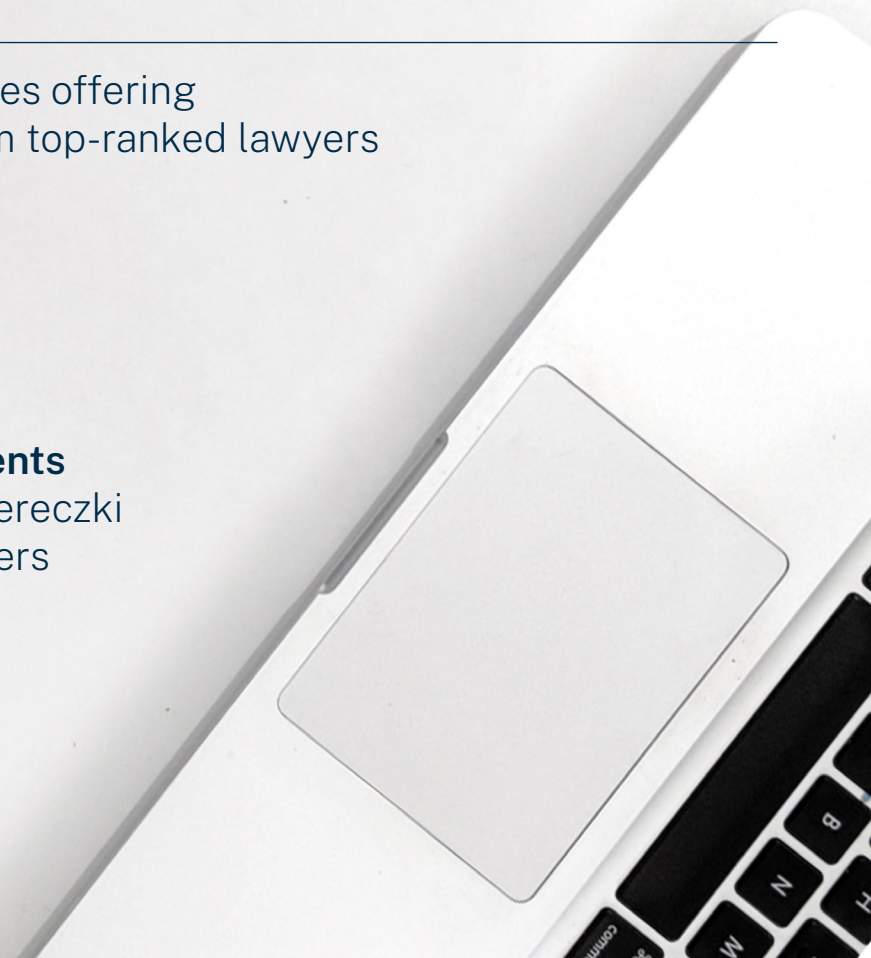
Chambers
AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2025

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

Hungary: Law & Practice
and Trends & Developments
Adam Liber and Tamás Bereczki
PROVARIS Varga & Partners



HUNGARY

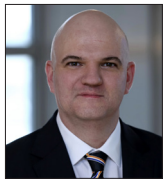
Law and Practice

Contributed by:
Adam Liber and Tamás Bereczki
PROVARIS Varga & Partners

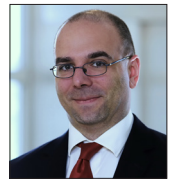
Contents

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 LLM 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

1053 Budapest
Károlyi utca 9
CENTRAL PALACE
5th floor

Tel: +36 70 605 1000
Email: info@provaris.hu
Web: www.provaris.hu

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Hungary adheres to a singular legislative privacy regime without any regional variations in data protection laws. The national framework, integrating the GDPR and Hungarian law, is consistently enforced throughout the country. This legal structure showcases a significant interplay between national regulations and multinational frameworks, especially those established by the European Union. Hungary is also a participant in international data protection agreements, including the Convention for the Protection of Individuals with Automatic Processing of Personal Data and its amending Protocol.

Key aspects of Hungary's data protection law in relation to multinational systems include:

- GDPR Implementation: Hungary has aligned its national laws with the EU's GDPR. In instances of conflict between GDPR and Hungarian privacy rules, GDPR takes precedence, as confirmed by Hungary's National Authority for Data Protection and Freedom of Information (*Nemzeti Adatvédelmi és Információszabadság Hatóság,* or NAIH).
- Directive (EU) 2016/680 of the European Parliament and of the Council (the "Law Enforcement Directive") Implementation: Act No CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (the "Information Act") in Hungary serves as the primary legislation implementing the EU's Law Enforcement Directive.
- E-Privacy Laws: Hungary has incorporated the EU Directive on privacy and electronic communications into its national law, primarily through the Act on Electronic Commerce and Information Society Services and the Act on Electronic Communications.

In the EU's cross-border data protection framework, the NAIH collaborates with authorities in other member states under the GDPR's one-stop-shop mechanism. This system allows a lead supervisory authority, typically in the country where a company's main EU establishment is located, to primarily enforce GDPR, with NAIH providing support when needed.

Legal Background

In Hungary, privacy and data protection are governed by a combination of the national constitu-

tion, specific laws, EU regulations, and guidelines. The Hungarian legal framework for data protection is primarily influenced and governed by the EU's GDPR, but it also includes national and sectorial laws that complement or specify the GDPR's provisions.

