Legal 500
Country Comparative Guides 2024

Sweden
Data Protection & Cybersecurity

Contributor

Kompass Advokat

Anna Lööv

Partner | anna.loov@kompassadvokat.se

Lina Sandmark

Senior Associate | lina.sandmark@kompassadvokat.se

Lisa Nordbeck

Associate | lisa.nordbeck@kompassadvokat.se

Rebecca Larsson

Associate | rebecca.larsson@kompassadvokat.se

Viktor Tunón

Associate | viktor.tunon@kompassadvokat.se

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Sweden.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Sweden: Data Protection & Cybersecurity

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered by them; what sectors, activities or data do they regulate; and who enforces the relevant laws).

The Swedish legal framework for data protection, privacy and cybersecurity is primarily governed by EU law.

The main regulation on the personal data protection and privacy area is the EU regulation 2016/679 (the **General Data Protection Regulation**, **"GDPR"**). The GDPR lays down rules for the processing of personal data. The GDPR is applicable on any operation or set of operations which is performed on personal data, for example collection, use, storage and destruction of personal data. The only exceptions are processing by a natural person in the course of a purely personal or household activity and actions taken by competent authorities concerning criminal offences, execution of criminal penalties or public security. Processing of personal data concerning the latter is regulated by the Swedish **Crime Data Act**, which implements the EU directive 2016/680 on the protection of individuals regarding the processing of their personal data by police and criminal justice authorities and on the free movement of such data.

In some cases, the GDPR requires or allows the member states to have supplementary provisions concerning data protection. The main Swedish act in this area is the **Act with Supplementary Provisions to the EU's Data Protection Regulation**. This act contains certain provisions about processing of special categories of personal data, such as personal identity numbers and personal data relating to criminal convictions and offence. It also specifies the applicability of the legal grounds. The supplementary Swedish framework for data protection also contains sector-specific legislation with special rules for the processing of personal data, for example in sectors concerning health care and social care. In many cases, there are supplementary Swedish ordinances containing further provisions about data processing. For example, these ordinances may specify the purposes for which personal data may be processed and determine who the data controller is.

Another Swedish act governing data protection and privacy is the **Camera Surveillance Act**, which supplements the GDPR in relation to personal surveillance by an optical-electronic instrument.

The Swedish Authority for Privacy Protection exercises supervision over these laws on data protection.

Furthermore, the EU directive 2002/58/EC (the **ePrivacy Directive**) governs privacy regarding electronic communications networks and services. For example, this directive regulates the use of online identifiers in a user's terminal equipment, so-called "cookies". The directive is mainly implemented in Swedish law by the **Electronic Communications Act**. The Swedish Post and Telecom Authority exercises supervision over this act.

Other EU legislation on data processing and privacy is the EU regulation 2018/1807 (the **Non-Personal Data Regulation**) on a framework for the free flow of non-personal data in the European Union and the EU directive 2019/1024 (the **Open Data Directive**), governing re-use of public sector information.

The GDPR contains several provisions about cyber security regarding personal data processing. Another important EU legislation governing cyber security is the EU directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the **NIS Directive**). The NIS Directive is implemented into Swedish law by the **Act on information security for essential and digital services**. Another EU legislation on cyber security is regulation 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (the **Cybersecurity Act**).

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2024–2025 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments (together, "data protection laws"))?

Privacy and data protection

In early spring 2024, consent was reached between the EU legislators on adopting the EU regulation on artificial

intelligence (AI), the so-called **AI Act**. The regulation sets down a regulatory and legal framework for the use of AI. Because of the consequences AI might have on individuals, the use of AI has a close connection to the privacy area. Since the use of AI in many cases involve usage of personal data, the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**) and AI Act will in many cases be applied simultaneously.

Concerning Swedish privacy and data protection laws on health data, public investigators have laid down proposals for an overview of the laws on the reuse of health data for care and clinical research. The investigators propose changes in laws concerning health data and professional secrecy legislation to enable such reuse of personal data, amongst other things by making a new legislation on the reuse of personal data for clinical research purposes. The amendments and legislation are proposed to be entered into force in January 2025.

Cybersecurity

In the cybersecurity area, important changes will take place. In October 17, 2024 the EU directive 2022/2555 (the **NIS2 Directive**) will become applicable and replace the EU directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the **NIS Directive**) and the **Swedish Act on information security for essential and digital services**. The NIS2 Directive stipulates obligations for the member states to adopt national cybersecurity strategies and cyber security risk management measures and reporting obligations for entities and applies to private and public entities in sectors of high criticality and other critical sectors. Actions are now being taken by the Swedish legislator to implement this law into Swedish law.

In January 2025, the EU regulation 2022/2554 (**Digital Operational Resilience Act**, "**DORA**") will become applicable. The purpose of DORA is to make entities in the financial sector, including the insurance companies and third-party service providers, to strengthen its resilience against information and communication-related (ICT) disruptions and threats. Proposals for a Swedish law with supplementary provisions to DORA has been presented by the Swedish legislators. The proposed act includes provisions on, for example, supervision and interventions by the supervisory authority.

3. Are there any registration or licensing requirements for entities covered by these data protection laws, and if so what are the requirements? Are there any exemptions?

