that regulates data privacy and security for healthcare entities. HIPAA's Security Rule includes prescriptive requirements for covered entities to implement specific safeguards to ensure the confidentiality, integrity and availability of ePHI, including through risk assessments, encryption, "minimum necessary" access controls, a contingency plan to restore any loss of data, and business associate contracts. In December 2024, the HHS published a Notice of Proposed Rulemaking and announced proposed changes to the Security Rule that would heighten the requirements for covered

entities – for example, newly requiring annual penetration testing, as well as a written technology asset inventory mapping the data flows of ePHI within the covered entity's systems. Shortly after his election, President Trump issued an executive order directing federal agencies to not propose or issue any rule until a department or agency head appointed by President Trump approved such rule. Accordingly, the future of these proposed amendments remains unclear.

Additionally, the HIPAA Breach Notification Rule requires covered entities to provide notification of certain breaches of protected health information to affected individuals, the HHS, and the media.

Through the Health Breach Notification Rule, the FTC separately requires vendors of personal health records and their third-party service providers to report certain breaches to affected individuals and the FTC.

Trends and Developments

Contributed by:

Beth George, Timothy Howard, Brock Dahl and Megan Kayo
Freshfields

Freshfields is a global market leader in handling data crises, investigations, class actions, and regulatory engagement. The firm has in-depth experience in cybersecurity – from prevention to governance to responding to incidents – and has a deep bench of cybersecurity and privacy attorneys who provide clients with global coverage from offices around the world, including in the USA, Europe, the UK, and Asia. With a

strong market-leading data and cyber practice comprising more than lawyers, Freshfields' global team of experts works seamlessly at the highest level, leveraging their expertise in crisis management and judicial proceedings to provide high-quality advice. This includes extensive know-how, honed through involvement in hundreds of international cases.

Authors



Beth George leads Freshfields' strategic risk and crisis management practice. Based in Silicon Valley, Beth regularly advises boards of private and public companies on risk

management and governance, including advising on governance related to AI, data practices and cybersecurity, content management, cybersecurity incidents, and geopolitical events. Her practice has included representing a large company facing high-profile congressional investigations and litigation regarding its data security practices, investigating alleged nation state insider threats at a leading tech company, and advising a public company in a high-profile breach that resulted in an FBI investigation and criminal charges.



Timothy Howard is Freshfields' US head of data security and is based in New York, where his practice focuses on white-collar and government regulatory investigations, with special

attention to cybersecurity, data breaches, and cryptocurrency. Tim is an accomplished trial lawyer and investigator, having managed cases across a range of disciplines, including securities fraud, tax fraud, Foreign Corrupt Practices Act violations, cyber-intrusions, and healthcare fraud. He has advised Freshfields' clients on complex cross-border data breach incidents, including managing incident response, forensic investigation and engagement with regulators, Department of Justice and SEC investigations, and advising companies on AI, cybergovernance, and other data security risks.

USA TRENDS AND DEVELOPMENTS

Contributed by: Beth George, Timothy Howard, Brock Dahl and Megan Kayo, **Freshfields**



Brock Dahl brings cutting-edge cyber experience to Freshfields from his time at the National Security Agency (NSA). As deputy general counsel in operations at the NSA, Brock

advised leadership on how to achieve mission objectives within the boundaries of state, federal and international cyber, privacy, and national security laws. He has a deep understanding of advanced technologies and the legal challenges they raise and has played a key role in the US government's response to significant global cyber-incidents in recent years.



Megan Kayo of Freshfields specialises in cybersecurity and privacy issues. Based in Silicon Valley, she has worked on hundreds of data breach incidents, including

investigations, notifications and interactions with regulators and affected individuals. Megan represents clients in regulatory investigations of their information security programmes, products (including generative AI products), and their responses to data breaches and security incidents. She also helps clients with privacy compliance and data governance, including risk assessment and management, breach mitigation, business continuity and disaster recovery planning, oversight of third-party service providers, due diligence in corporate transactions, and board of director advice and counselling.