- Constitutional Laws: The Fundamental Law of Hungary, which is the country's constitution, provides the basis for privacy and data protection rights. Article VI guarantees the respect for and protection of private and family life, communication, and the protection of personal data.
- GDPR: As a member of the EU, Hungary is subject to the GDPR which applies directly in Hungary and has significantly influenced national laws and practices.
- GDPR and Law Enforcement Directive Implementation: The Information Act is the main piece of national legislation supplementing the GDPR in Hungary and it also implements the Law Enforcement Directive. The scope of the Information Act applies broadly to any data processing activity covering automatic as well as manual data processing, even if the personal data is not contained or intended to be contained in a filing system.
- Sector-Specific Regulations: Various other laws and regulations address data protection in specific sectors, such as employment, healthcare, genetic data, criminal laws, including:
  (a) Act XLVII of 1997 on the Processing and Protection of Health and Related Personal Data (the "Health Data Act") lays down the detailed rules for the processing and the professional secrecy obligations of medical personnel.
  (b) Act No CVIII of 2001 on Electronic Commerce and Information Society Services is the primary legislation implementing the EU Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
  (c) Act No C of 2003 on Electronic Communications implements the Directive on privacy and electronic communications with regard to electronic communication services.
  (d) Act No XXI of 2008 on the Protection of Human Genetic Data and the Regulation of Human Genetic Studies, Research and Biobanks regulates the processing of human genetic data, including the transfer of such data to other countries.
  (e) Act I of 2012 on the Labour Code (the "Labour Code") stipulates that the employer must respect the personal rights of workers. Employers may monitor the behaviour of workers only to the extent pertaining to the employment relationship. Monitoring measures must respect human dignity. The employer may not monitor the private lives of workers.
  (f) Act C of 2012 on the Criminal Code (the "Criminal Code") penalises breaches of privacy (Section 219) and breaches of privacy of correspondence and communications (Section 224), which apply to illegal wiretapping and eavesdropping of electronic communications.
  (g) Act V of 2013 on the Civil Code (the "Civil Code"): Sections 2:42 and 2:48 of the Civil Code establish the general protection of personality rights, including rights to recorded images and voice.
  (h) Act LIII of 2018 on the Protection of Privacy: Section 8(1) of this Act protects the right to respect private life, including

voice recordings and it establishes the right to bring civil law claims if this right is violated. Section 11 of the Act generally protects the privacy of communications.

1.2 Regulators

The NAIH, Hungary's chief data protection authority, serves as the independent overseer of the country's data protection rights. Its core role is to ensure the lawful and secure processing of personal data by enforcing data protection laws. The NAIH's responsibilities include setting and implementing regulations and guidelines, and compelling organisations to maintain stringent data security standards. It conducts investigations and audits to verify compliance with data protection laws, focusing on organisations' data security measures. Additionally, the NAIH regulates data breach notifications, ensuring timely reporting of breaches and implementation of risk mitigation strategies. The authority also educates and advises data controllers on best practices for data protection and security. The NAIH has the power to enforce penalties and legal actions against entities that breach data security and privacy regulations.

1.3 Enforcement Proceedings and Fines

Enforcement Environment in Hungarian Data Protection Law

In the realm of data protection in Hungary, the enforcement environment encompasses various types of sanctions to ensure compliance with data protection regulations. These sanctions are designed to address different aspects of non-compliance and are critical in maintaining the integrity of data protection practices. The key types of sanctions include:

- Administrative Fines: These are the primary sanction under the GDPR framework. In cases of non-compliance, organisations may face substantial fines, which can amount to up to EUR20 million or 4% of their annual global turnover, whichever is higher. These severe financial penalties underline the importance the EU places on data protection. The fine that may be imposed on a state budget authority is capped at a maximum of HUF20 million (approximately EUR52,000).
- Civil Law Sanctions: Hungarian law enables individuals to initiate private legal actions against data controllers and processors for breaches of data protection rules. This right empowers data subjects to seek redress directly, including pecuniary (financial) and non-pecuniary (such as emotional distress) damages.
- Criminal Sanctions: In more severe instances, where the abuse of personal data is driven by financial gain or causes significant harm to individuals, criminal penalties can be imposed by Hungarian criminal courts.

Data Protection Procedures of the NAIH

The NAIH in Hungary conducts two main types of procedures in data protection cases: investigation procedures and administrative procedures for data protection.

- Investigation Procedure: This can be initiated by complaints from data subjects, third parties, data controllers/processors, or by the NAIH itself. Its purpose is to gather evidence and ascertain if there has been a breach of data protection laws. If no breach is found, the case is closed. However, if unlawful data processing is identified, the NAIH may instruct the data controller to rectify it within 30 days. Failure to comply or severe breaches can lead to an administrative procedure.
- Administrative Procedure: This serves as the primary enforcement mechanism, enabling the NAIH to impose fines or other corrective

measures. It can be initiated independently of an investigation procedure.

Both procedures can be triggered ex officio or through complaints. For administrative procedures, complaints can only be filed by the directly affected data subject. The NAIH has extensive investigatory powers, including on-site inspections and access to data processing equipment. Controllers are often required to provide GDPR-compliant documentation swiftly, highlighting the importance of GDPR's accountability principle.

Fine Calculation

Regarding the calculation of fines, the EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR generally apply.

According to the Information Act, the NAIH shall consider all circumstances of the case to decide whether imposing a fine is justified and to determine the amount of the fine. In particular, the NAIH takes into account:

- the scale of the group affected by the infringement;
- the severity of the infringement;
- the culpability of the behaviour; and
- whether the infringer has previously been found to have committed a breach of personal data protection rules.

Under the Act on the Sanctions for Administrative Violations, when imposing a fine, the NAIH must evaluate all relevant circumstances of the case, including but not limited to the criteria set forth in the Information Act. Specifically, the NAIH shall also consider the following factors in determining the amount of the fine:

- the harm caused by the infringement, including costs related to preventing, mitigating, or remedying the harm, as well as the benefits gained through the infringement;
- the reversibility of the harm caused by the infringement;
- the scale of the group affected by the infringement;
- the duration of the infringing conduct;
- the frequency and recurrence of the infringing behaviour;
- the infringer's co-operative conduct and assistance during the proceedings; and
- the economic standing of the infringer.

1.4 Data Protection Fines in Practice

- Incomplete Camera Warning Signs in Bank Lobby: In 2024, the NAIH fined a bank approximately EUR145,000 for deficiencies in the camera warning signs in the lobby of a branch office. The NAIH highlighted that camera warning signs must be detailed and placed at the entrance, with references to detailed privacy information, and that a simple pictogram is insufficient. Detailed notices must not be placed where access is limited outside business hours and should also be available online. A single data subject's complaint led to an investigation of the transparency practices concerning all branches. The unlawful practice persisted for one-and-a-half years, which was considered an aggravating factor, but the bank's prompt correction of the issue was treated as a mitigating circumstance. A three-day delay in responding to the data subject's request was noted but did not result in a fine.
- AI Use: In 2022 the NAIH imposed a fine of approximately EUR650,000 on one of Hungary's largest banks for using emotion analysis software in customer care. This decision was later upheld by the court, reinforcing the

NAIH's position on the importance of GDPR compliance in AI applications, especially in automated decision-making and profiling. In this instance, the bank employed AI technology for applying sentiment analysis on every incoming phone call, which the NAIH found disproportionate in terms of the risks posed to data subjects' fundamental rights. The NAIH highlighted that the bank did not provide any information about the application of this technology and therefore data subjects were deprived of their respective data subject rights. This decision highlights the NAIH's stringent stance on ensuring that AI and ML applications, especially those involving automated decision-making and profiling, comply with GDPR principles. It also underscores the necessity for data controllers to conduct thorough data protection impact assessments and balancing test assessments when implementing AI solutions.