Processing of personal data is in general not based on registration or licensing requirements. However, to process personal data relating to criminal convictions and offences it is in some cases required to get authorization from the Swedish Authority for Privacy Protection.

According to the Swedish **Camera Surveillance Act,** license from the Swedish Authority for Privacy Protection is required when camera surveillance is performed at a place to which the public has access, if the surveillance is to be carried out by a public authority or someone other than an authority when carrying out a task of public interest.

4. How do these data protection laws define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data") versus special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction?

Since the relevant laws in the data protection, privacy and cyber security is based on EU law, the key definitions set forth in the Swedish laws are the same as those provided in the relevant EU regulations.

The EU regulation 2016/679 (the **General Data Protection Regulation**, "**GDPR"**) defines personal data as any information relating to an identified or identifiable natural person. The definition provided in the GDPR is also applicable when applying Swedish supplementary legislation about data protection. There is no specific definition of personally identifiable information. "Personal information" can be used as a synonym for personal data and have therefore the same meaning as personal data as defined in the GDPR.

A special category of personal data is sensitive personal data. According to the GDPR, sensitive personal data is personal data revealing 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 is subject to special safeguards and conditions (for these conditions, please see question 8).

Another special category of personal data is personal data relating to criminal convictions and offences, which also is subject to special safeguards. Also, personal identify number could be considered as a special category of personal data. Personal identity number is specifically regulated in the Swedish **Act with Supplementary Provisions to the EU's Data Protection Regulation**. In can also be mentioned that the Swedish Authority for Privacy Protection considered certain kind of personal data as privacy sensitive personal data. It can be, for example, payroll information, evaluation information or information relating to a person's personal sphere. Such data could require stronger protection.

5. What are the principles related to the general processing of personal data in your jurisdiction? For example, must a covered entity establish a legal basis for processing personal data, or must personal data only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

The EU regulation 2016/679 (the **General Data Protection Regulation**, **"GDPR"**) states six principles relating to processing of personal data. All six principles must be fulfilled for the processing to be lawful.

The principle of lawfulness, fairness and transparency

The processing of personal data must be covered by a legal basis in the GDPR and/or in Swedish supplementary legislation to be lawful. The principle also prohibits a processing of personal that is not fair or reasonable in relation to the registered. Lastly, the principle requires that personal data is processed in a transparent way and has a connection to the data subjects right to information.

The principle of purpose limitation

The personal data shall be collected for specified, explicit and legitimate purposes. The collected data may not be further processed in a manner that is incompatible with the original purposes. However, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is not to be considered as incompatible with the initial purposes.

The principle of data minimization

The personal data processed shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The principle stipulates that it is not permitted to process more personal data than is necessary to be able to fulfil the specific purpose or purposes of the processing.

The principle of accuracy

The personal data processed shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

The principle of storage limitation

The personal data processed shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may however be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The principle requires that retention periods are settled for the specific processing of personal data. In some cases, the retention period is specified in national law, for example in the Swedish **Accounting Act**.

The principle of integrity and confidentiality

The personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Another important principle, the principle of liability, relates to these principles and stipulates that the controller of a specific processing of personal data (i.e. the entity that determines the purposes and means of the processing of personal data) shall be responsible for, and be able to demonstrate compliance with, these principles.

6. Are there any circumstances for which consent is required or typically obtained in connection with the general processing of personal data?

Consent is one of the legal bases for which personal data may be processed according to the EU regulation 2016/679 (the **General Data Protection Regulation**, **"GDPR"**), but there are no circumstances where consent is required from the data subject to process data. However, the recitals to the GDPR state that data subjects should be allowed to give their consent to certain areas of scientific research.

If there is any other applicable legal basis for the specific processing, the Swedish Authority for Privacy Protection recommends the use of another legal basis instead of consent because of the inconveniences that may arise when the data subject revokes his or her consent.

A data controller may also choose to obtain consent from the data subject in addition to the legal basis legitimate interest. The consent then strengthens the legal basis.

7. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

According to the EU regulation 2016/679 (the **General Data Protection Regulation**, **"GDPR"**), consent of the data subject means *any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*. There are no form requirements for a valid consent; the data subject may express its consent in writing, oral or electronically.

When assessing whether consent is *freely* given, consideration must also be given to whether the execution of an agreement, including the provision of a service, has been made dependent on consent to such processing of personal data that is not necessary for the execution of that agreement. This, in turn, prohibits so-called "packaging" of consent, that is, a prohibition against entering into an agreement that is conditioned by the data subject also consenting to his personal data being processed, when the processing of personal data is not necessary for the implementation of the agreement. It is therefore necessary to determine the very purpose of the processing and which information is necessary to process for these purposes.

Consent is not presumed to be freely given if it is not possible for the data subject to give separate consents for different processing of personal data. This prohibits that one single consent is given for multiple processing operations with different purposes.

8. What special requirements, if any, are required for processing sensitive personal data? Are any categories of personal data prohibited from collection or disclosure?

As a principal rule, processing of sensitive personal data is prohibited. The EU regulation 2016/679 (the **General Data Protection Regulation**, **"GDPR"**) provides an exhaustive list of exceptions from this rule. The exceptions are based on:

- the data subject's explicit consent to the processing
- labour law, social security and social protection
- protection of the vital interests of the data subject or of another natural person
- processing of personal data within non-profit organizations
- publication of the personal data by the data subject
- legal claims and court ruling
- substantial public interest
- health care and social care
- public health
- archival, research and statistical purposes.

