Legal 500
Country Comparative Guides 2025

Sweden

Data Protection & Cybersecurity

Contributor

Kompass Advokat

Anna Lööv

Lawyer and Managing Partner, Head of Data Protection and Finance Regulatory | anna.loov@kompassadvokat.se

Mina Gholiof Roa

Lawyer and Senior Associate | mina.gholiof@kompassadvokat.se

Johanna Borg

Senior Associate | johanna.borg@kompassadvokat.se

Lisa Nordbeck

Associate | lisa.nordbeck@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; 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 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 enforce 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 certain 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 nominate the data controller and specify the purposes for which personal data may be processed.

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.

On October 17 2024, the EU directive 2022/2555 (the **NIS2 Directive**) became applicable and replaced 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 **Swedish Act on information security for essential and digital services** is therefore soon to be replaced by a new national law implementing the NIS 2 Directive. 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. 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**).

On 17 January 2025, the EU regulation 2022/2554 (**Digital Operational Resilience Act**, "**DORA**") became 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. In some cases, DORA requires or

allows the member states to enforce supplementary provisions in national law concerning digital operational resilience in the financial sector. The main Swedish act in this area is the **Act with Supplementary Provisions to the EU's Regulation on digital operational resilience for the financial sector**. This act contains provisions on threat-led penetration testing (TLPT), supervision, intervention by the Swedish Financial Supervisory Authority and effective remedies.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2025 - 2026 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments)?

Data protection and privacy

On 11 September 2025, the EU Regulation 2023/2854 (the **Data Act**) shall apply. Stipulating harmonized rules on access, sharing and storage of data, the purpose of the Data Act is to establish processes and structures to facilitate data sharing between companies, individuals and the public sector by stipulating harmonized rules on access, sharing and storage of data. The Data Act is applicable both on non-personal data and personal data. However, regarding processing of personal data, the EU regulation 2016/679 (the **General Data Protection Regulation**, "**GDPR**") shall prevail.

On 1 August 2024, the EU Regulation 2024/1689 (the **regulation on artificial intelligence,** "**AI Act"**) entered into force. 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 GDPR and AI Act will in many cases be applied simultaneously. Most of the provisions of the AI Regulation will apply 24 months after its entry into force, i.e. on 1 August 2026. However, the provisions on purpose, scope, and basic definitions of AI systems and provisions on prohibited AI practices applies from 2 February 2025, as well as provisions on, for example, requirements for high-risk AI systems and transparency and information obligations for AI systems.

Cybersecurity

Regarding the entry of the EU directive 2022/2555 (the **NIS2 Directive**), actions are now being taken by the Swedish legislator to implement this directive into Swedish law, which at earliest is expected during the autumn of 2025.

3. Are there any registration or licensing requirements for entities covered by these data protection and cybersecurity laws, and if so what are the requirements? Are there any exemptions? What are the implications of failing to register / obtain a licence?

Processing of personal data is in general not based on registration or licensing requirements. However, for individuals (i.e. not a public authority) to process personal data relating to criminal convictions and offences it is in some cases required to obtain authorization from the Swedish Authority for Privacy Protection.

4. How do the data protection laws in your jurisdiction define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data")? Do such laws include a specific definition for special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction (e.g., "controller", "processor", "data subject", etc.)?

Since the relevant laws in the data protection, privacy and cyber security areas are 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 is not specifically defined.

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 7).

Additionally, it can be mentioned that the Swedish Authority for Privacy Protection considers certain kinds 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.

'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. In certain cases, the controller is nominated in supplementary Swedish data protection law, such as sector specific law. 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Regarding the concept of controller and processor in the GDPR, the European Data Protection Board has adopted guidelines 07/2020 which contains further guidance.

'Data subject' is defined as an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly (see preamble 26 to GDPR).

In addition to these definitions, article 4 in the GDPR includes other important definitions, such as the definition of "personal data breach", "pseudonymization", "data concerning health" and the definition of "consent of the data subject".

5. What principles apply to the processing of personal data in your jurisdiction? For example: is it necessary to establish a "legal basis" for processing personal data?; are there specific transparency requirements?; must personal data only be kept for a certain period? Please provide details of such principles.