- Cookies Use and Dark Patterns: The NAIH fined a leading Hungarian media service provider approximately EUR25,000 for failing to comply with lawful, fair, and transparent data processing in cookie management, based on the Interactive Advertising Bureau (IAB) Europe's Transparency and Consent Framework. The NAIH found that cookie usage and assigning identifiers constitute personal data processing. The controller must clearly define, describe, and justify processing purposes and legal bases, ensuring cookie banners meet fairness and transparency standards. The authority criticised the provider's lengthy, confusing banner text, the complex process for selecting data transfer partners, and the misleading presentation of consent and legitimate interest. The NAIH highlighted the need for easy consent withdrawal, critiquing the design where the "Reject All" option was less accessible than "Accept All Cookies". The decision aligns with the Belgian Data Protection Authority's ruling against IAB Europe's framework.
- Digi Case: In another instance, the NAIH fined an electronic communications service provider, Digi Távközlési és Szolgáltató Kft., EUR250,000 due to a personal data breach resulting from a known website vulnerability. The NAIH's investigation revealed that the service provider had failed to address this vulnerability for years, neglecting its own internal security policies. The authority cited several aggravating factors, including the prolonged existence of the vulnerability and the large number of affected data subjects. The service provider appealed the decision, leading to a referral to the Court of Justice of the European Union (CJEU) for a preliminary ruling on the interpretation of GDPR principles related to purpose and storage limitation. In October 2022, the CJEU clarified that further processing of personal data for carrying out tests and correcting errors must be compatible with the original collection purposes and that data should not be retained longer than necessary. Subsequently, the NAIH reassessed the case and, in June 2023, reduced the fine to approximately EUR208,000.

1.5 AI Regulation

The Hungarian government has adopted Resolution No 1301/2024 (IX. 30.) on the implementation of the European Parliament and Council Regulation (2024/1689/EU) on artificial intelligence in Hungary. The resolution provides that the domestic implementation of the AI Act shall be overseen by a specialised organisation established by law under the supervision of the Minister for the National Economy. This responsibility was not assigned to the NAIH. This organisation ensures a one-stop shop for administrative procedures, performs market surveillance tasks,

and operates a regulatory sandbox, providing opportunities for the preliminary testing of artificial intelligence developments. Additionally, the Resolution provides that the Hungarian Artificial Intelligence Council will be established, with members delegated by the NAIH, as well as the NMHH (National Media and Infocommunications Authority), MNB (Hungarian National Bank), GVH (Hungarian Competition Authority), SZTFH (Supervisory Authority for Regulated Activities), and DMÜ Zrt. (Digital Government Agency). The Council may issue guidelines and opinions regarding the implementation of the Regulation.

The Bill No T/10011 was submitted to the Hungarian Parliament by the Hungarian government on 19 November 2024, proposing measures necessary for implementing the European Parliament and Council Regulation on artificial intelligence. This draft law aimed to designate the Hungarian Minister of Justice as the authority responsible for ensuring the protection of fundamental rights in connection with the implementation of Article 77 of the AI Act. However, the legislative proposal was later withdrawn before reaching the Parliamentary Legislative Committee upon the recommendation of members of the governing party, without any justification being provided for the withdrawal.

1.6 Interplay Between AI and Data Protection Regulations

The intersection of AI regulation and data protection laws in Hungary reflects the broader European Union regulatory framework, primarily shaped by the GDPR and the EU's AI Act. These two frameworks aim to address different aspects of technological innovation but are closely interlinked, particularly when AI systems process personal data. The NAIH is the primary body overseeing GDPR compliance in Hungary. Although the NAIH will likely play an advisory role in AI regulation, the implementation of the AI Act is set to involve a specialised organisation under the supervision of the Minister for the National Economy or the Minister of Justice, as outlined in Hungary's recent governmental decisions. This suggests a separation of oversight responsibilities between general data protection and AI-specific risks.

2. Privacy Litigation

2.1 General Overview

In Hungarian legal proceedings, specific standards for alleging data protection violations are not defined, but adherence to the established evidentiary rules in procedural legislation is required. Litigation often incorporates a variety of evidence, including documents, witness statements, and expert insights. The Information Act enables individuals to initiate private legal actions against data controllers or processors for violating data protection laws.

2.2 Recent Case Law

Under Section 2:52 of the Hungarian Civil Code, individuals whose personality rights have been infringed may claim grievance awards (*sérelemdíj*) for non-pecuniary damages. The law presumes that harm occurs automatically when a violation is established, eliminating the need for claimants to prove actual damage. Courts can determine the amount of the award in a lump sum, considering the severity of the infringement, its recurrence, the degree of fault, and the impact on the claimant and their environment. The Budapest Court of Appeal in case Pf.20300/2024/7 emphasised the distinct nature of the sanctioning systems under the Hungarian Civil Code and the Information Act. It held that a violation of data protection regulations does not automatically amount to an infringement

of personality rights under the Civil Code. The consequences of unauthorised data processing under the Information Act differ from those under the Civil Code, and claims for grievance awards for data processing violations must primarily rely on the Information Act's framework. The Curia (the Supreme Court), in decisions Pfv. IV.20.927/2020/7 and Pfv.IV.21.084/2020/4, also confirmed that not all data protection breaches result in violations of personality rights. The Civil Code and Information Act protect personality differently, with separate legal standards and scopes of protection.

The New Civil Code Advisory Board has opined that the occurrence of non-pecuniary harm is a prerequisite for awarding a grievance award. Therefore, even if an infringement is established, the claim for a grievance award may be denied if no actual harm is demonstrated. Article 82 of the GDPR establishes that any person who suffers material or non-material damage as a result of an infringement of the GDPR has the right to receive compensation from the controller or processor responsible for the damage. The provision aims to protect individuals' data rights and ensure accountability for GDPR violations.

