Chambers
Global Practice
Guides

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

Data Protection & Privacy 2022

Sweden: Law & Practice
Henrik Nilsson, Johan Grenefalk,
Carl Gleisner and Annastasios Martidis
Wesslau Söderqvist Advokatbyrå

practiceguides.chambers.com

SWEDEN

Law and Practice

Contributed by:
Henrik Nilsson, Johan Grenefalk, Carl Gleisner and Annastasios Martidis
Wesslau Söderqvist Advokatbyrå see p.21

CONTENTS

Contributed by: *Henrik Nilsson, Johan Grenefalk, Carl Gleisner and Annastasios Martidis,*
Wesslau Söderqvist Advokatbyrå

1. BASIC NATIONAL REGIME

1.1 Laws

Key Legislation

Sweden belongs to the civil law tradition, which – in contrast to common law – is codified. The primary constitutional law is The Instrument of Government (1974:152), which contains a guarantee that everyone shall be protected in their relations with government institutions against significant invasions of their personal privacy, if these occur without their consent and involve the surveillance or systematic monitoring of the individual's personal circumstances.

The central piece of legislation for the protection of personal data since 25 May 2018 has been the Regulation (EU) 2016/679 (the General Data Protection Regulation or GDPR). On the same date, the Act (2018:218) with supplementary provisions to the EU Data Protection Regulation (the Data Protection Act, hereinafter the DPA), supplemented by an Ordinance (2018:219) (Data Protection Ordinance), came into force. During 2021, the DPA was amended to reflect new laws on the processing of personal data by the Swedish Armed Forces, the National Defence Radio Establishment and the security services.

EU and Swedish law use the term "personal data". Personal data is defined by the GDPR as "any information relating to an identified or identifiable natural person".

A great many further acts and ordinances contain regulations regarding personal data registries and other processing of personal data. This body of law is known, collectively, as the Registry Acts. The Registry Acts cover areas such as law enforcement, financial activities, healthcare and much more. There is no authoritative list of the Registry Acts. Relevant legislation outside of the Registry Acts includes the Camera Surveillance Act (2018:1200) and the Electronic Communications Act (2003:389) (due to be fundamentally updated on 1 June 2022, implementing the European Electronic Communications Code Directive (EU) 2018/1972).

The text of the European Convention on Human Rights has been incorporated into law in the ECHR Act (1994:1219).

The European Commission has tabled a proposal for an Artificial Intelligence Act (COM(2021/0106 (COD)), which at this time (February 2022) is the subject of discussion in the EU Parliament. The Swedish government presented an AI Strategy in 2018, which did not contain any legislative proposals. The view of the government was that such regulation is best formulated at the EU level.

Enforcement

Chapter 8 of the GDPR regulates remedies, liability and penalties with regard to data protection. Article 58 of the GDPR grants many varied powers to the relevant national data protection authority. The DPA explicitly authorises the Swedish data protection authority (*Integritetsskyddsmyndigheten*, or IMY) to exercise the powers set out in Article 58.1–58.3. The IMY is restricted under the DPA to imposing administrative sanctions for breaches of the GDPR as listed in Article 83, and also breaches of Article 10. The IMY is authorised to decide administrative sanctions against public authorities should one come to breach the GDPR.

The penalty fee for a public authority shall be determined up to a maximum of SEK5 million in the case of infringements referred to in Article 83(4) of the EU Data Protection Regulation, and up to a maximum of SEK10 million in the case of infringements referred to in Articles 83.5 and 83.6 of the Regulation. Breaches of the GDPR or the DPA cannot lead to criminal penalties in

Sweden, with the exception of a breach of secrecy or confidentiality by a data protection officer concerning the performance of their tasks.

Under the Swedish Criminal Code (Chapter 4, Section 9C), a person who unlawfully obtains access to information intended for automatic processing, or unlawfully alters, erases, blocks or, in a register, inserts such information, is guilty of breach of data security and is sentenced to a fine or imprisonment for at most two years. The same applies to a person who seriously disturbs or impedes the use of such information in an unlawful way through some other, similar measure. If the offence is gross, the person is guilty of gross breach of data security and is sentenced to imprisonment for at least six months and at most six years. When assessing whether the offence is gross, particular consideration is given to whether the act caused serious damage, or related to a large quantity of information, or was otherwise of a particularly dangerous nature.

1.2 Regulators

The supervisory authority regarding data protection is the IMY. The mission of the IMY is, according to the Ordinance (2007:975) instructing the IMY, "to work to ensure that fundamental human rights are protected in connection with the processing of personal data, to facilitate the free flow of personal data within the European Union and to ensure that good practices are observed in credit and debt collection operations".

The IMY is a public authority reporting to the Ministry of Justice. It has long been a comparatively small organisation, comprising 91 employees at the end of 2020 with an operating budget for 2022 of approximately SEK124.8 million. The IMY is also the supervisory authority for the Debt Recovery Act of 1974 (1974:182), the Credit Information Act of 1973 (1973:1173) and the Camera Surveillance Act of 2018 (2018:1200).

The IMY may initiate investigations as a result of complaints filed with the authority or widely reported allegations of infringement. It also conducts annual supervisory audits of different sectors of society according to a supervisory plan that is revised annually. The IMY's Annual Report for 2020 relates that the IMY initiated 52 new ongoing inspection matters during 2020 concerning the GDPR. The IMY issued administrative fines during 2020 at a combined amount of SEK 150 million. The IMY Annual Report for 2021 was published in mid-February 2022.

The IMY has the power to request access to personal data that is being processed by someone in its jurisdiction, including access to the premises of the processing. It may request information and documentation regarding the processing and regarding any security measures applied to that processing. The IMY may order that certain security measures shall be applied to the processing, and may prohibit a controller from processing personal data in any other manner than by storing it.