Freshfields

3 World Trade Center
175 Greenwich St
51st Floor
New York
NY 10007
USA

Tel: +1 212 277 4000
Fax: +1 212 277 4001
Email: beth.george@freshfields.com
Web: www.freshfields.us

FRESHFIELDS

Current Cybersecurity Threats Faced by US Companies and How to Minimise Liability in the Event of a Cyber-Attack

Top of mind for many US cybersecurity executives has been the threat of personal liability for cybersecurity incidents. In late 2023, the SEC charged SolarWinds' chief information security officer Timothy Brown for defrauding investors by making public statements regarding the company's cybersecurity standards that he allegedly knew was not accurate. SolarWinds provides cybersecurity software to thousands of companies. In 2020, it suffered a supply chain attack whereby nation state threat actors were able to insert code into a software update that allowed the threat actors to access SolarWinds customers' networks, leveraging the accesses that SolarWinds' software was given on these systems.

Relying on internal communications between information security engineers at SolarWinds, in addition to accusing the company of having inadequate internal accounting controls, the SEC alleged that Brown defrauded investors by falsely touting SolarWinds' cybersecurity strength. Specifically, the SEC alleged Brown was aware that the company's security controls were weak but he nevertheless approved the company's risk factors on cybersecurity – which the government described as “generic” – and supported a number of other public statements about the company's high cybersecurity standards, including blogs and a security statement that was provided to actual and prospective customers.

In 2024, a federal district court dismissed some – but not all – of the charges against Brown. Even though the court disagreed with the SEC's accusation that the risk factors were “generic”, it did find that the company's public “security

statement” (which was posted on its website and discussed its cybersecurity standards) could be a material statement. Whether the statement was inaccurate, and whether Brown was aware the statement was inaccurate, are issues that the court allowed to proceed to trial.

The SEC case is not the only case in which senior executives have faced personal liability. In 2023, the Federal Trade Commission (FTC) finalised a settlement with Drizly, an app for the delivery of alcohol, that imposed personal liability on its CEO for the company's security failures. The FTC alleged that Drizly and its CEO implemented woefully inadequate cybersecurity practices at the company, resulting in a data breach affecting more than 2.5 million customers.

In the settlement, which included a consent decree binding the company, the FTC reached an agreement that Drizly CEO James Cory Rellas would be required to implement an information security programme at any future company where he was a majority owner, CEO, or senior officer with information security responsibilities, if that company collected consumer information from more than 25,000 individuals. The settlement ensured that these requirements would follow Rellas to future companies, likely due in part to the fact that Drizly had been acquired by another company.

These cases highlight a newly aggressive posture of regulators towards executives who have cybersecurity responsibility. In the aftermath of the SolarWinds charges, many companies have reviewed their directors' and officers' liability insurance to ensure it covers senior security professionals. The cases also highlight the importance of ensuring that executives understand their legal obligations regarding accurate disclosures, including with regard to cybersecurity

controls, and the importance of ensuring companies meet certain cybersecurity standards.

Ransomware

Ransomware continues to be a leading cybersecurity threat for corporations, with several companies reporting multiple attacks within the course of a year. Threat actors in this space have commodified software supporting the attacks – a trend dubbed “ransomware as a service” (RaaS) – thereby making the attacks more accessible and executable by less sophisticated actors.

RaaS is a business model in which cybercriminals provide ransomware tools and services to other attackers, often for a fee or a share of the ransom payments. Essentially, RaaS operators develop and maintain the ransomware software, while affiliates or customers use it to carry out attacks. The RaaS operators typically provide user-friendly interfaces, technical support, and even updates to ensure the ransomware remains effective. This approach has led to an increase in the frequency and scale of ransomware attacks, as it lowers the barrier to entry for cybercriminals and allows them to focus on targeting victims and extorting payments.