The Curia, in decision Pfv.20003/2024/13, provided clarity on the interpretation of GDPR Article 82 in Hungary. It ruled that the mere occurrence of a GDPR violation does not automatically entitle a data subject to compensation. Claimants must demonstrate actual damage – whether material or non-material – and establish a direct causal link between the infringement and the harm suffered. The judicial practice underscores the nuanced relationship between the Civil Code grievance awards and the GDPR compensation mechanism. Under the Civil Code, the presumption of harm simplifies the claimant's burden in personality rights cases, but judicial scrutiny still considers the specific circumstances of the case. In contrast, Article 82 of the GDPR requires proof of actual damage and a causal link, focusing on the material or non-material harm caused by data protection violations.

2.3 Collective Redress Mechanisms

From June 2023, it is possible to file class actions for GDPR infringements. These class actions allow competent authorities and representative organisations to represent a broad consumer base adversely affected by unlawful data protection practices, seeking civil law remedies in court. Aligning with GDPR guidelines, the Information Act clarifies that in legal disputes, the burden of proof to demonstrate compliance with data protection regulations rests on the data controller or processor who is the defendant. The courts can award both damages and injunctive relief.

3. Data Regulation on IoT Providers, Data Holders and Data Processing Services

3.1 Objectives and Scope of Data Regulation

Hungary does not have specific regulations governing IoT. Instead, sector-specific laws establish general information security and cybersecurity requirements in high-risk industries where IoT is widely used. The NAIH issued guidance on smart energy metres in 2019. The data protection impact assessment (DPIA) blacklist mandates a DPIA for public utilities using smart metres.

3.2 Interaction of Data Regulation and Data Protection

The GDPR establishes stringent standards for the processing of personal data, emphasising principles such as lawfulness, fairness, trans-

parency, data minimisation, and purpose limitation. These principles take precedence over other data-related regulations to ensure the fundamental rights of individuals are upheld. The Information Act complements the GDPR by addressing specific national concerns, including data processing for purposes of law enforcement, national security, and defence, which may fall outside the direct scope of the GDPR. Certain sectors, such as healthcare and finance, are subject to additional data protection obligations under Hungarian law. For instance, the Health Data Act governs the processing of health-related personal data, implementing a comprehensive regulatory framework for entities in the healthcare sector. These sectoral laws often impose more stringent requirements to address the unique nature of data processing activities within these fields.

3.3 Rights and Obligations Under Applicable Data Regulation

IoT providers and data processors in Hungary must ensure lawful data processing based on legal grounds such as consent, contractual necessity, or legal obligations. Transparency is required through clear privacy notices, and data subjects' rights (access, deletion, correction, etc) must be respected. Strong technical and organisational measures, such as encryption, are necessary to protect data security. High-risk processing requires a DPIA, and data breaches must be reported to the NAIH within 72 hours. Data processing agreements are mandatory for third-party processors, and a Data Protection Officer (DPO) must be appointed for large-scale or sensitive data processing.

3.4 Regulators and Enforcement

The NAIH oversees compliance with data protection laws, including the GDPR and the Information Act. Other regulatory bodies, such as the Hungarian Competition Authority (GVH), the National Media and Infocommunications Authority (NMHH), may also play roles in enforcing data protection and cybersecurity regulations within their respective sectors. The Supervisory Authority for Regulated Activities (SZTFH) and the Special Service for National Security (NBSZ) also play a pivotal role in enforcing cybersecurity regulations, particularly concerning the implementation of the NIS2 Directive. Established to oversee compliance with cybersecurity standards, the SZTFH and NBSZ ensure that organisations adhere to national and EU-level cybersecurity requirements.

4. Sectoral Issues

4.1 Use of Cookies

The use of cookies in Hungary is primarily governed by the ePrivacy Directive as implemented through the E-Commerce Act (Act CVIII of 2001 on Electronic Commerce and Information Society Services) and complemented by the GDPR for personal data processing. Hungarian regulations require that cookies be categorised based on their purpose, with explicit user consent necessary for all non-essential cookies. Essential cookies, such as those facilitating communication or strictly required for the provision of services explicitly requested by users, are exempt from the consent requirement. However, even in these cases, transparency is mandatory, requiring clear notice to users about the cookies in use, their functions, and the scope of data processing.

Consent for cookies must be voluntary, informed, and obtained through a clear affirmative action by the user. Practices such as pre-ticked checkboxes or ambiguous consent mechanisms are considered non-compliant under both the GDPR

and the ePrivacy Directive. Cookie banners must provide an "Accept All" and "Reject All" button with equal prominence, ensuring users have an easy and straightforward option to refuse cookies. Consent must also be specific and granular, meaning users should be able to decide individually on different cookie categories. Importantly, once consent is withdrawn, cookies must be securely deleted or rendered inoperative on the user's device. This reinforces the requirement for data controllers to ensure technical solutions that respect user preferences and maintain compliance throughout the lifecycle of cookie use.

Transparency plays a critical role in cookie management. Websites must provide clear, detailed, and accessible information about each cookie, including its name, purpose, expiration date, and any third parties involved in data collection or processing. Multi-layered approaches to informing users, such as brief notices linked to more comprehensive details, are generally considered effective. Social media plugins and similar technologies that involve data sharing with third-party platforms must be set to inactive by default and activated only after obtaining explicit user consent. These plugins should include detailed notices explaining the scope of data collection, including any potential data transfers outside the EU, ensuring users are fully informed about the implications of their consent.

Regulatory authorities in Hungary, including the NAIH, the NMHH, and the HCA, actively enforce compliance with these requirements. Non-compliance risks include significant fines, reputational damage, and operational disruptions. Recent enforcement actions have highlighted the importance of avoiding manipulative practices, such as "dark patterns", which could mislead users or undermine genuine consent. These practices, including cookie walls, hidden rejection options, or deceptive banner designs, may be deemed unfair commercial practices, leading to additional scrutiny under consumer protection laws.