1.3 Administration and Enforcement Process

The administrative process before the IMY is governed by the Data Protection Act and the general provisions of The Administrative Procedure Act (2017:900). Decisions regarding orders or sanctions can, in accordance with the IMY's internal procedural rules, be taken by the case officer in charge, the head of department or by the director-general, depending on the gravity or importance of the decision. There is no requirement to submit a draft decision to the receiving party for comment prior to adopting it, but this has been known to happen in a small number of cases. Administrative fines may not be imposed unless the respondent has been given an opportunity to file its opposition within five years of the alleged breach.

The IMY's decisions, according to the GDPR and national provisions for administrative fees, may be appealed to the Administrative Court. The process before the Administrative Court is almost exclusively a written procedure. The Administrative Court's decision may also be appealed to The Administrative Court of Appeal, but this requires a review permit.

Sweden applies the principles of free sifting of evidence and free assessment of evidence. The administrative process is generally less stringent and typically adapted to the type of matter, as opposed to the legal standards applied in general court proceedings. As a general rule however, in matters regarding administrative fees, the IMY and the courts will apply the legal standard of "proven" (*styrkt*).

1.4 Multilateral and Subnational Issues

Processing of personal data is primarily regulated through the GDPR, which belongs to the supranational authority of the European Union (see **1.1 Laws**). The GDPR is immediately applicable before Swedish courts upon being promulgated by the EU legislature without any further adoptions or procedures.

Sweden is a signatory to the European Convention on Human Rights (ECHR). As set out in **1.1 Laws**, the ECHR has been incorporated into national legislation through the ECHR Act and may be invoked directly before Swedish courts.

The legislature has given the government the authority to issue ordinances supplementing the national law supplementing the GDPR. Under this ordinance, the government has given the IMY the competence to issue regulations. With this competence, the IMY has issued a Regulation regarding the processing of personal data having to do with criminal offences (DIFS 2018:2).

1.5 Major NGOs and Self-Regulatory Organisations

The GDPR gives data subjects the right to mandate certain kinds of duly constituted not-for-profit organisations to lodge complaints on their behalf. Furthermore, data subjects may also mandate such not-for-profit organisations to receive compensation on their behalf. While the GDPR authorises member states to adopt legislation that allows not-for-profit organisations to act without the data subjects' mandate, Sweden has elected not to adopt such legislation.

The IMY has, so far, not published any approved codes of conduct pursuant to Article 40 of the GDPR. However, the IMY did approve several codes of conduct under the previous Data Protection Act for sectors such as municipalities and landlords. To the extent such codes have not been superseded, they may at least serve to provide guidance in their respective sectors.

Given the strict nature and general applicability of the GDPR, industry self-regulatory organisations do not play a decisive role in Sweden.

1.6 System Characteristics

The rules on data protection in Sweden follow the EU omnibus model and primarily consist of directly applicable EU legislation and are highly developed. The IMY, and its predecessor, have traditionally not demonstrated an aggressive approach to enforcement of data protection laws. As in most EU member states, however, the adoption of the GDPR created expectations that enforcement activities would become more aggressive. The investigative activities of the IMY have increased, but, as of February 2022, have not risen to the aggressive level initially expected.

1.7 Key Developments

The IMY, on 10 February 2021, imposed an administrative fine of SEK2.5 million (approxi-

mately EUR240,000) on the Swedish Police Authority for processing personal data in breach of the Criminal Data Act. Several officers attached to a specialised unit had used the facial recognition platform Clearview AI in the course of their duties, without having acquired the platform through the Authority's regular procurement process. The IMY found that the Police Authority had processed biometric data without it being absolutely necessary and done this in breach of the Criminal Data Act. The ruling was upheld by the Administrative Court, and is now being reviewed by the Administrative Court of Appeals.

The IMY, on 7 June 2021, imposed an administrative fine of SEK12 million on Medhelp AB, SEK600,000 on Voice Integrate Nordic AB and an aggregated SEK1 million on three regional public health care authorities. Recorded calls from the general public to the national public health care information and management service – 1177 Vårdguiden – were found to have been stored on web servers accessible over the internet without password protection or other adequate security. These rulings imposing sanctions have been appealed to the Administrative Court.

The IMY, on 21 June 2021, imposed an administrative fine of SEK16 million on the Stockholm region public transport authority, SL, for use of bodycams on roving ticket control personnel under circumstances in breach of the GDPR. The sanctions decision has been appealed to the Administrative Court.

The IMY, in November 2020, initiated an investigation of six large data controllers' transfers of personal data to third countries following the CJEU's judgment in Schrems II (ECJ C-311/18). All of the six inquiries concern complaints filed by the interest group None of Your Business (NOYB). The transfers under investigation concern transfers to the USA related to the use of Google Analytics. The inquiries remain ongoing.

The IMY has since launched investigations – in June 2021 – against financial services provider Avanza and the insurance company Länsförsäkringar, following personal data breach notifications from these companies that significant amounts of personal data had inadvertently been shared with Facebook for a longer period of time. These investigations remain ongoing.

1.8 Significant Pending Changes, Hot Topics and Issues

Public authorities' use of cloud services for storing information that is classified as secret under the Public Access to Information and Secrecy Act (2009:400) continues to be a hot topic in Swedish data protection circles. While the Act only applies to Swedish authorities and certain public entities, service providers to such authorities and entities may be indirectly affected through missed business opportunities. This topic is also related to the transfer of personal data to third countries under the mechanisms provided for by the GDPR (see **4. International Considerations**).

2. FUNDAMENTAL LAWS

2.1 Omnibus Laws and General Requirements

Under the GDPR, personal data may only be processed if a legal basis set out in Article 6 applies. The Data Protection Act (DPA) specifies that the GDPR does not apply if it contravenes the constitutional Freedom of the Press Act and the Fundamental Law on Freedom of Expression.