Additionally, the RaaS model can make threat actors more unpredictable. Famously, the BlackCat ransomware gang had a very public falling out with one of its affiliates in connection with the Change Healthcare attack that – according to the company’s public statements – may have affected the personal information of approximately 190 million individuals. Reportedly, the company made a USD22 million ransom payment to the BlackCat ransomware gang to try to get services back online and for the ransomware gang to delete the company’s stolen data. However, the affiliate who claimed to have given BlackCat access to the company’s network also

claimed that BlackCat cheated the affiliate of its share of the ransom. Accordingly, the affiliate did not delete the information that Change Healthcare had reportedly paid BlackCat to return and destroy.

In 2024, ransomware demands and payments also continued to climb, reflecting the evolution and aggressiveness of cybercriminals’ tactics. In 2024, ransomware attacks increased in both frequency and scale, with the average ransom demand reaching more than USD3 million and the average ransom paid estimated at more than USD9.5 million. The increase in ransomware payments has been largely driven by the continued success of extortion schemes whereby attackers often exfiltrate data prior to encrypting it, threatening to release sensitive information if ransoms are not paid, in addition to seeking payment for the decryption keys.

Ransomware attackers have also threatened to deploy distributed-denial-of-service attacks or threatened employees and customers of victims so as to apply additional pressure on companies. Some attackers have even notified regulatory authorities of victims’ data breaches, using the law as a means of exerting pressure. The emergence of new groups and ransomware variants of cyber-attacks, including rebranded ransomware groups, has also contributed to the record-breaking number of incidents and payments.

There have been ongoing law enforcement efforts, including a successful 2024 bust of infrastructure used by the Lockbit, a leading ransomware group. Nevertheless, the overall threat continues to grow, increasing pressure on companies to have plans for detection of ransomware attacks and develop plans for sophisticated recovery.

Supply chain attacks

Beyond ransomware attacks, supply chain attacks continue to be a significant issue. Hackers have found that third-party vendors (including security vendors) can create successful avenues of attacks, allowing them to leverage accesses and service deliveries to the vendors' customers to amplify their attack space. In addition to the SolarWinds attack, in June 2023, a significant cyber-attack exploited a vulnerability in managed file transfer software MOVEit. The vulnerability allowed attackers to steal files from organisations through SQL (structured query language) injection on public-facing servers. This breach affected thousands of organisations and millions of individuals – including government agencies, media outlets, and organisations in other sectors – and was considered one of the largest supply chain attacks to date. The C10p ransomware gang, a Russian-affiliated cyber group, claimed responsibility for the attack.

Cyber-attacks on and exploitation of vulnerabilities at vendors have resulted in significant losses for their customers. In fact, supply chain risk has become such a significant issue that the US' National Institute of Standards and Technology (NIST) released its first major update of the NIST Cybersecurity Framework, incorporating practices to manage cybersecurity risks within and across organisations' supply chains.

Supply chain attacks can be more challenging to investigate, as an affected customer may have limited visibility into an attack on a third-party vendor and limited control over the vendor's investigation. Companies need to assess which of their vendors have the greatest access to their systems – and thus are the highest risk – in order to identify the greatest risks posed by supply chain attacks. By focusing on those highest-risk areas, companies can develop

mitigations by placing technical limitations and increased monitoring on those vendors as well as by requiring the vendors to engage in robust cybersecurity practices, in addition to potentially shifting liability through contractual agreements.

Cybersecurity and AI

Cybercriminals are increasingly using AI to automate and target their attacks. This allows them to carry out individualised mass phishing attacks tailored to their targets – not only greatly increasing the efficiency of the attacks, but also allowing well-organised threat actors to automatically create fake login pages that are virtually indistinguishable from the legitimate pages. Additionally, research has indicated that the use of AI will significantly improve the capability of threat actors to crack passwords.