4.2 Personalised Advertising and Other Online Marketing Practices

In Hungary, online marketing is regulated by the provisions of the Act XLVIII of 2008 on Business Advertising Activity (the "Advertising Act") and by the E-Commerce Act. Direct marketing is permissible only based on the explicit opt-in consent of the targeted individual and this consent requirement is independent from the B2B or B2C standing of the recipient. The relevant legal requirements can be summarised as follows:

- Consent to Direct Marketing Communications: The Advertising Act requires the natural person recipient's explicit consent to any direct marketing communications. The Advertising Act requires that the opt-in consent language for direct marketing communications must:
  - (a) be explicit;
  - (b) contain the name of the person providing the consent;
  - (c) identify the scope of personal data for which consent is being provided; and
  - (d) state that the consent is being given voluntarily in possession of the information about the data processing (this means that the sign-up language should provide a reference to the privacy notice providing information about data processing relating to sending email marketing messages by the sender); and
  - (e) if the consent is sought for sending electronic marketing messages that may be addressed only to persons of a specific age, then the opt-in consent language must also contain the place and date of birth of the person providing the consent.

Permission-based electronic marketing messages and communications with social, societal aims are subject to the same consent requirements as applicable to direct marketing communications.

- Soft Opt-In: The explicit consent requirement for electronic direct marketing is general because the soft opt-in exemption (as provided by Art 13 (2) of the ePrivacy Directive) has not been implemented in Hungarian law. Accordingly, if a merchant obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, then this merchant may not target the relevant customers with direct marketing communications, unless the customer consented to such communications.
- Withdrawal: Under the Advertising Act, the natural person recipient of the marketing message must be able to withdraw his/her consent/unsubscribe from such communications without any restrictions, free of charge and without providing any explanation.
- Record-Keeping Obligations: The Advertising Act states that the advertiser must maintain a record of the personal data of individuals who provided opt-in consent to direct marketing communications. The data contained in these records – relating to the person to whom the advertisement is addressed – may be processed only for the purpose defined in the statement of consent, until withdrawn, and may be disclosed to third persons only with the explicit consent of the data subject.
- Disclosure requirements: Under the Advertising Act, the body of the marketing message must clearly and visibly disclose the opt-out instructions along with an electronic and a postal address to which opt-out requests may be sent. Also, pursuant to the E-Commerce Act, the following disclosure requirements apply with regard to electronic marketing messages:
  (a) The message must clearly reflect the commercial/marketing nature of the message as soon as it is accessible to the data subject. (Practically, the email header must transparently reflect that the email is an ad).
  (b) The sender must be clearly identifiable.
  (c) Promotional offers, such as discounts, premiums and gifts, must be clearly identifiable as such, including the conditions which must be met to qualify for them.
  (d) Promotional competitions or games must be clearly identifiable as such, including the conditions for participation. The electronic message must also include a link to the conditions of the relevant offers and games.

4.3 Employment Privacy Law

Employment Privacy

The Act I of 2012 on the Labour Code lays down the general rules governing workplace privacy under its Sections 9 to 11, and these lay down the following conditions for the processing of employee data:

- Data Collection Limitation: Employers can only request data from employees that is essential for the establishment, fulfilment, or termination of the employment relationship, or for the enforcement of claims arising from the Labour Code. The data requested from the employee must be directly related to these specific purposes and the employer can only collect the relevant and necessary information.
- Privacy Rights Limitation: An employee's privacy rights can be limited only if it is strictly necessary for reasons directly related to the purpose of the employment relationship and

if the limitation is proportional to the objective pursued.
- Surveillance and Monitoring Restrictions: Monitoring of employees is permissible only in relation to work-related activities. The methods used must respect human dignity (no harassment, intimidation, or disturbance), be limited in time and space, and conducted only by authorised personnel. Personal life and private correspondence shall be excluded from such monitoring.
- Transparency and Information Duty: The employer must inform the employees in advance about the nature, conditions, and expected duration of any limitations on their privacy rights. Employers must provide written notification about data processing activities and the use of technical monitoring tools.
- Processing of Documents: The employer can only ask for the presentation of documents (identification cards, certificates, diplomas, etc) from the employee, but copying is restricted unless legally permitted.
- Biometric Access Control Measures: Biometric identification measures can be used to prevent unauthorised access to sensitive information or assets, considering the potential serious or irreversible consequences.
- Processing of Criminal Data: Employers may process criminal personal data of job applicants and employees for vetting purposes, particularly to protect financial interests, safeguard information protected by law, or in relation to the handling of hazardous materials.
- Prohibition of Private Use of Company IT Equipment: The Labour Code restricts private use of company IT equipment, unless explicitly agreed otherwise between employer and employee.
- Consultation Requirement: Consultation with the works council is required for implementing any measures and internal regulations affecting large number of employees; this information obligation covers the processing and protection of personal data of employees as well as the use of technical measures used for employee monitoring.

Employee Whistle-Blowing

The Hungarian Act No XXV of 2023, known as the Complaints Act, aligns with the EU Directive 2019/1937 to govern employee whistle-blowing. It requires employers with 50 or more employees, including certain sectors like financial services, banks, and airlines, to implement an internal whistle-blowing system. The Act covers a wide range of reportable issues, such as illegal activities or suspected illegalities, and includes the ambiguous category of “other abuses”, which it does not specifically define. While anonymous reporting is allowed, investigations for such reports are not legally mandated. The Act sets procedural deadlines, obliging employers to acknowledge reports within seven days and complete investigations within three months. It also restricts smaller employers, those with 50 to 249 employees, from forming joint internal whistle-blowing systems with other employers.

4.4 Transfer of Personal Data in Asset Deals

In Hungary, there is a limited amount of specific case law directly addressing due diligence processes. Data protection-related due diligence in corporate transactions requires strict compliance with the GDPR and local legislation. This process includes verifying the lawful processing of personal data, closely examining data handling practices, especially for sensitive information, and ensuring compliance with data subjects’ rights. Under NAIH case law, legitimate interest is generally accepted as a legal basis for the transfer or disclosure of client personal data in asset transfer transactions, provided that

such data transfer is ancillary to the asset transfer itself. In addition, the merging of databases between the target and the acquirer in a transaction may require a DPIA.

5. International Considerations

5.1 Restrictions on International Data Transfers

In Hungary, international data transfers of personal data are primarily regulated under the GDPR. The GDPR imposes specific restrictions and requirements on the transfer of personal data outside the European Economic Area (EEA) to ensure that the level of data protection afforded within the EEA is not undermined. When using adequacy measures, such as standard contractual clauses (SCCs) or binding corporate rules (BCRs), organisations are required to conduct a Transfer Impact Assessment (TIA) to evaluate the level of data protection in the recipient country, especially considering the recent Schrems II judgment of the CJEU. This assessment should consider the laws and practices of the third country, particularly those that may impact the effectiveness of the chosen transfer mechanism.