The DPA applies to those controllers of personal data that are established in Sweden. The DPA also applies to the processing of personal data

performed by controllers or processors established only in countries outside the EU/EEA, if the processing concerns data subjects located in Sweden and is related to the offering of goods or services to those data subjects, or the monitoring of their behaviour in Sweden.

The GDPR applies to the processing of personal data wholly or partly undertaken by automated means and to the processing, other than by automated means, of personal data which forms part of a filing system or is intended to form part of a filing system.

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a data controller or data processor within the EU, regardless of whether the processing take place within the EU or not.

Data Protection Officers

In accordance with Article 37 of the GDPR, controllers and processors are required to appoint a data protection officer (DPO) where the processing is carried out by a public authority or other public body, or where the core activities of the controller or the processor consist of processing operations which – by virtue of their nature, their scope or their purposes – require regular and systematic monitoring of data subjects on a large scale, or finally, where the core activities of the controller or the processor consist of large-scale processing of sensitive personal data as categorised in Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

The overall and most important task for the DPO is to ensure that the organisation complies with the DPA. This means, among other things, collecting information about how the organisation processes personal data, checking that the organisation complies with regulations and internal governing documents, and giving training and advice within the organisation. The DPO must also provide advice on impact assessments, be the contact person for the IMY, be the contact person for the data subjects and staff within the organisation and co-operate with the IMY during, for example, inspections.

While the GDPR elaborates on the position and tasks of the data protection officer, the only explicit legal responsibility is to maintain the confidentiality requirement set out in the DPA. The DPO has no personal responsibility for the organisation's compliance with the DPA. That responsibility always lies with the controller or with the data processor. The person responsible for personal data may not punish the DPO for having performed their duties.

There is an ongoing debate in Sweden as to whether, and under what circumstances, a DPO can incur personal liability for their actions in the role. The possibility of personal liability has not been authoritatively ruled out.

Lawful Basis and Fundamental Principles for Processing

Under the GDPR, personal data may be processed only if a legal basis set out in Article 6 applies.

The DPA specifies that the GDPR does not apply if it contravenes the constitutional Freedom of the Press Act and the Fundamental Law on Freedom of Expression.

Personal data may be processed on the basis of Article 6(1)(c) or (e) of the GDPR if the processing is necessary for the personal data controller to comply with a legal obligation arising from a law or other regulation, collective labour market agreements or decisions issued under a law or other regulation, or as part of the data protection officer's exercise of authority by a law or other constitution.

Personal data may also be processed on the basis of Article 6(1)(e) of the GDPR if the processing is necessary to perform a task of public interest arising from a law or other regulation, collective agreements or decisions issued pursuant to law or other constitution, or as part of the personal data officer's exercise of authority by a law or other regulation.

The GDPR makes a distinction for the processing of special categories of personal data, labelled sensitive data under the DPA.

Special categories of personal data include those that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Sensitive personal data in the field of employment and social security and social protection law may be processed pursuant to Article 9(2)(b) of the GDPR if the processing is necessary for the data controller or the registrant to fulfil their obligations and exercise their special rights in the field of labour law and in social security and social protection.

Personal data thus processed may be disclosed to third parties only if there is an obligation for the data controller to do so or, in the field of social security and social protection, where the data subject has explicitly agreed to the disclosure.

Processing by a public authority of sensitive personal data that is necessary for reasons of substantial public interest is permitted if the information has been submitted to the authority and the processing is required by law, where the processing is necessary for the handling of a case, or otherwise, if processing is necessary in view of an important public interest and does not constitute an improper infringement of the personal privacy of the data subject. Chapter 3 of the DPA elaborates the circumstances under which special categories of personal data may be processed.

Privacy by Design and Privacy by Default

The European Data Protection Board adopted Guidelines 4/2019 on Article 25 Data Protection by Design and by Default on 20 October 2020. There has been no Swedish national guidance at this point, though the IMY encourages the use of encryption for emails of any sensitivity.

Privacy Impact Analyses

Data controllers are required to perform privacy impact analyses where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons under Article 35 of the GDPR. This applies especially where the processing concerns a systematic and extensive evaluation of personal aspects to persons through automated decision-making rendering legal decisions, large-scale processing of sensitive data and large-scale monitoring of public places.

The IMY has published a list of occasions on which an impact assessment is required. No guidance has been published relating to possible fairness or legitimate impact analyses.

Privacy Policies

There is no explicit general national requirement, as such, to adopt internal or external privacy policies. The GDPR, however, integrates accountability as a principle which requires that organisations put in place appropriate technical and organisational measures and are able to demonstrate, on request, what they have done in this area and its effectiveness.

Contributed by: *Henrik Nilsson, Johan Grenefalk, Carl Gleisner and Annastasios Martidis,*
Wesslau Söderqvist Advokatbyrå

Data Subject Rights

Under Article 15 of the GDPR, the data subject has the right to obtain, from the controller, confirmation as to whether or not personal data concerning them is being processed, and, where this is the case, access to that personal data. The information shall be provided in writing or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. The information shall be provided without undue delay and, in any event, within one month of receipt of the request. This period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

While the information shall, as a general rule, under Article 12, be provided free of charge, where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may charge a reasonable fee taking into account the administrative costs of providing the information or refusing to act on the request.

Information does not need, under the DPA, to be provided with regard to personal data in running text that has not been given its final wording when the application was made or that comprises an aide memoire or similar. However, this does not apply if the data has been disclosed to a third party or if the data was only processed for historical, statistical or scientific purposes or, as regards running text that has not been given its final wording, if the data has been processed for a period longer than one year.

To the extent that it is specifically prescribed by a statute or other enactment, or by a decision that has been issued under an enactment that information may not be disclosed to the data subject, the right to information is curtailed. A controller of personal data that is not a public authority may, in a corresponding case as referred to in the Public Information and Secrecy Act (2009:400), refuse to provide information to the data subject.