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 data subject (the individual whose data is processed). Lastly, the principle requires that personal data is processed in a transparent way in the meaning that the data subject shall be informed about the processing. The principle of transparency therefore has a connection to the data subject's right to information. For more information about the specific requirements on information to the data subject, please see question 16.

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 accountability, 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 processing of personal data? 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)?

Consent is one of the legal grounds which can form a basis for processing of personal data according to the EU regulation 2016/679 (the **General Data Protection Regulation**, **"GDPR"**).. 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.

For a consent to be valid, certain criteria must be met:

- It must be freely given,
- It must be informed,
- It must be given for a specific purpose,
- All the reasons for the processing of personal data must be clearly stated,
- It must be explicit and given via a positive act by the data subject (i.e. it is not sufficient to provide a pre-ticked box, but the data subject must tick the box him-/herself,
- It must use clear and plain language and be clearly visible,
- It must be possible to withdraw the consent.

7. What special requirements, if any, are required for processing particular categories of personal data (e.g., health data, children's data, special category or sensitive personal data, etc.)? Are there any prohibitions on specific categories of personal data that may be collected, disclosed, or otherwise processed?

As a principal rule, processing of special categories of personal data ("sensitive 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.

8. Do the data protection laws in your jurisdiction include any derogations, exemptions, 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.

9. Does your jurisdiction require or recommend risk or impact assessments in connection with personal data processing activities and, if so, under what circumstances? How are these assessments typically carried out?

If a processing activity, in particular when 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 (a so-called data protection impact assessment ("DPIA"). A DPIA must be carried out before starting the processing activity.

There are three specific cases mentioned which by default require 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 personal 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 of the GDPR 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.

10. Are there any specific codes of practice applicable in your jurisdiction regarding the processing of personal data (e.g., codes of practice for processing children's data or health data)?

There are no established codes of practice applicable regarding data processing. However, the Swedish Authority for Privacy Protection has drafted practical guidance on for example the process for carrying out a DPIA which can be used within an organization on a voluntary basis.

11. Are organisations required to maintain any 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. In practice, many organisations are within scope of this requirement, at least for processing activities that are not occasional, such as processing of personal data for salary payments.

12. 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 4, 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.

13. Under what circumstances is it 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.

14. Do the data protection laws in your jurisdiction require the appointment of a data protection officer, chief information security officer, or other person responsible for data protection? If so, 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. Is 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 to provide information and advise 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 to appoint 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.

15. 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) or recommendation(s).

There are no explicit legal requirements or recommendations 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, is 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 advise 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 applies as of 17 January 2025.

16. 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 obtained from the data subject, generally the same information requirements apply as for the situation above. There is no explicit requirement on how the information shall be given, other than that it should be provided in writing. 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 19. 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.

17. Do the data protection laws in your jurisdiction draw any distinction between the responsibility of controllers and the processors of personal data? If so, what are the implications?

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 activities performed by the processor on the controller's behalf.

18. 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 or any similar terms defined?

Under 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., controllers must establish the legal ground for processing, and adhere to the data protection principles set out in the GDPR. 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 their consent to the website's use of cookies. A valid consent must meet the higher standards of consent stated in the GDPR, described above. It is not sufficient to collect a "passive consent" through pre-ticked boxes and pre-defined statements in privacy policies. However, the above does not prevent the website holder from performing such storage or access activity that is necessary to transmit an electronic 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 according to 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.

19. Please describe any restrictions on targeted advertising and/or 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 targeted advertising). The use of cookies requires consent from the website visitor. Cookies are considered personal data if they can be used to identify visitors at a website, e.g. by being combined with an IP address. If so, EU regulation 2016/679 (the **General Data Protection Regulation**, **"GDPR"**) applies and the requirements regarding consent and legitimate interest must be met.

20. Please describe any data protection laws in your jurisdiction restricting the sale of personal data. How is the term "sale" or such related

terms defined?