Regarding the mechanisms or derogations that apply to international data transfers, the key restrictions and requirements are outlined below:

- Adequacy Decisions: Personal data can be freely transferred to countries outside the EEA that have been deemed by decision of the European Commission to provide an adequate level of data protection. These adequacy decisions are based on a comprehensive assessment of the data protection framework and practices in the non-EEA country.
- Appropriate Safeguards: In the absence of an adequacy decision, transfers are permitted if appropriate safeguards are in place. These safeguards may include tools such as SCCs, BCRs, or specific conditions met under Article 46 of the GDPR.
- Derogations: The GDPR also allows for data transfers in certain specific situations under Article 49, such as when the data subject has explicitly consented to the proposed transfer after being informed of the possible risks, or for the performance of a contract between the data subject and the data controller, or for important reasons of public interest.

Data controllers are required to document these assessments and decisions as part of their accountability obligations under the GDPR. They may also need to consult with or obtain authorisation from the NAIH in certain cases.

5.2 Government Notifications and Approvals

Transfers of personal data within the EEA and to adequate countries are generally permitted and no government notifications or approvals are required. Under the GDPR, certain adequacy measures (such as approval of ad-hoc contractual clauses) will require authorisation from the NAIH or the derogation under the “compelling legitimate interests” legal basis of Article 49(1)(2) of the GDPR requires notification of the data transfer.

The Genetic Data Act requires data exporters to notify the Chief Public Health Officer of Hungary in connection with the international transfer of genetic data and genetic samples for the purpose of human genetic research or human genetic testing, and the relevant notification must also indicate a reference to the appropriate adequacy safeguards provided by the data exporter and the data importer.

5.3 Data Localisation Requirements

Data localisation and residency requirements in Hungary are governed by Act LXIX of 2024 on Hungary's Cybersecurity. These requirements apply to administrative bodies, state-owned enterprises, and entities designated as essential or important. Such organisations must conduct a data classification process in accordance with Annex I of Government Decree 418/2024 (XII. 23.). Depending on their criticality, certain data classes may only be stored within the territory of the EU or specifically within Hungary. Furthermore, under Act XCI of 2021 on National Data Assets, more stringent rules have been established for the handling of state databases belonging to national data assets, including criminal records, land registry records, company registry records, and ID records. This law stipulates that data processing activities may only be performed within the territory of Hungary.

5.4 Blocking Statutes

Article 48 GDPR provides that: "Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter". The request of a foreign government for access to personal data does not automatically establish a legal ground under the GDPR. When a foreign government requests access to personal data held by an organisation, the organisation must carefully assess the request considering its legal obligations. This assessment includes considering any applicable data protection laws, international treaties, and the legal basis for processing and transferring such data.

5.5 Recent Developments

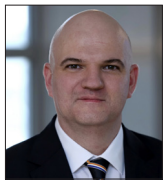
The NAIH emphasises concerns regarding data sovereignty and national security risks associated with the international transfer of personal data. This issue has been brought into focus due to political parties storing Hungarian citizens' personal data abroad without sufficient justification. NAIH president, Attila Péterfalvi, has publicly stated that the authority will continue to prioritise investigations into improper data processing practices by political organisations to safeguard individuals' rights. This stance emerged following complaints received by the NAIH during the 2022 election campaign, where 112 Hungarian voters reported the unauthorised use of their personal data. The investigation highlighted the complexities of enforcing data protection standards when processing is carried out by third-country service providers. Transparency and accountability were found to be compromised due to convoluted contracting chains. The President underlined the risks of storing and processing large volumes of sensitive data, such as political opinions, in jurisdictions outside Hungary. He emphasised that such data should ideally be processed domestically to ensure compliance with national and EU data protection laws. Moreover, the NAIH president warned that controllers cannot circumvent their responsibilities through contractual arrangements, stressing that accountability under the GDPR remains with the data controller regardless of where processing occurs. He urged political parties and organisations to strictly adhere to data protection regulations, ensuring clear accountability and transparency in their practices. The NAIH's position highlights the need for robust safeguards, local processing where possible, and a commitment to upholding GDPR principles to mitigate risks associated with international data transfers.

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 LLM 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

1053 Budapest
Károlyi utca 9
CENTRAL PALACE
5th floor

Tel: +36 70 605 1000
Email: info@provaris.hu
Web: www.provaris.hu

Data Protection Enforcement Trends in Hungary

Current Hungarian data protection enforcement trends are related to regulating emerging technologies like Artificial Intelligence (AI) and other classical areas such as direct marketing, workplace privacy CCTV surveillance, cookie management and data subject rights as articulated regularly by the Hungarian Data Protection and Freedom of Information Authority (NAIH). Furthermore, the Hungarian Competition Authority (HCA) has recognised in its practice that data protection forms an integral part of "consumer welfare" because consumers consider the privacy aspects of online products as a significant product characteristic. On this basis, the HCA adopted a policy to intervene and enforce unfair competition rules where data protection violations constitute an unfair commercial practice against consumers. This is particularly important regarding ongoing enforcement actions regarding the use of AI and machine learning technologies.

These enforcement trends align with broader EU and Hungarian regulatory activities focusing on the appropriate purpose and legal basis for data processing, adherence to the principles of purpose limitation and data minimisation, and the importance of transparent communication with data subjects regarding their rights and the processing of their data.

Continuing Surge of AI Use and Implementation

The anticipated surge in AI adoption is expected to continue in Hungary, with numerous businesses integrating Large Language Model (LLM)-based AI solutions to enhance efficiency in everyday operations. Such solutions are readily available from big-tech service providers and may be integrated into existing processes. GenAI use is generally twofold: intra-company employee use and the implementation of "off-the-shelf" GenAI services. To address unsolicited employee use and the related information security risks of confidentiality breaches, companies tend to prohibit access to public, open services by both implementing organisational (ie, introducing acceptable AI use policies) and technical controls (ie, firewall rules to block access to public services). AI's integration also poses a risk to market fairness, as it is currently a resource-heavy and innovative field dominated by large tech companies. These companies' access to extensive resources and advanced technology allows them to gain a significant competitive advantage. This could lead to market domina-

tion by a few industry giants, potentially disrupting competition in digital markets. Moreover, the rise of AI technologies increases consumer vulnerabilities, particularly in data collection and advertising. With AI, companies can more effectively gather and use consumer data, applying strategies like "dark patterns" and tailored advertising. This is especially concerning in scenarios like chatbot interactions, where consumers might not discern if the information provided is reliable or influenced by sponsored content. These developments highlight the need for careful consideration of AI's broader implications on market dynamics and consumer protection.