Individuals have, under certain circumstances, under Articles 15 to 22 of the GDPR, the right to object, require rectification, blocking or erasing (as applicable) of personal data. The controller must also notify a third party to whom the data has been disclosed about the measure, unless it is shown to be impossible or would involve a disproportionate effort.

The data subject is entitled, at any time, to revoke consent that has been given in those cases where the processing of personal data is only permitted on the basis of consent.

Anonymisation, De-identification and Pseudonymisation

Under Article 25 of the GDPR, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects. Under Article 35 of the GDPR, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data where a type of processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons.

Automated Decision-Making

Data subjects are entitled to be informed of the occurrence of any automated decision-making.

As a general rule, data subjects have the right not to be subject to automated decision-making, including profiling, if this can have legal consequences. However, there are exceptions for when such actions are necessary for the performance of a contract, are allowed by EU or member state law or where the data subject has given their consent.

Injury or Harm

The concepts of "injury" and "harm" are relevant for data protection laws before Swedish courts in that the data subject should be put in the same position as though no violation of the GDPR had occurred. Due to the difficulties in proving to what extent harm or injury was suffered, Swedish courts have adopted standard amounts. This practice has previously been adopted for compensation for victims of crimes. In addition to compensating loss of income, bodily harm, hospital fees, etc, victims are also awarded standardised amounts for the violation in and of itself.

2.2 Sectoral and Special Issues

Some personal data is, by its nature, sensitive and hence needs stronger protection. Processing of sensitive personal data is forbidden but there are certain exceptions. Before processing sensitive personal data, data processors must fully understand what lawful grounds they have for that processing. Sensitive personal data is data about racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health, a person's sex life or sexual orientation, genetic data and biometric data used to uniquely identify a person.

Financial Data

Whether or not financial data is recognised as sensitive, depends on the view of the data subject. Financial data is, by its nature, commonly regarded as sensitive and hence in need of stronger protection. Processing of financial data is therefore forbidden, but there are certain exceptions.

Financial data may be processed by financial institutions that are under the supervision of the Swedish Financial Supervision Authority (SFSA), under the rule of lex specialis. Financial companies, under the supervision of the SFSA, have the right to process sensitive personal data since special laws take precedence over the GDPR. The personal data of management personnel and employees is processed in order to be able to find out if these persons are suitable to provide advice to other private individuals.

Health Data

Personal data concerning health includes all data concerning the health status of a data subject which reveals information relating to the past, current or future physical or mental health status of the data subject. This includes:

- information about the natural person collected in the course of the registration for, or the provision of, healthcare services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person;
- a number, symbol or particular assigned to a natural person to uniquely identify that natural person for health purposes;
- information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and
- any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

Contributed by: *Henrik Nilsson, Johan Grenefalk, Carl Gleisner and Annastasios Martidis,*
Wesslau Söderqvist Advokatbyrå

The National Board of Health and Welfare (*Socialstyrelsen*) has adopted Regulation HSLF-FS 2016:40 on keeping medical records and data protection in healthcare, together with extensive Guidelines to the Regulation.

Communications Data

Privacy in the sector of electronic communications is governed by the Electronic Communications Act (2003:389), or ECA, implementing the E-Privacy Directive 2002/58/EC. The ECA applies to processing data in connection with the provision of publicly available electronic communications services in public communications networks. Providers must safeguard the security of their services. Traffic data must only be processed for billing, marketing of services and administration by third parties. Traffic data must be erased when no longer needed. Contents of voice calls or messages must not be accessed or monitored. However, courts, law enforcement and service providers preventing network abuse may access traffic data or contents of calls or messages in certain cases and for specific purposes.

Children's Data

Children have a higher level of protection with regard to their personal data. Due to the fact that they are less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of the personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

Internet, Streaming and Video Issues

Cookies

Sweden passed the 2010 amendments to the EU electronic communications regulatory regime into law by an Act of the *Riksdag* on 17 May 2011. The new regulations came into force on 1 July 2011. Among the changes to the Electronic Communications Act (2003:389) was the updated "cookie regulation". The Act is due to be fundamentally updated on 1 June 2022, implementing the European Electronic Communications Code Directive (EU) 2018/1972.

Chapter 6, Section 18 of the Electronic Communications Act states that information may be stored in or retrieved from a subscriber's or user's terminal equipment only if subscribers or users are provided with access to information on the purpose of the processing and consent to the processing. This does not apply to the storage or retrieval necessary for the transmission of an electronic message over an electronic communications network, or for the provision of a service explicitly requested by the subscriber or user.

The preparatory work to the new legislation emphasises that internet users should not be inconvenienced through cumbersome routines relating to the use of legitimate tools such as cookies. This work suggests that consent to cookies may be expressed through web browser settings, but stops short of explicitly stating that browser settings are sufficient.

Guidance on cookies in the form of "soft law" was eventually published by the Swedish Post and Telecom Authority (PTS), together with the Agency for Digital Government (DIGG) in the form of a dedicated website. DIGG is responsible for the website as of 1 January 2019.

Cloud computing

The GDPR also applies to the use of cloud computing services; there is no regulation specific to such services. The IMY has issued guidance on the subject, a four-page pamphlet titled "Cloud services and the Personal Data Act" (also published in English). The guidance emphasises that whoever appoints a cloud provider is still a controller of personal data and that the controller must carry out a risk and impact assessment with regard to engaging the provider. The IMY reminds cloud service users that when processing sensitive personal data (eg, information about health), information about legal offences and secrecy-protected information, the IMY requires that strong authentication be used when transferring data in an open network and that the data shall be protected by encryption. When such information is processed, the requirement for access checks often means that the controller of personal data shall not only carry out checks for particular reasons but also regularly and systematically follow up who has had access to which information. The IMY also stresses the importance of entering into an adequate processor agreement that complies with DPA requirements. The IMY has previously raised objections to processor agreements used by Microsoft Azure and Google Apps services.