Processing of personal data relating to criminal convictions and or related security measures shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

According to the Swedish **Act with Supplementary Provisions to the EU's Data Protection Regulation**, personal identity numbers and coordination number (i.e. identification number) may only be processed without the data subject's consent when it is clearly justified by the purpose of the processing, the importance of secure identification or any other considerable reason.

9. How do the data protection laws in your jurisdiction address health data?

The EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**) addresses 'data concerning health' as personal data related to the physical or mental health of a natural person, including the provision of health care

services, which reveal information about his or her health status. According to the case law of the European Court of Justice (CJEU), the expression must be given a wide interpretation to include information concerning all aspects, both physical and mental, of the health of an individual. It also includes information that may indirectly reveal a person's health status.

10. Do the data protection laws in your jurisdiction include any derogations, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

The Swedish **Act with Supplementary Provisions to the EU's Data Protection Regulation** contains several exclusions and limitations of the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**), some of them already mentioned above. Other examples are that the GDPR shall not apply to the extent that it would conflict with the Swedish constitutional acts **Freedom of the Press Ordinance** or **Freedom of Expression Act**. Also, the above-mentioned Act contains exemptions from the data subject's rights in the GDPR, for example if the controller is prohibited by law to disclose the personal data concerned (for more information, see question 39).

11. Do the data protection laws in your jurisdiction address children's and teenagers' personal data? If so, please describe how.

The EU regulation 2016/679 (the **General Data Protection Regulation**, **"GDPR"**) applies in its entirety to the processing of children's and teenagers' personal data. However, there are several provisions in the GDPR that aim to strengthen the protection of children's personal data, such as requirements on using an easily accessible form, using clear and plain language when providing data processing information and on the assessment whether the controller has a legitimate interest to process the personal data.

In relation to the offer of information society services directly to a child, the child can only consent to such processing of personal data if the child is at least 13 years old. If the child is under the age of 13 years and lives in Sweden, consent or approval of consent is required by the person who has parental responsibility for the child. This applies regardless of where the personal data controllers or personal data assistants are established.

12. Do the data protection laws in your jurisdiction address online safety? Are there any additional legislative regimes that address online safety not captured above? If so, please describe.

In general, the data protection laws themselves do not specifically address online safety. However, all these legislations include provisions that relate to online safety, for example the provisions about technical safety measures for processing personal data according to the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**) and rules about cookies according to the Swedish **Electronic Communications Act**.

In addition, in February 2024 the EU Regulation 2022/2065 on Single Market For Digital Services (the **Digital Services Act, "DSA"**) became applicable. The main aim of the DSA is to prevent illegal and harmful online activity and disinformation. The DSA contains rules for intermediaries and internet platforms such as marketplaces, social media, content sharing platforms and app stores. A requirement according to the DSA is that online platforms must take new measures that improve transparency regarding e.g. advertising and also protect minors online.

13. Is there any regulator in your jurisdiction with oversight of children's and teenagers' personal data, or online safety in general? If so, please describe, including any enforcement powers. If this regulator is not the data protection regulator, how do those two regulatory bodies work together?

In Sweden, the Swedish Authority for Privacy Protection exercises supervision over the protection for personal data, including the processing for children's and teenagers' personal data. Infringement of the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**), regardless of what category of data subject the data processing concerns, could lead to warnings, reprimands and administrative fines etc. There is no regulator specially designated with oversight of children's and teenagers' personal data or online safety.

14. Are there any expected changes to the online safety landscape in your jurisdiction in 2024–2025?

There are no expected changes to the online safety landscape in 2024-2025.

15. Does your jurisdiction impose 'data protection by design' or 'data protection by default' requirements or similar? If so, please describe the requirement(s) and how businesses typically meet such requirement(s).

The EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR")** set forth the principle of data protection by design and privacy by default. The controller is required to implement appropriate technical and organisational measures which are designed to implement the data-protection principles in an effective manner and to integrate the necessary safeguards into the processing to meet the requirements of the GDPR and protect the rights of data subjects *(privacy by design).*

The controller is also required to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed *(privacy by default)*. Such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Businesses typically meet these requirements by implementing internal policies concerning data protection and adopts a risk-based approach in matters concerning data protection. Businesses also implements different kind of technical and organisational measures such as authorization system and measures protecting personal data from unauthorized access.

16. Are controllers and/or processors of personal data required to maintain any internal records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

A controller is obligated to maintain a record of processing activities under its responsibility. The record shall be in writing, including in electronic form. Among other things, the record shall contain the purposes of the processing, a description of the categories of data subjects and of the categories of personal data and the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations. A processor shall also maintain a record of its processing activities. Such a register is however more limited.

Businesses typically meet this requirement by keeping a well-structured and organized electronical record that is easy to update.

The obligation to maintain a record of processing activities does not apply to an enterprise or an organization employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes sensitive personal data or personal data relating to criminal convictions and offences.

17. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

As mentioned in question number 5, one of the main principles in the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**) is storage limitation which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. This means that organizations processing personal data must limit the storage for such data. This said, no explicit retention period is specified in the GDPR. The personal data must be anonymized or deleted once the purpose for which the personal data is processed has been fulfilled. However, the retention period is specifically stipulated in some acts, for example in the Swedish **Anti-money laundering Act**, where the principal rule is that certain documents and data shall be maintained for five years, counting from when the measure or transaction was performed.

Requirement on having policies and procedures on data retention and data disposal appear from the general main principle about accountability where it is indirectly stated that such policies and procedures covering data retention and data disposal are necessary to demonstrate compliance of applicable articles in GDPR.

18. Under what circumstances is a controller operating in your jurisdiction required or recommended to consult with the applicable data protection regulator(s)?

According to the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**) a controller shall consult with the Swedish Authority for Privacy Protection prior to processing where a data protection impact assessment (DPIA) under the GDPR indicates that the processing would result in a high risk, if measures were

not taken by the controller to mitigate the risk.

19. Do the data protection laws in your jurisdiction require or recommend risk assessments in connection with data processing activities and, if so, under what circumstances? How are these risk assessments typically carried out?

If a processing, in particular using new technologies and taking into account the nature, scope, context and purpose of the processing, is likely to result in high risk to individual people's rights and freedoms the controller must carry out an impact assessment. The assessment must be made prior to starting the processing activity.

There are three specific cases mentioned which by default requires a DPIA:

- When a systematic and extensive evaluation of personal aspects is intended, relating to natural persons which is based on automated processing, incl. profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- When processing is planned to be performed on a large scale of special categories of data;
- When a systematic monitoring is planned of a publicly accessible area on a large scale.

Also, the Swedish Authority for Privacy Protection has published a list of situations where a DPIA is required. If two or more criteria are met, a DPIA should be performed:

- Evaluation or scoring people
- Processing of personal data for the purpose of making automated decisions that have legal consequences or similarly significant consequences for the data subject
- Systematic monitoring of people
- Processing of sensitive personal data according to article 9 or data of a very personal nature
- Processing of personal data to a large extent
- Combination of personal data from two or more processes in a way that deviates from what the data subjects could reasonably expect
- Processing of personal data about people who for some reason are at a disadvantage or in a dependent position and are therefore vulnerable
- Using of new technology or new organizational solutions
- Processing of personal data with the aim of preventing data subjects from accessing a service or entering into an agreement

The list is not exhaustive and is likely to be updated in the future.

The data protection impact assessments are typically carried out as follows:

1. Analyse what risks the personal data processing may involve and suggest appropriate security measures. Document the findings to be able to demonstrate compliance with the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**).
2. Based on the risk analysis, decide whether there is a need to go further and make an impact assessment, DPIA.
3. If a DPIA is to be performed, include at least the following:
    1. Description of the planned processing of personal data
    2. Assessment of the necessity and proportionality
    3. Planned actions to demonstrate compliance
    4. Assessment of risks to the rights and freedoms of the data subjects
    5. Planned measures to manage the risks
    6. Documentation
    7. Monitoring and review

Where appropriate, the controller shall also seek the views of data subjects or their representatives on the intended processing.

20. Do the data protection laws in your jurisdiction require a controller's appointment of a data protection officer, chief information security officer, or other person responsible for data protection, and what are their legal responsibilities?

If any of the following three questions is answered with a "Yes", it is required to appoint a data protection officer (DPO) according to the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**):

1. Are the organization/company at hand an authority or an elected assembly, i.e. a public

body?
2. Is the core business to monitor individuals regularly, systematically and extensively?
3. Is it the core business to process sensitive personal data or information about crimes on a large scale?

The legal responsibilities for a DPO are to collect information about how the organization processes personal data, monitor and control that the organization complies with regulations and internal policies as well as provide information and advice within the organization. Besides that, the DPO shall give advice on impact assessments, be the contact person for the Swedish Authority for Privacy Protection and the data subjects and the organizations employees as well as cooperate with the Swedish Authority for Privacy Protection, for example during inspections.

Note that all organizations must make their own assessment of whether they need a DPO. It may be so that a personal data processor needs a data protection officer even if its principal (the controller) does not need a data protection officer.

The appointment of a DPO shall be reported to the Swedish Authority for Privacy Protection.

21. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s).

There are no explicit legal requirement or recommendation regarding employee training. However, for employees to be able to comply with the overall obligations set out in the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR**") and the employers internal policy documents on personal data, they must have sufficient knowledge in the area. A way of demonstrating compliance, when the controller shall comply with the requirement in the GDPR on appropriate technical and organizational measures, are to educate employees and give them sufficient training and knowledge about data protection.

Also, one of the tasks assigned to the data protection officer is to inform and advice employees who carry out processing of personal data in their work, about their obligations pursuant to the GDPR. The data protection officer shall also monitor compliance with internal policies including awareness-raising and training of staff involved in processing activities.

It can be noted that EU regulation 2022/2554 (**Digital Operational Resilience Act, "DORA"**) requires financial entities to provide digital operational resilience training and ICT skills to employees. The regulation will apply from 17 January 2025.

22. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

When personal data are contained from the data subject the controller shall, at the time when personal data are obtained, provide certain information. Generally, information required to be disclosed is the identity and contact details of the controller, details about the data protection officer if applicable, purpose of the processing, legal basis, the recipients, or categories of recipients of personal data and if applicable information about whether the controller intends to transfer personal data to a third country. Further, the individual shall be informed of its rights under the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**) and of the right to file a complaint with respect to the processing with the supervisory authority. Some additional information requirements apply according to succeeding articles in the GDPR. When personal data are not contained from the data subject, generally the same information requirements apply as for the situation above. There is no explicit requirement on the format for how the information shall be given. However, the information shall be easily accessible and easy to understand, and clear and plain language shall be used. This concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the data subjects concerned and their right to obtain confirmation and communication of personal data concerning them and which are being processed.

Also, there are other laws detailing specific requirements on disclosure of information such as the Swedish **Camera Surveillance Act** stipulating that controllers are required to give detailed information to data subjects if any video surveillance is at use. The information requirements are described in detail in the European Data Protection Board's (EDPB) Guidelines 3/2019 on processing of personal data through video devices. The Swedish **Electronic Communications Act** also requires controllers to inform all visitors to a website who uses cookies about their use of cookies and the purpose thereof. Please see

further about cookies in question number 26. In addition, the EU regulation 2022/2065 (**Digital Services Act**, **"DSA"**) requires that providers of online platforms provide meaningful information to recipients of services in the online interface on the main parameters used for determining that a specific advertisement is presented to them, providing meaningful explanations of the logic used to that end, including when this is based on profiling.

23. Do the data protection laws in your jurisdiction draw any distinction between the controllers and the processors of personal data, and, if so, what are they?

The EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**) draws a distinction between the controller and the processor in the way that the controller remains responsible for being able to demonstrate compliance of the processing undertaken on the controller's behalf even if it's provided by a processor.

24. Do the data protection laws in your jurisdiction place obligations on processors by operation of law? Do the data protection laws in your jurisdiction require minimum contract terms with processors of personal data?

Certain obligations in the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**) apply for the controller being the one who determines for what purpose the personal data is processed and how it is processed. However, many of the obligations that apply to the controller also apply for the processor being the one who processes personal data on behalf of the controller.

A contract, or other legal act under union or member state law, must be entered into by a controller and a processor when a controller appoints a processor to process personal data on behalf of the controller. Often a so-called data processing agreement (DPA) is used between the parties. The GDPR specify certain minimum requirements for the controller to include in the DPA between the controller and the processor, including instructions to the processor and information security requirements.

25. Are there any other restrictions relating to the appointment of processors (e.g., due diligence, privacy and security assessments)?

No specific due diligence process is stipulated in the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**). However, there are requirements on the controller to only contract a processor who provide sufficient guarantees on safeguarding the data subject's rights and ensures to meet the data protection requirements within the GDPR.

26. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these terms defined, and what restrictions on their use are imposed, if any?

In the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**), profiling means any form of automated processing of personal data where the data is used to assess certain personal qualities, in particular to analyse or predict the person's work performance, financial situation, health, personal preferences, interests, reliability, or behaviour etc. Profiling is subject to the rules governing the processing of personal data in general, i.e., the legal grounds for processing and data protection principles. Sometimes profiling results or overlap with automated individual decision-making which can be exemplified as an automatic rejection to an online credit application or an automatic negative reply in an online recruiting process. The data subject has the right to not be subject of a decision that is only based on automated decision-making, including profiling, if the decision has legal consequences for the individual or if it affects the data subject in a similar way. Since both automated decision-making and profiling imply processing of personal data, the data subject always has the right to information about how the data is processed.

According to the Swedish **Electronic Communications Act** all visitors to a website must be informed if the website uses any cookies and why. Visitors must also leave its consent to the website's use of cookies. A valid consent will have to meet the higher standards of consent in the GDPR, compared to a "passive consent" through pre-ticked boxes and pre-defined statements in privacy policies. However, the above does not prevent the website holder to such storage or access that is necessary to transmit an electric message via an electronic communications network or provide a service explicitly requested by the visitor.

The EU regulation 2022/2065 (**Digital Services Act, "DSA"**) specifies that providers of online platforms must not present advertisements on their interface based on

profiling using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor or when the personal data used is special categories of personal data in the GDPR. Furthermore, the DSA specifies that providers of very large online platforms and of very large online search engines that use recommendation systems shall provide at least one option for each of their recommender systems which is not based on profiling.

Monitoring is not mentioned nor defined in the GDPR. If it involves processing of personal data, the GDPR is applicable and the regulation must be complied with.

27. Please describe any restrictions on targeted advertising and/or cross-contextual behavioral advertising. How are these terms or any similar terms defined?

The Swedish **Electronic Communications Act** include rules on cookies and similar trackers (including third party cookies which can be used for targeting advertising). The use of cookies requires consent from the website visitor. Cookies are considered personal data if they are used to identify visitors at a website. If so, the EU regulation 2016/679 (the **General Data Protection Regulation**, **"GDPR"**) applies and the requirements regarding consent and legitimate interest must be met.

28. Please describe any data protection laws in your jurisdiction addressing the sale of personal data. How is the term "sale" or such related terms defined, and what restrictions are imposed, if any?