AI also allows threat actors to replicate proofs of concept or other types of successful attacks more quickly. By way of example, if a zero-day vulnerability is identified, the amount of time for threat actors to identify and target companies with such vulnerabilities in their systems is becoming shorter. The dwell time that threat actors are in a company's systems is also decreasing, as AI allows threat actors to identify data that appears to be valuable more efficiently and thus extract that data more quickly.

There is some good news, however. AI is increasingly being leveraged in cyberdefence to enhance the detection and prevention of cyberthreats and enhance the response to such threats. One of the primary applications of AI in this field is the identification and quarantine of suspicious emails that may be part of phishing campaigns. AI-powered tools use machine-learning algorithms to analyse email content and detect phishing attempts by identifying patterns

and anomalies that are indicative of malicious intent.

Another significant application of AI in cyberdefence is the detection of vulnerabilities and malicious or anomalous activity within a company's systems. These tools utilise AI to monitor network traffic and identify unusual behaviour that could signify a cyber-attack. By continuously learning from the network's normal behaviour, these tools can quickly detect deviations and alert security teams to potential threats.

Although AI tools and systems can benefit companies, cybersecurity plays a crucial role in ensuring that AI systems are resilient to attempts by malicious third parties to exploit the system's vulnerabilities and thereby alter the system's behaviour, performance or security properties. Cyber-attacks against AI systems can exploit AI-specific assets, such as training data sets or trained models, but also vulnerabilities in the AI system's (underlying) digital assets or the underlying ICT (information and communications technology) infrastructure. To address these risks, the EU AI Act requires certain high-risk AI systems to meet a specific cybersecurity standard.

Insider threats

With the increase in remote work and readily available AI tools during the past few years, there has also been an uptick in insider threat risk from nation state actors. North Korea, in particular, has been exploiting the recruitment and onboarding processes to install thousands of fraudulent remote IT workers at companies. These fraudsters typically use falsified or stolen identities to secure their positions. The wide availability of AI tools reportedly has increased this trend, as these tools help the fraudulent IT workers to create convincing profiles and evade detection during the hiring process.

Once hired, these fraudulent IT workers can remotely access company systems within the scope of their job responsibilities and steal proprietary information, which they can then use to extort payment from the victim company. Alternatively, fraudulent IT workers can deploy malware within the network or create backdoor access into the company's network for future cyber-espionage campaigns, as they often have deeply embedded and difficult-to-detect access to company systems. Additionally, this creates sanctions risk, given that the US Treasury's Office of Foreign Assets Control recently advised that the vast majority of these fraudulent IT workers' earnings were used to fund North Korea's weapons of mass destruction and ballistic missile programmes.

Mitigation measures

While cyber-attacks such as ransomware, supply chain attacks, and insider threats are pervasive, there are measures that companies can take to mitigate the impacts of such incidents, including:

- regularly updating and patching systems – given that exploited vulnerabilities are one of the most common attack vectors and easily accessible AI tools are increasing the rate at which zero-day vulnerabilities are exploited;
- conducting employee training on phishing and social engineering, as another one of the most common attacks vectors is phishing;
- using advanced threat detection and response tools, as industry research and statistics show that the cost of responding to incidents is significantly lower for companies that have deployed such tools within their systems;
- maintaining an asset inventory to ensure the company has visibility of all its endpoints and throughout its systems;

Contributed by: Beth George, Timothy Howard, Brock Dahl and Megan Kayo, **Freshfields**

- implementing network segmentation, including by following the principle of least privilege and limiting third-party access to systems and data;
- sufficiently logging and monitoring, which is crucial for any investigation and can help identify anomalous behaviour that could signal an insider threat risk; and
- regularly backing up critical data and testing those back-ups to help minimise the impact of ransomware and increase the likelihood that the company can recover without making a ransom payment.

Leveraging these practices as part of a comprehensive information security programme may not prevent all incidents. However, such practices can minimise damage if a cyber-attack occurs, which – in turn – can minimise liability (including personal liability) in relation to a cyber-attack.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com