2.3 Online Marketing

The Marketing Act (2008:486) has regulations on marketing by email, fax or telephone.

Under the Marketing Act, a trader may, in the course of marketing to a natural person, use email, a telefax or automatic calling device or any other similar automatic system for individual communication that is not operated by an individual, only if the natural person has consented to this in advance.

Where a trader has obtained details of a natural person's email address in the context of a sale of a product to that person, the consent requirement shall not apply, provided that:

- the natural person has not objected to the use of the address for the purpose of marketing via email;
- the marketing relates to the trader's own similar products; and
- the natural person is clearly and explicitly given the opportunity to object, simply and without charge, to the use of such details for marketing purposes, when they are collected and in conjunction with each subsequent marketing communication.

In marketing via email, the communication shall, at all times, contain a valid address to which the recipient can send a request that the marketing cease. This also applies to marketing to a legal person.

A trader may use methods for individual distance communication other than those referred to above, unless the natural person has clearly objected to the use of such methods.

Behavioural or Targeted Advertising

All processing of personal data must, whether for marketing or any other purpose, comply with the basic principles of data prescribed in Article 5 of the GDPR.

Personal data processing, whether for marketing purposes or any other purpose, must comply with the legality requirement of Article 5.1 a of the GDPR. The principle of legality means that the processing must be based on the data subject's consent or any other legal basis listed in Article 6.1 of the GDPR.

The data processor is required to have the data subject's consent or some other legal basis for the processing of personal data to be permitted. Which means that at least one of the condi-

tions of Article 6.1 of the GDPR must be fulfilled. The processing of personal data for marketing purposes can therefore primarily be based on consent or the legitimate interest of the person responsible for personal data or a third party after a balance of interests.

Under Article 6.1 f of the GDPR, processing is permitted if it is necessary to satisfy a legitimate interest and the interests of the data subject do not take precedence. It is clear from the last sentence of recital 47 of the GDPR, that direct marketing is a typical example of such a legitimate interest.

The third sentence of recital 47 the GDPR states that a legitimate interest under the GDPR requires a careful assessment in each individual case. That includes the data subject's reasonable expectations.

The data subject must be considered to be sufficiently protected in a balance of interests (eg, through the rights in Article 21 – objection, Article 18 – restriction, and Article 17 – deletion, in the GDPR). According to the wording, the rules regarding balancing of interests also apply to the legitimate interests of a third party.

That profiling for marketing reasons must be based on a balance of interests is indirectly stated in Article 21 of the GDPR. However, the more intrusive the measure, the more difficult it becomes for data controllers to justify the processing on the basis of balancing interests.

2.4 Workplace Privacy

Employers must research and find legal grounds for the processing of personal data of their employees. For example, for the fulfilment of the employment agreement or compliance with legal obligations such as the need to submit information to the Tax Authority.

Laws and Considerations

Workplace privacy is not subject to any specific laws in Sweden. The processing of personal data in the workplace is governed by the general provisions of the GDPR.

Monitoring Workplace Considerations

Employers are typically interested in collecting information regarding their employees to monitor performance, presence, and compliance with policies, as well as to protect against corporate espionage and security. The GDPR generally allows for monitoring for such purposes where employers have a legitimate interest. However, employers must ensure that their legitimate interests are not overridden by the interests or fundamental rights of the employees.

Monitoring activities may include camera surveillance, reading employees' emails, reviewing logs, and implementing cybersecurity tools in equipment provided by the employer, etc.

Role of Labour Organisations

Swedish labour organisations enjoy a strong position in the workplace and the Swedish labour market is characterised by few labour disputes. Labour organisations therefore play an important role in asserting workers' rights in general. However, Swedish data protection legislation does not give labour organisations any formal role.

Whistle-Blower Hotlines and Anonymous Reporting

Sweden has a long tradition of whistle-blower protection for persons giving information to publishers who enjoy constitutional protection under the Freedom of The Press Act. Public officials who investigate the identities of sources may face criminal liability and imprisonment. Reprisals against public servants for their giving of information to protected publishers are also criminal offences.

However, whistle-blowers' protection against actions from public authorities is not absolute. The Freedom of The Press Act contains an exclusive catalogue of criminal offences for which whistle-blowers may be held liable. This catalogue includes unlawful threat, defamation, incitement, agitation against an ethical or national group, treason, espionage, incitement for war, unlawful possession of secret information. The Chancellor of Justice is the sole prosecutor for any acts committed where the Freedom of The Press Act applies.

On 17 December 2021, Sweden adopted the Act (2021:890) on Protection for Persons Who Report Grave Ills, implementing the EU Whistle-Blowing Directive (2019/1937).

E-discovery

Swedish procedural law typically does not include a discovery process. The Procedural Code provides means for litigants to request and obtain documents from the other party, or third parties, if said documents may be of evidentiary value. However, the duty of disclosure is typically not invoked in most proceedings.

2.5 Enforcement and Litigation

Legal Standards

Sweden applies the principles of free sifting of evidence and free assessment of evidence. IMY enforcement activities are governed by administrative law. Claims for damages are tried by general courts. The administrative process is generally less stringent and typically adapted to the type of matter, as opposed to the legal standards applied in general court proceedings.

Potential Penalties

The penalty fee for a public authority shall be determined up to a maximum of SEK5 million in the case of infringements referred to in Article 83(4) of the EU Data Protection Regulation, and up to a maximum of SEK10 million in the case of infringements referred to in Article 83.5 and 83.6 of the Regulation. Breaches of the GDPR or the DPA cannot lead to criminal penalties in Sweden, with the exception of a breach of secrecy or confidentiality of a data protection officer concerning the performance of their tasks.

Enforcement Cases and Major Cases

See **1.7 Key Developments** above.