Processing of personal data according to the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**) is a broad term and the sale of personal data is considered a processing activity. Sale of personal data is therefore governed by the same requirements in the GDPR as any other processing, i.e. legal basis must be established, information requirements must be met, etc. There is no specific national legislation targeting the sale of personal data.

21. Please describe any data protection laws in your jurisdiction restricting telephone calls, text messaging, email communication, or direct marketing. How are these terms defined?

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 prior sales of products 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 (that the person has previously 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 meets the requirements 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.

22. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined?

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 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 data protection impact assessment ("DPIA") to ensure whether the intended processing is lawful and, if necessary, initiate a prior consultation with the Swedish Authority for Privacy Protection.

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

EU Regulation 2024/1689 ("**AI Act**") lays down harmonized rules on artificial intelligence in the EU. The AI Act entered into force on 1 August 2024 as a regulation, but its articles enter into force gradually during 2025. The AI Act sets out risk-based rules for AI developers and deployers regarding specific uses of AI, and defines four levels of risk for AI systems. These levels are:

- Unacceptable risk. AI systems that are categorized within this risk level are prohibited.
- High risk. These AI systems are subject to strict obligations.
- Limited/transparency risk. This risk level refers to risks associated with a need for transparency regarding the use of AI in the system.
- Minimal risk. These types of AI systems are not covered by any rules under the AI Act.

24. 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 the Commission has assessed that 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 results in that transfers to organizations certified under the EU-US Data Privacy Framework is permitted (an exhaustive list of certified companies can be found at www.dataprivacyframework.gov). However, the adequacy decision does not mean that the transfer of personal data to US cloud service providers is unrestricted, as they typically also have operations and recipients in other countries. There has also been recent debate on whether the adequacy decision will last, in light of certain changes made by the current president of the U.S.

25. What personal data security obligations are imposed by the data protection laws in your jurisdiction?

In accordance with the EU regulation 2016/679 (the **General Data Protection Regulation, "GDPR"**), data controllers and data processors are obligated to 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.

Examples of technical and organizational security measures include 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 are subject to specific requirements.

26. Do the data protection laws in your jurisdiction impose obligations in the context of security breaches which impact personal data? If so, how do such laws define a security breach (or similar term) and under what circumstances must such a breach be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

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.

27. Do the data protection laws in your jurisdiction establish specific rights for individuals, 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, and any exceptions.

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, as a main rule, obligated to respond no later than within one month.

The rights of the data subject are the following:

- 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 restrict 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 merely constitutes a memory note.

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 necessary 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.

28. 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 with the Swedish Authority for Privacy Protection but also bring 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.

29. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual and material damage to have been sustained, or is non-material 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 compensation.

30. How are data protection laws in your jurisdiction typically 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.

31. 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.

32. 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.

33. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

Yes, enforcement decisions made by the Swedish Authority for Privacy Protection can be appealed to the court within 21 days counted from the day when the plaintiff was made aware of the decision by the authority. The authority's decision-making process can also be challenged by submitting a complaint to the judicial ombudsman.

34. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

As of 2023, the Swedish Authority for Privacy Protection received increased resources from the government, which has shown 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 2024, the Swedish Authority for Privacy Protection initiated 415 inspections in the form of supervision, a significant increase from 207 the previous year. The authority decided on penalty fees in a total of five supervisory cases amounting to SEK 60 580 000. The amount of cases as well as the total fees are lover than the previous year, since the authority focused on complaint based inspections, which resulted in fewer penalty fees being issued.

During 2025, the Swedish Authority for Privacy Protection plans to focus on AI, digitalization within healthcare, protection for children and young individuals, employers' processing of employees' personal data and camera surveillance.

35. Do the cybersecurity laws in your jurisdiction require the implementation of specific cybersecurity risk management measures and/or require that organisations take specific actions relating to cybersecurity? If so, please provide details.

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**.

On October 17, 2024 the EU directive 2022/2555 (the **NIS2 Directive**) became applicable and replaces the **NIS Directive**. However the Swedish act implementing the NIS2 Directive is belated and the **Swedish Act on information security for essential and digital services** is therefore still in force. The NIS2 Directive imposes specific security requirements on certain public or private entities in 18 different sectors referred to in the directive and stipulates obligations for the member states to adopt national cybersecurity strategies and cyber security risk management measures as well as reporting obligations for entities. The directive applies to private and public entities in sectors of high criticality and other critical sectors. Actions are being taken by the Swedish legislator to implement this directive into Swedish law. The implementing law is expected to enter into force during autumn 2025.

