



The Legal
500 &
The In-
House
Lawyer

Comparative Legal Guide

Sweden: Data Protection & Cyber Security

This country-specific Q&A provides an overview to data protection and cyber security laws and regulations that may occur in Sweden.

This Q&A is part of the global guide to Data Protection & Cyber Security. For a full list of

jurisdictional Q&As

visit <http://www.inhouselawyer.co.uk/practice-areas/data-protection-cyber-security/>

Country Author:
Advokatfirman Delphi

The Legal 500



Peter Nordbeck, Partner / Advokat

peter.nordbeck@delphi.se

The Legal 500



Rebecka Harding, Senior Associate / Advokat

rebecka.harding@delphi.se



Felix Makarowski, Associate

felix.makarowski@delphi.se



Christina Björn, Associate


christina.bjorn@delphi.se

1. **Please provide an overview of the legal framework governing privacy 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 laws enforced)?**

One key law governing privacy in Sweden is the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (the “**GDPR**”), which is directly applicable in Sweden.

It regulates the processing of personal data wholly or partly by automated means and the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. The GDPR applies to all Swedish establishments which process personal data in their capacity as controller (i.e. 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) or processor (i.e. a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller), regardless of in which country the processing takes place. Exemption from the GDPR’s material scope includes for example processing of personal data by a natural person in the course of a purely personal or household activity.

Two key laws in Sweden which complement the GDPR are the Act containing supplementary provisions to the EU General Data Protection Regulation (*sw. Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning*) (the “**Data Protection Act**”) and the Ordinance containing supplementary provisions to the EU General Data Protection Regulation (*sw. Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning*) (the “**Data Protection Ordinance**”).



The Data Protection Act essentially applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in Sweden. The Data Protection Act and the Data Protection Ordinance inter alia regulate Sweden's implementation of the areas where the GDPR allows flexibility for the individual EU member states to further specify and supplement the GDPR's provisions, such as age of consent in relation to information society services as well as the lawfulness of processing special categories of personal data and personal data relating to criminal convictions and offences. They also contain provisions regarding enforcement of sanction decisions and the role of the supervisory authority.

The supervisory authority for the GDPR, the Data Protection Act and the Data Protection Ordinance is the Swedish Data Protection Authority (*sw. Datainspektionen*).

It is also worth mentioning that Sweden in general has a long tradition of sector specific legislation governing privacy, such as for example the Patient Data Act (*sw. Patientdatalag (2008:355)*) which govern processing of personal data within health and medical care. Such sector specific legislation has been adapted with regard to the GDPR. Generally, such sector specific legislation complement the GDPR but the GDPR has priority.

Finally, there are certain central laws which do not specifically govern privacy but which are closely related and sometimes complement and/or overlap with Swedish privacy laws such as for example:

- the Electronic Communications Act (*sw. Lag (2003:389) om elektronisk kommunikation*) (the "**Cookie Act**");

- the Act on Information Security regarding providers of critical infrastructure and digital services (sw. *Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster*) (the "NIS Act"); and
- the Ordinance Information Security regarding providers of critical infrastructure and digital services (sw. *Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster*) (the "NIS Ordinance"),

which will be described in more detail below.

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

Are there any exemptions?

There are no registration or licensing requirements under the GDPR, the Data Protection Act or the Data Protection Ordinance.

3. How do these laws define personally identifiable information (PII) versus sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

The terms personally identifiable information (PII) and sensitive PII are not used. Instead, key definitions are personal data and special categories of personal data. Both of these terms are defined in article 4 of the GDPR.

The term "personal data" is defined in article 4 of the GDPR as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number,*

location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

The term “special categories of personal data” is explained in article 9 of the GDPR as “Processing of 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 shall be prohibited”.

Other key definitions which are defined in article 4 of the GDPR are controller, processor and processing.

The term “controller” is defined as “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”.

The term “processor” is defined as “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”.

The term “processing” is defined as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by

transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.

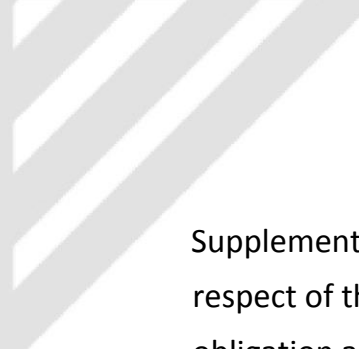
4. Are there any restrictions on, or principles related to, the general processing of PII – for example, must a covered entity establish a legal basis for processing PII in your jurisdiction or must PII only be kept for a certain period? Please outline any such restrictions or “fair information practice principles” in detail?