In 2023, the HCA launched proceedings against Microsoft for allegedly failing to adequately inform users about certain features of its search engine with artificial intelligence chat.

The HCA conducted a market analysis, which started in the beginning of 2024 and was released on 21 October 2024. It aimed to determine whether the rapid growth of AI technologies could distort market competition across various sectors and increase consumer vulnerability, and also sought to explore the broader implications of AI adoption, focusing on the banking and telecommunications sectors, and potential data protection challenges associated with their rapid development and integration into various sectors.

The analysis highlighted that AI technologies can increase consumer vulnerability due to their ability to collect and process vast amounts of data, which can be exploited for purposes like highly personalised advertising or the use of manipulative design strategies often referred to as dark patterns. Consumers may also be subjected to AI-driven systems such as chatbots without clear indications about whether the responses they receive are unbiased or influenced by commercial interests. The study underscores the critical importance of transparency in AI systems, emphasising that businesses leveraging AI technologies should provide clear and accessible information to consumers about the use of such systems, including their data sources, processing methods, and any inherent risks or limitations.

This lack of transparency poses significant data protection concerns, particularly under the framework of the GDPR, which mandates accountability and informed consent when handling personal data. The analysis also delves into the global nature of AI technology, noting that key resources necessary for AI development, such as vast datasets, computational power, and skilled expertise, are predominantly controlled by major international technology companies, often referred to as big tech, such as Google, Meta, Microsoft, and Amazon. This creates a concentration of power in these entities, which has implications not only for competition but also for data protection since these companies operate on a global scale without necessarily tailoring their products to the unique linguistic or cultural needs of smaller markets like Hungary.

The HCA pointed out that the lack of AI systems specifically developed for smaller languages like Hungarian has profound implications for data sovereignty, cultural identity, and the ability to maintain secure and localised data practices. While international companies provide standardised products and services globally, their lack of tailored solutions leaves smaller markets at a disadvantage in terms of leveraging AI for localised needs. The report further identified a disparity in AI adoption between larger corporations and small and medium-sized enterprises (SMEs) in Hungary, with the latter lagging due

to limited awareness, a shortage of specialised expertise, and financial constraints. While larger firms are more likely to integrate AI technologies into their operations, SMEs often restrict their use of AI to non-critical applications such as chatbots or fraud prevention tools. The slow adoption among SMEs could widen the gap in competitiveness as larger firms continue to invest in and benefit from AI technologies.

The analysis emphasises that while AI has the potential to significantly boost efficiency, competitiveness, and even GDP, the failure to address the challenges related to its adoption and regulation could exacerbate inequalities and lead to long-term disadvantages for smaller enterprises. The HCA therefore recommended targeted interventions to address these challenges, including support for local AI training and development programmes that emphasise compliance with data protection laws and the inclusion of smaller languages in AI systems. It also suggested that regulators should maintain constant oversight of the evolving AI landscape to ensure that its deployment aligns with principles of fairness, transparency, and accountability, as required under the GDPR. The study concludes that a strategic approach to AI development and adoption is essential to mitigate data protection risks, preserve cultural and linguistic identity, and foster equitable economic growth.

Artificial Intelligence and Data Protection

The NAIH has also displayed a marked focus on the regulation of AI as a high-risk data processing activity, particularly considering evolving technologies and their implications for the rights of data subjects. The NAIH's approach, especially in the context of the use of machine learning (ML) technologies and AI, emphasises GDPR compliance, underscoring the need for a balance between technological advancements and the protection of fundamental rights of data subjects and transparency of the related data processing activity.

A key case highlighting this concern involved one of the largest Hungarian banks, where the NAIH imposed a fine of approximately EUR650,000 for using emotion analysis software in customer care. This decision was later upheld by the court, reinforcing the authority's position on the importance of GDPR compliance in AI applications, especially in automated decision-making and profiling. In this instance, the bank employed AI technology for applying sentiment analysis on every incoming phone calls, which the NAIH found disproportionate in terms of the risks posed to data subjects' fundamental rights. The NAIH highlighted that the bank did not provide any information about the application of this technology and therefore data subjects were deprived of their respective data subject rights.

This decision highlights the NAIH's stringent stance on ensuring that AI and ML applications, especially those involving automated decision-making and profiling, comply with GDPR principles. It also underscores the necessity for data controllers to conduct thorough data protection impact assessments and balancing test assessments when implementing AI solutions.

Furthermore, the NAIH's ongoing investigation into ChatGPT, in co-ordination with other EU supervisory authorities, due to OpenAI not having an EU establishment at the launch of the procedure, reflects its proactive approach in addressing potential risks associated with new and emerging technologies.

Customer Satisfaction Surveys

The NAIH has reviewed the data processing practices of a parcel delivery company regard-

ing a customer satisfaction survey, where the survey invitation was included in delivery status update messages. The NAIH found the practice lawful and determined that the data processing was compatible with the performance of the contract, eliminating the need for a separate legal basis. The NAIH specified that the customer's name and email address were lawfully processed for purposes necessary for contract performance and that the processing was not based on consent or EU/member state law, as these would preclude the application of the compatibility test under Article 6(4) of the GDPR. It emphasised the need to document the compatibility test, including an analysis of the relationship between the original and new purposes, the circumstances of data collection, whether special categories of data are involved, and the potential consequences of further processing. The NAIH concluded that the status updates and customer satisfaction survey were intrinsically linked to the service, its performance, and evaluation as part of the delivery service process and did not infringe on the privacy of data subjects, as the survey invitation was included in an email about the successful delivery, which recipients could choose to disregard. Adopting a business-friendly approach, the NAIH limited the scope of customer satisfaction measurement to contract-based grounds and noted that data subjects had no right to object to this type of data processing.