On 17 January 2025 the EU regulation 2022/2554 (**Digital**

Operational Resilience Act, "**DORA**") became applicable. The purpose of DORA is to make entities in the financial sector, including insurance companies and third-party service providers, strengthen their resilience against information and communication related (ICT) disruptions and threats. DORA requires implementation of a variety of risk management measures.

36. Do the cybersecurity laws in your jurisdiction impose specific requirements regarding supply chain management? If so, please provide details of these requirements.

The **NIS 2 Directive** stipulate obligations for the member states to adopt national laws that ensure that essential and important entities tape appropriate and technical, operational and organizational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimize the impact of incidents on recipients of their services and on other services. These measures shall include supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.

DORA incorporates several provisions addressing supply chain transparency and risk assessments regarding third-party information and communication technology, ICT, service providers. Dora thus requires financial entities in the EU to identify and handle ICT risks associated with third-party ICT service providers, among other things through extensive provisions on contractual arrangements between the financial entities and third-party ICT service providers.

37. Do the cybersecurity laws in your jurisdiction impose information sharing requirements on organisations?

The **NIS 2 Directive** lays down measures that aim to achieve a high common level of cybersecurity across the EU, with a view to improving the functioning of the internal market. To that end the Directive lays down rules and obligations on cybersecurity information sharing, among other between computer security incident response teams in each EU member state and rules imposed on the member states to support voluntary cybersecurity information sharing between entities in accordance with Union law.

According to **DORA** financial entities should be encouraged to exchange among themselves cyber security threat information and intelligence, and to collectively leverage their individual knowledge and practical experience with a view to enhancing their capabilities to adequately assess, monitor, defend against, and respond to cyber threats, by participating in information sharing arrangements. Dora thus lays down requirements on information and intelligence sharing in relation to cyber threats and vulnerabilities.

38. Do the cybersecurity laws in your jurisdiction require the appointment of a chief information security officer, regulatory point of contact, or other person responsible for cybersecurity? If so, what are their legal responsibilities?

There currently is not any requirement to appoint a chief information security officer, a regulatory point of contact, or other designated person responsible for cybersecurity in the **NIS Directives** or the **DORA** regulation.

39. Are there specific cybersecurity laws / regulations for different industries (e.g., finance, healthcare, government)? If so, please provide an overview.

The **Act on information security for essential and digital services** imposes specific cyber 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 2 Directive** cover the same industries as the NIS Directive, but also covers waste water, ICT service management, public administration, space, postal and courier services, research, waste management, manufacture, production and distribution of chemicals, manufacturing, digital providers and production, processing and distribution of food while **DORA** covers the financial market.

40. What impact do international cybersecurity standards have on local laws and regulations?

Since the Swedish legal framework for data protection, privacy and cybersecurity is primarily governed by EU law the cybersecurity standards of these laws have a great impact on the local Swedish laws and regulations.

41. Do the cybersecurity laws in your jurisdiction

impose obligations in the context of cybersecurity incidents? If so, how do such laws define a cybersecurity incident and under what circumstances must a cybersecurity incident be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

The **Swedish Act on information security for essential and digital services** does impose obligations regarding incidents related to network and information systems. An incident is defined as an event with an actual negative impact on the security of networks and information systems. According to the Swedish Act on information security for essential and digital services essential service providers and providers of digital services shall take appropriate action to prevent and minimize the impact of incidents that affect network and information systems, in order to ensure continuity of their services. The essential service providers and providers of digital services are also required to report incident that have a significant impact on the continuity of the essential service or digital service that they provide to the relevant competent authority.