3. LAW ENFORCEMENT AND NATIONAL SECURITY ACCESS AND SURVEILLANCE

3.1 Laws and Standards for Access to Data for Serious Crimes

The laws applicable to law enforcement access to data for serious crimes are the Code of Judicial Procedure (1942:740), the Act on Measures to Prevent Serious Crimes (2007:979), the Act on Collection of Information Regarding Electronic Communications in The Law Enforcement Authorities' Intelligence Activities (2012:278) and the Electronic Communications Act (2003:389). While not a law enforcement activity, the Swedish Armed Forces may collect data under the Act on Signals Intelligence in The Intelligence Activities of the Swedish Armed Forces (2008:717).

Secret Interception and Surveillance of Telecommunications

In the course of preliminary investigations, public prosecutors may apply for court authorisation to undertake secret interception of electronic communications (contents) or secret surveillance of electronic communications (metadata, geolocation, units present in a given area).

Interception and surveillance may concern the suspect's phone number as well as the phone numbers of persons the suspect is highly likely to contact. Permits are granted when the suspi-

cion rises to the level of reasonable grounds and it is of exceptional importance for the investigation of a serious crime.

3.2 Laws and Standards for Access to Data for National Security Purposes

Swedish Police, Security Services and Customs may intercept or monitor electronic communications in the course of their intelligence activities according to the Act on Collection of Information Regarding Electronic Communications in The Law Enforcement Authorities' Intelligence Activities (2012:278).

The communications in question must concern serious crimes and the interception or monitoring must be of particular importance for the prosecution of such crimes. The intercepting or monitoring authorities were previously authorised to initiate such activities independently, but must, as of 1 October 2019, apply for a permit from the Prosecution Authority. The Security and Integrity Committee must be notified of the decision within one month of ceasing the activities.

The National Defence Radio Establishment intercepts and monitors electronic communication intercepts signals intelligence under its specific charter, the Act on Signals Intelligence in Defence Intelligence Activities (2008:717). It operates according to its charter upon being given authorisation from the government or government offices, the armed forces, the Security Service and the National Operations Offices of the Police. Activities may only concern foreign threats such as military attacks, international terrorism, the development of weapons of mass destruction, serious threats against utilities, etc.

Wired collection may only take place for signals passing the boarders of Sweden and in the networks of operators of public communications networks. Furthermore, only signals between parties outside of Sweden are allowed to be intercepted. The authority must seek authorisation from the Defence Intelligence Court before initiating interception and monitoring. Such authorisation is only given if formal requirements are met, no less intrusive measures are available, the intrusion is motivated by the value of the sought-after information and the authorisation does not concern only one specific natural person.

3.3 Invoking Foreign Government Obligations

Private entities processing personal data under the GDPR may not invoke requests from foreign governments as a legitimate interest for processing and transferring personal data. Private entities may rely on a specific legal basis for processing which is necessity to comply with a legal obligation. The legal obligation however must be laid down by EU law or member state law to which the entity is subject.

Public authorities processing personal data under the GDPR cannot rely on legitimate interest as a legal basis. Outside of the application of the GDPR, public authorities with responsibility for intelligence and law enforcement may rely on their statutory basis for collecting and transferring personal data.

Sweden does not participate in a Cloud Act agreement with the USA.

3.4 Key Privacy Issues, Conflicts and Public Debates

The Public Health Agency of Sweden elected not to recommend the adoption of so-called tracing apps proposed to lower the spread of the SARS-CoV-2 virus or the "coronavirus". Due to this, there has been little public debate regarding the privacy issues related to app-based tracking. The IMY guidance has been to emphasise that where work environment regulations necessitate the processing of health-related data, such as

COVID-19 illness, such processing is acceptable from a data protection point of view. As work environment regulations have not been found to mandate vaccination or wide-spread routine testing, there have been next to no privacy conflicts related to the pandemic.

4. INTERNATIONAL CONSIDERATIONS

4.1 Restrictions on International Data Issues

The GDPR provides a general prohibition against transferring personal data outside of the EU or the EEA (so-called third countries). From this general prohibition the GDPR provides a set of exceptions (see **4.2 Mechanisms or Derogations that Apply to International Data Transfers**).

As noted above, see **1.8 Significant Pending Changes, Hot Topics and Issues**, a public inquiry into public authorities' use of cloud services issued a partial report in early 2021. With regard to processing of personal data, the report assessed that personal data is not considered to be transferred to third countries unless actual processing takes place outside of the EEA. Any processing outside of the EEA, regardless of how brief or whether the data is encrypted or pseudonymised, constitutes a transfer to a third country in the view off the report. The report further assessed that the mere fact that a processing entity is established in a third country, or that an entity established in the EEA but being a subsidiary of an entity established in a third country, does not constitute a transfer to the third country in question.

Sweden has adopted special national exceptions from the rules relating to, inter alia, restrictions on international transfers of personal data using the competence granted to member states in Articles 85 and 86 of the GDPR. The rules on international transfers of personal data therefore do not apply to the Freedom of The Press Act and the Fundamental Law on Freedom of Expression as well as processing of personal data in the field of journalism and in the course of academic, artistic or literary activities.

4.2 Mechanisms or Derogations that Apply to International Data Transfers

The GDPR offers a set of mechanisms to transfer personal data to third countries.

Adequacy Decisions

The GDPR offers a general authorisation of transfers of personal data to third countries or international organisations where the European Commission has decided that a third country, a territory or one or more specified sectors within that third country, or the organisation in question ensures an adequate level of protection. The European Commission adequacy decision on 12 July 2016 for transfers of personal data to the USA for commercial reasons ((EU) 2016/1250) was struck down by the CJEU on 16 July 2020. Following the decision, industry actors as well as public authorities have struggled with assessing their transfers of personal data and their legal exposure from said transfers. The European Data Protection Board (EDPB) has issued guidelines regarding supplementary measures to eliminate the risks of USA authorities accessing personal data transferred relying on any of the other transfer mechanisms. However, these guidelines practically restrict the utility in processing to encrypted and non-indexed storage and pseudonymised processing.