Yes, there are restrictions on, and principles related to, the general processing of personal data.

The controller must always have lawful basis in order to process personal data. Article 6 of the GDPR outlines the following six (6) available lawful bases for the general processing of personal data:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Which basis is most appropriate to use will depend on the controller’s purpose of the processing and relationship with the data subject.



Supplementary provisions are found in the Data Protection Act, which state in respect of the lawful bases in article 6(1)(c) and 6(1)(e) of the GDPR, that the legal obligation and public interest respectively, must follow from statute, collective bargaining agreement or decision based on statute.

The controller must also make sure that its processing of personal data complies with the following six (6) principles relating to processing of personal data (article 5(1) of the GDPR):

- Lawfulness, fairness and transparency: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;
- Purpose limitation: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Data minimisation: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accuracy: Personal data 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;
- Storage limitation: Personal data 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 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 subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject;
- Integrity and confidentiality: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5. Are there any circumstances where consent is required or typically used in connection with the general processing of PII and, if so, are there are rules relating to the form, content and administration of such consent?

Neither the GDPR, the Personal Data Act nor the Personal Data Ordinance require a controller to use consent in connection with the general processing of personal data.

It is worth mentioning that many avoid using consent as the lawful base because:

- the GDPR's stringent consent requirements (the term "consent" is defined in article 4 of the GDPR as "*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*"); and
- the data subject has the right to withdraw his or her consent at any time (article 7(3) of the GDPR).

Chapter 6 paragraph 18 of the Cookie Act on the other hand stipulates that a website with cookies must obtain consent from its visitors to the cookies being used, unless the cookie is necessary to transmit an electronic message via an electronic communications network or to provide a service explicitly requested by visitor. The consent requirements should correspond to the consent requirements in the GDPR (see above). However, in reality, consent is usually obtained through the visitor's browser settings.

See also question 7 regarding age of consent and question 24 regarding profiling.

6. **What special requirements, if any, are required for processing sensitive PII? Are there any categories of PII that are prohibited from collection?**

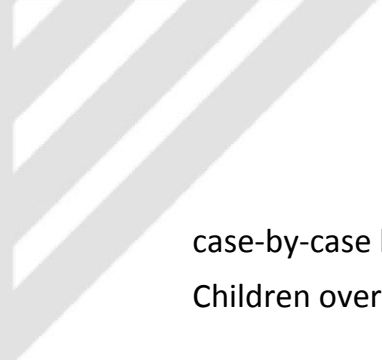
Processing of special categories of personal data is as a rule prohibited, unless one of the available lawful bases for the processing of special categories of personal data applies (article 9 of the GDPR). Examples of such lawful bases:

- The explicit consent of the data subject was obtained.
- The data is required for the establishment, exercise or defence of legal claims.
- The personal data was manifestly made public by the data subject.

7. **How do the laws in your jurisdiction address children's PII?**

The only explicit difference that is made between processing of personal data related to children and adults in data protection legislation concerns age of consent in relation to information society services (chapter 2, paragraph 4 of the Data Protection Act). More specifically that when a controller offer an information society service to children and processes their personal data on the basis of consent, only children aged 13 or over are able to provide their own consent (unless the online service is a preventive or counselling service). For children under the age of 13 consent must instead be obtained from whoever holds parental responsibility for the child.

Moreover, the Swedish Data Protection Authority has expressed that although there are no other explicit age of consent than the above mentioned, a controller must always ensure that the child understands what it is it consents to in order for the consent to be valid. The Swedish Data Protection Authority has therefore recommended that a controller always should obtain consent from whoever holds parental responsibility if the child is under the age of 13 and should assess on a



case-by-case basis if a child between the age of 13 and 16 can give a valid consent. Children over the age of 16 should however usually be able to give a valid consent.

8. **Are owners or processors of PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.**

Yes, according to article 30 of the GDPR controllers as well as processors are required to maintain a record in writing, including in electronic form. Article 30 stipulates all the information that the record shall contain such as for example the purposes of the processing, a description of the categories of data subjects and of the categories of personal data and, where possible, the envisaged time limits for erasure of the different categories of data.

The obligation to maintain a record does however not apply to an enterprise or an organisation 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 special categories of data or personal data relating to criminal convictions and offences.

It varies how businesses typically meet the requirement, many use a simple Excel-sheet to meet the requirement.

9. **Are consultations with regulators recommended or required in your jurisdiction and in what circumstances?**


According to article 36 of the GDPR, the controller is required to consult the Swedish Data Protection Authority prior to processing where a so-called data protection impact assessment (see explanation of what this means below under question 10) indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

10. **Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?**

Yes, according to article 35 of the GDPR, a controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (data protection impact assessment) where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.