DORA imposes requirements for reporting major ICT-related incidents and notifying, on a voluntary basis, significant cyber threats to the competent authorities, and reporting of major operational or security payment-related incidents to the competent authorities by certain financial entities such as credit institutions and payment institutions. In the DORA-regulation there are multiple definitions of different kinds of incidents related to ICT and cybersecurity. For example an "ICT-related incident" is defined as a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity. "Cyber threat" is defined as any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons, while a "significant cyber threat" is defined as a cyber threat the technical characteristics of which indicate that it could have the potential to result in a major ICT-related incident or a major operational or security payment-related incident. "Cyber-attack" is defined as a malicious ICT-related incident caused by means of an attempt perpetrated by any threat actor to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. Financial entities shall have in place crisis communication plans enabling a disclosure of at least major ICT-related incidents to clients and counterparts as well as to the public, as appropriate. The financial entities shall also report major ICT-related incidents to the relevant competent authority. Where a major ICT-related incident occurs and has impact on the financial interests of clients, financial entities shall, without undue delay inform their clients about the incident and about the measures that have been taken to mitigate the adverse effects of such incident. Financial entities may, on a voluntary basis, notify significant cyber threats to the relevant competent authority when they deem the treat to be of relevance to the financial system, service users or clients. In case of significant cyber threat, financial entities shall also inform, where applicable, their clients that are potentially affected of any appropriate protection measures which the latter may consider taking.

42. How are cybersecurity laws in your jurisdiction typically enforced?

Six different Swedish supervisory authorities, among them The Swedish Financial Supervisory authority, supervise and enforce the **Swedish Act on information security for essential and digital services**. The supervisory authorities have different investigative powers and have the authority to impose various measures, such as reprimands, orders or fines.

In accordance with **DORA** the Swedish Financial Supervisory Authority 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 financial entities to provide information and conducting investigations/audits including access to premises. Thus the Swedish Financial Supervisory Authority supervises and enforces **DORA** and the **Act with Supplementary Provisions to the EU's Regulation on digital operational resilience for the financial sector** and has the authority to impose various measures, such as reprimands, orders or fines on the financial entities affected by these legal acts.

43. What powers of oversight / inspection / audit do regulators have in your jurisdiction under cybersecurity laws.

Same as above.

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

The Swedish Supervisory Authorities may issue remarks, warnings and impose administrative fines. The action to be taken or the amount of the fines is much dependant on what kind of entity that has committed the violation and the nature and severity of the violation at hand. The fine can therefore amount from 5 000 SEK (approximately 500 EUR) to ten percent of the company´s annual turnover or of the annual turnover at group level.

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.

According to DORA, the authority determining the type and level of an administrative penalty or remedial measure should take into account the extent to which the breach is intentional or results from negligence, and all other relevant circumstances, including the following, where appropriate: (a) the materiality, gravity and the duration of the breach; (b) the degree of responsibility of the natural or legal person responsible for the breach; (c) the financial strength of the responsible natural or legal person; (d) the importance of profits gained or losses avoided by the responsible natural or legal person, insofar as they can be determined; (e) the losses for third parties caused by the breach, insofar as they can be determined; (f) the level of cooperation of the responsible natural or legal person with the competent authority, without prejudice to the need to ensure disgorgement of profits gained or losses avoided by that natural or legal person; (g) previous breaches by the responsible natural or legal person.

46. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

Enforcement decisions are open to appeal a decision made by any of the supervisory authorities to the court within 21 days 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 or regulatory priorities in enforcement activity in your jurisdiction?

Since **DORA** has come in to force in January 2025 the Swedish Financial Supervisory Authority will most likely initiate inspections or other kinds of investigations on the enforcement of the new legislation in the financial entities under its supervision.

When it comes to the implementation of the **NIS 2 Directive** in Swedish national law, it still remains to be seen when the implementation will be finalized.

Contributors

Anna Lööv
Lawyer and Managing Partner, Head of Data Protection and Finance Regulatory
anna.loov@kompassadvokat.se

Mina Gholiof Roa
Lawyer and Senior Associate
mina.gholiof@kompassadvokat.se

Johanna Borg
Senior Associate
johanna.borg@kompassadvokat.se

Lisa Nordbeck
Associate
lisa.nordbeck@kompassadvokat.se