Processing of personal data according to the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**) has a broad spectrum and the sale of personal data is considered as processing. Sale of personal data is therefore governed by the same requirements in the GDPR as any other processing, i.e. legal ground, purpose, information requirements etc. applies.

29. Please describe any data protection laws in your jurisdiction addressing telephone calls, text messaging, email communication, or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

The Swedish **Electronic Communications Act** states that electronic communication service providers must implement appropriate organizational and technical measures to secure protection for data processed in the service. Incidents must be handled correct and promptly as well as disclosed in certain cases to customers and users of the service. This is additional to the notification requirements stipulated in the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**). The above-mentioned act also stipulates limitations on the duration and purpose of the processing and erasure and anonymization requirements.

Unsolicited marketing is governed under the Swedish **Marketing Act** where marketing by automated means (through e-mail) to a natural person requires prior consent. If the following three criteria are met, no consent is required, if the person's email address was obtained in connection with sales of product or services:

- the person must not have objected against obtaining e-mail marketing;
- the marketing may only relate to the sellers own, similar products or services (as the person has shown interest for); and
- the person must clearly and explicitly have been able to object to the use of e-mail for marketing purposes when the data was collected and in conjunction with each subsequent marketing communication (i.e., a possibility to easily and free of charge opt out).

Direct marketing is allowed if the processing meet the requirement set forth in the GDPR. However, the data subject can at any time object to the processing and the controller must immediately cease with the targeted advertising.

30. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined, and what restrictions are imposed, if any?

The processing of biometric personal data to identify a data subject involves processing of special categories of personal data. The general rule in the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**) is that it is prohibited to process such data. However, an exception from the prohibition can apply. It may for example be permissible:

- If the data subject has given its explicit consent
- To protect a person's vital interests, or
- If it's necessary for the purpose of a

substantial public interest

However, there are cases where a processing can be considered unauthorized even with the data subject's consent, i.e. when an imbalance is imposed between the data subject and the controller.

A data controller should perform a DPIA to ensure whether it is lawful to process the intended processing and, if necessary, initiate a prior consultation with the Swedish Authority for Privacy Protection.

31. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

In early spring 2024, consent was also reached between the EU legislators on adopting the EU regulation on artificial intelligence (AI), the so-called **AI Act**. The regulation sets down a regulatory and legal framework for the use of AI. Because of the consequences AI might have on individuals, the use of AI has a close connection to the privacy area. Since the use of AI in many cases involve usage of personal data, the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**) and AI Act will in many cases be applied simultaneously.

32. Is the transfer of personal data outside your jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

Transfer of personal data outside of the EU/EEA is restricted but can be permitted if one of the mechanisms in the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**) applies:

- There is an adequacy decision from the European Commission, i.e. where a certain country ensures a sufficient level of protection of personal data,
- Appropriate protection measures have been taken, such as Binding Corporate Rules (BCR) or Standard Contractual Clauses (SCC),
- If none of the mechanisms above is applicable, transfer can be permitted provided that the transfer is not repetitive, concerns a limited number of data subjects, are necessary for the purposes of the data controllers compelling legitimate interests which is not overridden by data subject interests, the data controller has assessed all circumstances surrounding the transfer and therefor provided suitable safeguards. In these situations, the supervisory authority must be informed of the transfer.

Transfers of personal data from the EU/EEA to the US has been problematic since July 2020 when the European Court of Justice (CJEU) in the Schrems II case disallowed the Privacy Shield framework. In July 2023 the European Commission issued a new adequacy decision for the US. The Commission's decision means that transfers to organizations covered by the EU-US Data Privacy Framework is permitted. However, the adequacy decision does not mean that the transfer of personal data to US cloud service providers is unrestricted, as they still have operations and recipients in other countries.

33. What security obligations are imposed on data controllers and processors, if any, in your jurisdiction?

In accordance with the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**), data controllers and data processors are obligated implement appropriate technical and organizational measures in relation to the risks of the processing. The measures should reflect the nature, scope, context and purposes of processing as well as the risks for individuals. The appropriate security measures depend, among other things, on the sensitivity of the processing and the technical solutions available. In general, the higher the risks, the higher the level of security required to reduce the identified risks.

A selection of technical and organizational security measures is e.g. encryption, firewalls, anti-virus protection, back-ups, pseudonymization, processes for testing, access restriction and assessing and evaluating the effectiveness of the measures. Governmental authorities, healthcare providers and providers of electronic communication services also have special requirements.

34. Do the data protection laws in your jurisdiction address security breaches and, if so, how do such laws define a "security breach"?

The EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**) addresses personal data breaches,

which is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

35. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecom, infrastructure, AI)?

The EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**) applies generally in all sectors. However, there are some special security requirements within certain sectors. Several governmental authorities are subject to special security requirements by specific acts or ordinances. Operations of importance to national security are subject to specific security requirements according to the Swedish **Protective Security Act.**

The use of artificial intelligence in the EU will soon be regulated by the EU regulation on artificial intelligence (AI), the so-called **AI Act**, which the European Parliament adopted on March 13, 2024. It now needs a linguistic review before being formally approved by the Council. It will then be published in the Official Journal of the European Union. The AI Act will enter into force 20 days after publication and the rules will apply from 6 to 36 months depending on the regulation.