The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, the Republic of Korea, Switzerland, the United

Kingdom and Uruguay as providing adequate protection.

Appropriate Safeguards

Where there is no adequacy decision, personal data may still be transferred to a third country or an international organisation when the transferring party has provided appropriate safeguards and there are enforceable data subject rights and effective legal remedies available to data subjects.

The GDPR considers appropriate safeguards to be binding instruments between public authorities or bodies; such as binding corporate rules, standard data protection clauses adopted by the Commission, an approved code of conduct, or an approved certification mechanism.

Groups of undertakings or groups of enterprises engaged in economic activity with establishments in third countries may seek the approval for binding corporate rules to allow the transfer of personal data between their establishments.

As with the European Commission adequacy decisions, there are also ongoing discussions regarding the validity of the standard contractual clauses.

Derogations for Specific Situations

In the absence of adequacy decisions or appropriate safeguards, transfers to third countries may be allowed if the data subject has consented after having been informed of the possible risks and if the transfer is necessary for, for example, conclusion or performance of certain contracts or making legal claims. The IMY refers to the EDPB guidelines 2/2018 for guidance on such derogations.

4.3 Government Notifications and Approvals

Swedish law does not require any government notifications for transferring data internationally.

4.4 Data Localisation Requirements

The general rule under the GDPR is that data must be localised to the EU/EEA, unless transfers to third countries are permitted as set out in **4.2 Mechanisms or Derogations that Apply to International Data Transfers**. Within the EU/EEA, the GDPR ensures the free flow of data. There are no Swedish rules concerning the localisation of data.

4.5 Sharing Technical Details

Swedish law does not require any sharing of code, algorithms or similar technical details with the government.

4.6 Limitations and Considerations

The limitations and considerations that apply to organisations in connection with foreign data requests, foreign litigation and internal investigations carried out partially outside of the EU/EEA are the same as set out in **4.2 Mechanisms or Derogations that Apply to International Data Transfers**.

In the case of an internal investigation carried out exclusively inside the EU/EEA, such an investigation is primarily limited by the question of whether there is a legal basis for processing. An internal investigation would conceivably rest on either the need to defend or assert legal rights or claims, or finding a legitimate interest that overrides the interests of the data subjects in question.

4.7 "Blocking" Statutes

Sweden has transposed the so-called Copyright Directive or Information Society Directive (InfoSoc) through the Copyright Act (1960:729). The Copyright Directive, and thus the Copyright

Act, contains exceptions for transient reproductions of copyrighted works without independent economic value that occur on a network between third parties. However, rights-holders may secure injunctions against intermediaries (ie, internet service providers (ISPs)) if their services are used by a third party to infringe on copyrights or related rights. Most famously, rights-holders have secured injunctions against several Swedish ISPs forbidding their continued complicity in the Pirate Bay's ongoing infringement. In practice, such injunctions against ISPs constitute blocking orders.

The EU has adopted a blocking statute regarding the extraterritorial application of certain third country laws to protect EU operators engaged in lawful international trade, movement of capital and related commercial activities (Council regulation (EC) 2271/96). Operators may rely on the blocking statute to nullify the legal effects of blocked laws and recover damages caused by the application of such laws. Currently, the only third countries covered by the blocking statute are Cuba and Iran (Commission Delegated Regulation (EU) 2018/1100).

5. EMERGING DIGITAL AND TECHNOLOGY ISSUES

5.1 Addressing Current Issues in Law

Microsoft Products and the Risk of Personal Data Being Transferred to the USA

On 3 May 2021, the Swedish Tax Agency and the Enforcement Authority published a joint decision not to exchange the communications application Skype for the cloud-based Teams platform. The authorities would, however, continue to allow employees to participate in Teams-based meetings when so invited by external parties. In addition to commercial reasons, such as the risk of technical "lock-in", the authorities found that the lack of effective legal, technical or organisational measures means that the Swedish Tax Agency and the Enforcement Office could not live up to the requirements of the Public Access to Information and Secrecy Act to prevent unauthorised disclosure of confidential information in the respective authorities' activities if reliant on Teams. This means that the use of Teams will be in breach of the Act when confidential data is transferred to Microsoft's infrastructure.

"eSam", an association of 35 Swedish public authorities dedicated to promoting development of digitisation in the public sector, published a report on 18 November 2021 identifying vetted acceptable alternatives to the Teams platform on the market.

Furthermore, a risk assessment in accordance with the GDPR provision on appropriate technical and organisational measures in the authorities' assessment leaves no room for replacing Skype with Teams. This holds even if Microsoft were to process personal data only in the EU and Microsoft's commitment to oppose court decisions were in itself accepted as a sufficient guarantee that the provisions of the Data Protection Regulation would be complied with. The risks of a data transfer taking place are, according to the authorities, too great and the consequences are too serious.

In response to a prior consultation by the Municipality of Stockholm, the IMY published guidance on 2 June 2021 advising against the municipality's intended use of Azura AD and Teams until such time as the service provider, Microsoft, is able to give the necessary assurances in its capacity as data processor that no personal data will be transferred to a third country (ie, the USA) in breach of GDPR. The municipality decided in December 2021 to not implement Microsoft 365 in its units and corporations, while municipal schools who already had Microsoft 365 in use should seek alternative solutions.

Automated Decision-Making

Automated decision-making is explicitly allowed in the Administrative Procedure Act (2017:900). The act was introduced to give clarity to the already widespread use of such decision-making in public authorities such as the Social Insurance Agency. The use of automated decision-making in municipal matters has not enjoyed the same legal clarity in the Local Government Act (2017:725). The government initiated amendments to the Local Government Act to explicitly permit delegation of decision-making to an automated process, with a few excepted areas such as public procurement decisions.