Marketing Consent Validity

Regarding consent validity, the NAIH stringently requires that consent be articulated clearly. For example, the NAIH does not accept vague consent terms that refer broadly to data processing goals such as "electronic communications", which could imply various forms of digital communication that a data subject might not foresee or agree to. Furthermore, the NAIH has highlighted the lack of an option for separate consents for email messaging or data processing associated with targeted online advertisements by entities like Google and Facebook. The NAIH recognises these as distinct activities impacting data subjects' privacy differently. However, the NAIH has not analysed in detail the transparency and data protection issues related to Google, Facebook, and similar mass automated advertising systems, as these are examined by other supervisory authorities within the EU. The absence of clear information about the use of such services, which are complex and challenging to comprehend, may itself present significant issues regarding consent validity, as per the NAIH's perspective.

Transparency Issues

The NAIH follows a strict practice regarding transparency requirements, and regularly emphasises the need for clarity in privacy notices, insisting that they should not just list data processing purposes and legal bases, but also data retention and other relevant information in line with respective data processing activities in an easy-to-comprehend manner. This approach is in line with Articles 12(1) and 13(1) of the GDPR, which mandate clear and transparent communication about data processing activities. NAIH highlights that a detailed specification of the types of data processed, the legal provisions underpinning this processing, and the duration is crucial, especially for processing based on legal obligations. Furthermore, the NAIH criticises practices where there is a mix of service provision and legal obligation without clear differentiation, as this complicates the exercise of data subject rights. The NAIH also pointed out in its practice that optional website registration, purely for user convenience, does not constitute a necessary step for contract performance or pre-contractual measures under the GDPR and

therefore requires a different legal basis, such as the user's consent.

In 2024, the NAIH fined a bank approximately EUR145,000 for deficiencies in the camera warning signs in the lobby of a branch office. The NAIH highlighted that camera warning signs must be detailed and placed at the entrance, with references to detailed privacy information, and that a simple pictogram is insufficient. Detailed notices must not be placed where access is limited outside business hours and should also be available online. A single data subject's complaint led to an investigation of the transparency practices concerning all branches. The unlawful practice persisted for one-and-a-half years, which was considered an aggravating factor, but the bank's prompt correction of the issue was treated as a mitigating circumstance. A three-day delay in responding to the data subject's request was noted but did not result in a fine.

ePrivacy – Cookies Use, Notice and Consent Requirements

In a landmark decision, the NAIH fined a major Hungarian media service provider approximately EUR 25,000 for failing to comply with GDPR principles in its cookie management. This decision marked the first time the NAIH imposed a fine for cookie management issues and made it public. The NAIH's decision was based on several critical findings regarding cookie management practices. The authority determined that cookies and cookie identifiers used on websites constitute the processing of personal data. As a result, website operators, in their role as data controllers, bear the responsibility for the modules they use on their websites, the third parties they share data with, and the legal basis they rely upon for data processing. This requires clear, transparent communication about the specific purposes and legal grounds for data processing. A key issue identified by the NAIH was the design of the cookie banner. The NAIH found that the banner used by the service provider was overly complex and displayed too much information in a limited screen space. Furthermore, the process to reject all cookies was made more difficult than accepting them, with the "Reject All" option being less accessible than the "Accept All" option. The NAIH emphasised that withdrawing consent should be as easy as giving it, a principle not upheld in this case. The NAIH also criticised the misuse of the term "legitimate interest" and the lack of clarity in communicating the processing purposes for cookies based on consent versus those based on legitimate interest. The data controller's argument that it had based its cookie management solution on the IAB Europe's Transparency and Consent Framework was rejected by the NAIH. The NAIH referred to a Belgian DPA decision, which had found IAB Europe's framework illegal, and applied the same reasoning to this case. This decision is a clear message to businesses about the importance of GDPR compliance in cookie management and the potential risks of relying solely on third-party solutions for compliance. It signals a stricter enforcement regime for cookie consent management, implying that businesses can no longer claim the widespread nature of such infringements as a defence.

Data Subject Rights Management

The NAIH places a strong emphasis on the management of data subject rights, particularly in ensuring timely responses to data subject requests and the careful evaluation of data subject access rights. This focus is essential for ensuring that data subjects' rights under the GDPR are respected and fulfilled. The NAIH confirmed that data subjects may only have access to copies of their personal data, and the scope of such requests does not cover technical corre-

spondence. Accordingly, in response to a DSAR, the data controller does not need to provide information on facts and documents not related to the related data processing activity, including internal policy document copies, information on the company structure/organisation, internal procedures and copies of documents that cannot be entirely considered as the personal data of the data subject, such as email correspondence with technical details on the handling of a complaint. A data controller can lawfully reject a request for copies of internal documents and correspondence on the basis that such internal documents and correspondence do not contain the data subject's personal data. In this case, there is no need for the controller to prove that the provision of a copy will not adversely affect the rights and freedoms of others.

CCTV Use and Household Exemption

The use of CCTV surveillance remained one of the enforcement priorities of the NAIH in 2024. The NAIH issued a decision addressing the legality of surveillance camera usage on private property. The investigation was initiated following neighbours' complaints that the property owner's security cameras were monitoring shared land and public areas. Upon inspection, the NAIH confirmed that the cameras' fields of view did indeed capture these areas, and although digital masking was employed to obscure parts of the footage, some portions beyond the owner's private property remained under surveillance. The NAIH emphasised that the GDPR does not apply to personal data processing conducted by a natural person purely for personal or household activities, provided there is no connection to professional or commercial activities. This is commonly referred to as household data processing, which falls outside the GDPR's scope. However, the NAIH clarified that the use of surveillance systems qualifies as household data processing only if (i) the monitoring is confined to the boundaries of the private property, or (ii) exceptionally and minimally extends to the immediate vicinity of the property when such coverage is essential for effective protection.

The NAIH further stated that if surveillance extends beyond private property, it must be ensured through appropriate organisational and technical measures – such as digital masking – that the monitoring does not cover public areas or property owned by others. Failure to implement such measures means the data processing falls under the GDPR's scope of applicability, thereby establishing a need for a lawful basis for processing. In this particular case, the NAIH determined that the property owner's surveillance practices were unlawful due to inadequate masking, resulting in the monitoring of areas beyond their private property without a valid legal basis. This decision underscores the importance of ensuring that surveillance systems on private property are configured to avoid capturing images beyond one's own premises unless strictly necessary for security purposes, and even then, only with proper safeguards to protect the privacy of others.

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