The EU directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the **NIS directive**) imposes specific security requirements on certain essential and digital services including energy, transportation, banking, financial market infrastructure, healthcare, delivery and distribution of drinking water, digital infrastructure, as well as digital services. The NIS Directive is implemented into Swedish law by the **Act on information security for essential and digital services**.

In January 2025, the EU regulation 2022/2554 (**Digital Operational Resilience Act**, "**DORA**") will become applicable. The purpose of DORA is to make entities in the financial sector, including the insurance companies and third-party service providers, to strengthen its resilience against information and communication-related (ICT) disruptions and threats.

Currently, the Financial Supervisory Authority imposes information security requirements on banks and insurance companies through the application of guidelines from EBA and EIOPA. Payment service providers are subject to specific security requirements according to the Swedish **Act on Payment Services**.

36. Under what circumstances must a business report security breaches to regulators, impacted individuals, law enforcement, or other persons or entities? If breach notification is not required by law, is it recommended by the applicable regulator in your jurisdiction, and what is customary in this regard in your jurisdiction?

According to the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**) data controllers normally have 72 hours to submit a report to the supervisory authority of a security incident/personal data breach that could result in a risk for an individual. The data processor has an obligation to inform the data controller about a detected breach without undue delay. If a personal data breach is likely to result in a high risk for an individual there is also an obligation to immediately inform the individual.

Providers of publicly available electronic communication services, who are subject to the rules in the Swedish **Electronic Communications Act** are obligated to report integrity and security incidents to a supervisory authority. Subscribers or users affected by the processed data if they are likely to be negatively affected must also be informed or if the supervisory authority requests this.

Providers of an essential or digital service covered by the EU directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the **NIS directive**) must report incidents that have a significant impact on the continuity of the essential service they provide to a supervisory authority. The initial report shall be provided within six hours from the time of the incident. The NIS Directive is implemented into Swedish law by the **Act on information security for essential and digital services**.

The Swedish **Protective Security Ordinance** sets forth requirements regarding when a reporting obligation to the Security Service exists and the procedure that follows with such reporting. For instance, all companies that are subject to the ordinance have a responsibility to immediately report to the Security Service in case of an IT incident in an information system for which the operator is responsible, which is significant for security-sensitive operations and where the incident can seriously affect the security of the system.

37. Does your jurisdiction have any specific legal requirements or guidance for dealing with

cybercrime, such as in the context of ransom payments following a ransomware attack?

Cybercrimes are regulated in the Swedish **Criminal Code** and include breach of data security, data intrusion, unlawful identity use and data fraud. There are legal obligations on how to protect data using preventive measures and procedures to follow if a data breach is identified, such as reporting. The EU directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the **NIS Directive**) is one of the regulatory frameworks that regulate the obligations regarding the security level of data. The NIS Directive is implemented into Swedish law by the **Act on information security for essential and digital services**.

Another important regulatory framework is the EU regulation 2022/2554 (**Digital Operational Resilience Act**, "**DORA**") that will become applicable In January 2025. The purpose of DORA is to make entities in the financial sector, including the insurance companies and third-party service providers, to strengthen its resilience against information and communication-related (ICT) disruptions and threats and thereof also cybercrimes.

The Civil Contingencies Agency and the European Union Agency for Cybersecurity are among the authorities that can provide general guidance on cybersecurity. Information about cybersecurity can also, to some extent, be found through the Swedish Authority for Privacy Protection regarding protection of personal data, the Post and Telecom Authority regarding the protection of electronic communications and the Swedish Tax Authority, regarding identity theft.

38. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

There is no separate regulator for cybersecurity. However, the Civil Contingencies Agency is responsible for coordination of information security, cybersecurity and safe communications. The Agency is mandated to, within the area of cyber and information security, analyse and assess the development of the surrounding world, give advice to and support authorities, municipalities, regions, organizations and companies in their preventive work. There is also a National Cyber Security Centre, where multiple authorities collaborate to prevent, detect and manage cyber-attacks and other IT incidents that risk damaging national security.

39. Do the data protection laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, any exceptions and any other relevant details.

There are several individual data privacy rights provided by the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**). If the data subject contacts the data controller or processor to exercise these rights the data controller is usually obligated to respond no later than within one month.

- Right to information
- Right to access
- Right to rectification
- Right to erasure ("right to be forgotten")
- Right to restriction of processing
- Right to object
- Right to data portability
- Right to restrictions on automated decision-making

The data subject has the right to obtain information about the processing of their personal data. The right to access enables the data subject to request a copy of the personal data that is being processed, with additional information regarding e.g. the source from where the data was collected or during what time the data will be stored.

Restrictions on the right to access are found in the Swedish **Act with Supplementary Provisions to the EU's Data Protection Regulation**. The data subject is not entitled to information that the data controller may not disclose according to law, such as the Swedish **Publicity and Secrecy Act**. Neither does the right apply to personal data in running text that has not received its final form when the request was made or that constitutes a memory note or the like.

The data subject also has the right to request to have their personal data rectified or deleted. The right to erasure does not apply to data that is needed to comply with laws and regulations, such as the Swedish **Accounting Act**. If the individual requests restriction, the data may only be processed for certain limited purposes unless the data controller can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or if the processing is for the establishment, exercise or defence of legal claims.