Growing Awareness of Data Protection and Privacy Concerns

The issue of privacy and data protection is increasingly coming to the attention of decision-makers outside of public authorities and regulated financial institutions. Under Swedish law, members of boards of directors have a general duty to protect the interests of their principal and are responsible for any negligent acts that harm the principal. Since this is a general duty, it encompasses any circumstances that may harm the principal and therefore also includes matters concerning compliance with privacy and data protection laws and the upholding of information security. There have been no prominently reported cases concerning fiduciary duties to the extent that these relate to compliance with privacy and data protection regulation or information security. However, it can be expected that this aspect of directors' fiduciary duties will become of more interest and attention as issues concerning information security become more prevalent.

5.2 "Digital Governance" or Fair Data Practice Review Boards

Protocols for digital governance or fair data practice review boards or committees are uncommon in Sweden.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation.

Please see **1.7 Key Developments**, **2.5 Enforcement and Litigation** and **5.1 Addressing Current Issues in Law**.

5.4 Due Diligence

The due diligence process of reviewing information typically involves the processing of personal data. There is no Swedish regulation concerning due diligence in corporate transactions, as such. While the onus of the process falls on the prospective purchaser, it is not a requirement of the sort to provide a legal basis under the GDPR for data processing. Any legal basis will need to rely on the balancing of interests of Article 6.1 (f) of the GDPR. The outcome of such balancing will benefit from privacy-supporting measures such as the limitation of the amount of processed personal data, pseudonymisation and anonymisation of personal data where feasible, in conjunction with stringent non-disclosure commitments. Any transfer of personal data outside the EU will require special restrictions. Information and transparency requirements with regard to the data subjects whose data is processed in the context of due diligence is a challenge which may be mitigated through the data protection policies of the corporate entities concerned.

5.5 Public Disclosure

The Swedish Financial Supervision Authority's Guidelines (FFFS 2018:5) on reporting of events of material significance suggest undertakings should immediately report events that could lead to significant financial loss for a large number of customers and events that could lead to a considerable loss of reputation for the undertaking.

The events in question may include, for example, that:

- information provided in customer transactions is incorrect or deficient;
- customer transactions have been managed in an incorrect or deficient manner;
- errors have arisen in technical systems; or
- internal or external rules have been breached.

Providers of payment services are required to report serious operational incidents and security incidents to the Authority under the Guidelines (FFS 2018:4).

The Swedish Civil Contingencies Agency (MSB) has reporting requirements regarding information security incidents under Regulation (MSB-FS 2018:7) for providers of services of critical importance to society.

5.6 Other Significant Issues

The IMY adopted a supervision policy in January 2021 which entailed giving greater emphasis to the review of the personal data breaches reported to the authority. During 2020, approximately 4,600 incidents of personal data breaches were reported to the IMY, 200 less than the previous year. About 40% of the reported incidents concerned misdirected email. The IMY assumes a great number of breaches go unreported, possibly because the requirement to do so was only introduced in Sweden with the advent of the GDPR. Of the reported incidents in 2020, only three led to further investigation by the authority. All three investigated incidents concerned breaches in the operation of a public authority. Since 2018, altogether eight reported incidents have triggered IMY investigation. Once the IMY Annual Report 2021 is published, the effect of the new supervisory policy may become clear.

Contributed by: *Henrik Nilsson, Johan Grenefalk, Carl Gleisner and Annastasios Martidis,*
Wesslau Söderqvist Advokatbyrå

Wesslau Söderqvist Advokatbyrå (WSA) was founded through the merger of the law firms Gärde Wesslau and Hökerberg & Söderqvist, two prominent Swedish firms sharing a strong history. From its inception in the early 1950s, Gärde Wesslau became one of the leading law firms in Sweden. With its unique direct line to all the chambers of commerce in Europe and many international contacts, Gärde Wesslau became the law firm of choice for many international companies. Since the 1980s, Hökerberg & Söderqvist has been putting the business advantage of its clients in focus, working under the motto "to make the impossible possible". The firm made a name for itself through a series of high-profile insolvency cases in the financial sector. In 2016, the two firms merged to become WSA.

AUTHORS

Henrik Nilsson is a partner at Wesslau Söderqvist. He has worked for several Swedish and international law firms, and, prior to entering private practice, was a lawyer with the Swedish Competition Authority and the Swedish National Post and Telecom Authority. Henrik's professional focus is on regulatory law in a wide sense, with particular expertise in data protection and privacy, electronic communications, competition, EU and public procurement, and general commercial law. He regularly contributes to scholarly and general market publications on these matters.

Johan Grenefalk is a partner at Wesslau Söderqvist, advising clients primarily in the areas of capital markets, banking and finance, and data protection. In addition to holding an LLM, he also holds a BSc in Business Administration.

Carl Gleisner is a legal associate at Wesslau Söderqvist primarily advising clients on issues in tech law, such as information security, data protection, IT contracts and IP rights licensing. In addition to holding an LLM, he also holds a BSc in Computer Science and has experience with, and an extensive understanding of, software development.

Annastasios Martidis is a legal associate at Wesslau Söderqvist primarily advising clients in the areas of company reconstruction, insolvency, corporate and enterprise, commercial contracts, and banking and financial law. He worked as a corporate lawyer for several years in the insurance industry, with a special focus on collectively agreed occupational pensions. He has lectured on market law and intellectual property law at Linnaeus University.

Contributed by: *Henrik Nilsson, Johan Grenefalk, Carl Gleisner and Annastasios Martidis,*
Wesslau Söderqvist Advokatbyrå

Wesslau Söderqvist Advokatbyrå

Kungsgatan 36
Box 7836
SE-103 89
Stockholm
Sweden

Tel: +46 8 407 80 00
Email: info@wsa.se
Web: www.wsa.se