Right to data portability means that the data subject can demand to have their personal data transferred to another provider if the data was provided by the data subject and if the processing is based on consent or for the performance of a contract. The data subject may also request not to be subject to decisions based solely on automated decision-making or profiling, provided that the decision is likely to have legal consequences or significantly affect the data subject.

40. Are individual data privacy rights exercisable through the judicial system, enforced by a regulator, or both?

The Swedish Authority for Privacy Protection (supervisory authority) enforces the individual data privacy rights. In addition to supervise compliance with the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**), the authority also investigates incoming complains from individuals. If it is concluded that personal data is being processed in contrary to the GDPR the authority may impose various measures, such as reprimands, orders or fines. The data subject can also claim compensation for damages from the data controller or processor in court.

41. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

A data subject can file a complaint to the Swedish Authority for Privacy Protection but also bring a civil action against the data controller or processor in court and claim damages. To be eligible for damages, the data subject must have suffered damages caused by the data controller or data processor.

42. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual damage to have been sustained, or is injury to feelings, emotional distress or similar sufficient for such purposes?

Data subjects can claim compensation when they are affected by breaches of the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**), both for actual damage and injury of feelings, such as emotional distress. However, injuries of feelings normally render quite limited damage amounts.

43. How are data protection laws in your jurisdiction enforced?

In accordance with the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**), the Swedish Authority for Privacy Protection has the same mandate and tasks as all other supervisory authorities in the EU. More specifically, the authority has several investigative powers which involve e.g. ordering data controllers or data processors to provide information or respond to the data subject's request for their rights and conducts investigations/audits including access to premises. GDPR is also enforced by the data subjects right to submits complaints to the Swedish Authority for Privacy Protection or claims damages in court. An individual can also appeal the Swedish Authority for Privacy Protections decision not to act on a received complaint to court to have their case reviewed.

44. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

The Swedish Authority for Privacy Protection may issue warnings, reprimands, and bans on processing and impose administrative fines. The action to be taken or the amount of the fines depends on the severity of the violations. For minor infringements, the fine can amount to the higher of 2 percent of the company's total annual turnover and EUR 10 MEUR. For infringements of a more serious nature, fines can amount to the higher of 4 percent of the company's total annual turnover and EUR 20 MEUR. For public authorities, the maximum fine is 10 MEUR and for less serious infringements 5 MEUR.

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

According to the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**), the general conditions for imposing administrative fines includes that they should be effective, proportionate and dissuasive. In determining the amount of the fine the provision that has been infringed is considered as well as who committed the infringement and the circumstances in the individual case. The range therefore varies from 0 to the maximum amount set. In cases of several infringements, the amount of the fine is determined based on an overall assessment of these. In the assessment, considerations are taken to whether the conduct was negligent or intentional, the duration of the infringement, the number

of data subjects affected, the extent of the damage and the measures taken to mitigate the damage. The EDPB has published guidelines 04/2022 on the calculation of administrative fines under the GDPR.

46. Can controllers operating in your jurisdiction appeal to the courts against orders of the regulators?

Data controllers can appeal a decision made by the Swedish Authority for Privacy Protection to the court within 21 counted from the date of the decision. The authority's decision-making process can also be challenged by submitting a complaint to the judicial ombudsman.

47. Are there any identifiable trends in enforcement activity in your jurisdiction?

As of 2023, the Swedish Authority for Privacy Protection received increased resources from the government, which during the year showed clear results in the form of reduced processing times and case balances for all major case flows. The authority has also been able to manage a larger amount of complains and supervisions, a trend that is expected to continue.

In 2023, the Swedish Authority for Privacy Protection initiated 210 inspections in the form of supervision, a significant increase from 120 the previous year. The authority decided on penalty fees in a total of eleven supervisory cases amounting to SEK 120,400,000, an amount more than twice as high compared to the year before. The number of decisions regarding penalty fines shows an increasing trend.

The European Court of Justice also ruled in 2023 that European Data Protection Authorities have more far-reaching obligations to investigate complaints from individuals and the national Supreme Administrative Court ruled that individuals can appeal against the Swedish Authority for Privacy Protections decisions. There is also intensive work on new legal acts in the EU that will have a significant impact on national companies, the digitalization of the public sector and on the Swedish Authority for Privacy Protection operations.

During 2024, the Swedish Authority for Privacy Protection plans to examine e.g., in addition to complaints and risk-based inspections, how municipalities work with the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**) and new technical solutions on camera surveillance.

48. Are there any proposals for reforming data protection laws in your jurisdiction currently under review? Please provide an overview of any proposed changes and the legislative status of such proposals.

There are no current proposals for reforming the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**), the Swedish **Act with Supplementary Provisions to the EU's Data Protection Regulation** or the Swedish **Ordinance with Supplementary Provisions to the EU's Data Protection Regulation**.

Contributors

Anna Lööv
Partner
anna.loov@kompassadvokat.se

Lina Sandmark
Senior Associate
lina.sandmark@kompassadvokat.se

Lisa Nordbeck
Associate
lisa.nordbeck@kompassadvokat.se

Rebecca Larsson
Associate
rebecca.larsson@kompassadvokat.se

Viktor Tunón
Associate
viktor.tunon@kompassadvokat.se