The data protection impact assessment shall contain at least:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.



The Swedish Data Protection Authority further has upheld the principle that a risk- and vulnerability analysis must be conducted prior to entering into a cloud computing contract. It is somewhat unclear whether this principle will still be upheld by the Swedish Data Protection Authority, following the entering into force of the GDPR.

In addition to the above, some organisations must also take into account the NIS Act and the NIS Ordinance.

In short, the NIS Act and the NIS Ordinance implement the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (the “**NIS directive**”) in Sweden.

The NIS Act and the NIS Ordinance apply to both:

- operators of essential services (such as for example operators in the following sectors banking, health sector, transport, energy) who are established in Sweden, which provision of the essential service is dependent on network and information systems and where an incident would have a significant disruptive effect on the provision of the service, and
- digital service providers who has its main establishment in Sweden or has appointed a representative which is established in Sweden.

The NIS Act and the NIS Ordinance explicitly requires operators of essential services to carry out a risk analysis which shall form the basis for the choice of the operators of essential services’ security measures in relation to networks and information systems that they use to provide essential services. The analysis shall include an action plan, be documented and updated annually.

The NIS Act also indirectly requires digital service providers to carry out a risk analysis. This as digital service providers are required to, in relation to the risk at

hand, take appropriate and proportionate technical and organisational measures to manage risks that threaten the security in the networks and information systems that they use.

11. Do the laws in your jurisdiction require appointment of a data protection officer, or other person to be in charge of privacy or data protection at the organization? What are the data protection officer's legal responsibilities?

Yes, according to article 37 of the GDPR, the controller and the processor shall designate a so-called data protection officer in any case where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

There are no additional cases where a data protection officer must be designated in the Data Protection Act or the Data Protection Ordinance.

The data protection officer shall be involved in all issues which relate to the protection of personal data. The data protection officer shall at least have the following tasks:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the GDPR and to other Union or Member State data protection provisions;
- to monitor compliance with the GDPR, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of

personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

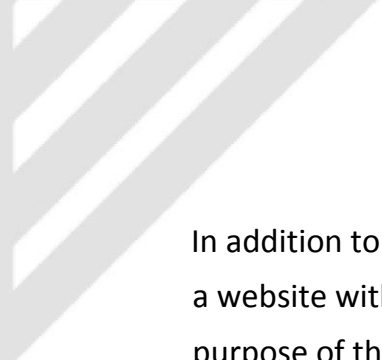
- to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to article 35 of the GDPR;
- to cooperate with the supervisory authority; and
- to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation described under question 9, and to consult, where appropriate, with regard to any other matter.

12. Do the laws in your jurisdiction require providing notice to individuals of the business' processing activities? If so, please describe these notice requirements (e.g. posting an online privacy notice).

Yes, according to articles 13 and 14 of the GDPR, the controller is required to provide data subjects with notice of its processing activities, such as identity and contact details of the controller and the purposes as well as the legal basis for the processing.

The information to provide the data subjects with varies to some extent depending on whether the personal data have been obtained from the data subject or not. Further, information shall under certain conditions be provided to the data subject in case of a data breach or other personal data incidents.

The information to the data subject shall be provided in an easily accessible, written form in a clear and simple language. Many chose to provide the information by posting an online privacy notice and include hyperlinks to the notice in for example its email signatures and marketing messages.



In addition to the above, chapter 6 paragraph 18 of the Cookie Act stipulates that a website with cookies must always provide its visitors with information about the purpose of the cookies being used, regardless of what data the cookies collect. This information is normally provided by posting a so-called cookie policy on the website.

13. **Do the laws in your jurisdiction apply directly to service providers that process PII, or do they typically only apply through flow-down contractual requirements from the owners?**

The GDPR is most often directly applicable to processors that process personal data although the controller is responsible for making sure, and be able to demonstrate compliance with, all privacy principles described under question 4 are adhered to.

Further, the Data Protection Act is to a limited extent also applicable to processors. The Data Protection Ordinance is however not applicable to processors.

14. **Do the laws in your jurisdiction require minimum contract terms with service providers or are there any other restrictions relating to the appointment of service providers (e.g. due diligence or privacy and security assessments)?**

Yes, according to article 28 of the GDPR, a controller's appointment of a processor shall be governed by a contract (so-called data processing agreement) or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter, including details about the processing which the processor shall carry out (duration, nature and

purpose of the processing, the type of personal data and categories of data subjects) and the obligations and rights of the controller (article 28(3) of the GDPR).


Further, if a controller wants to appoint a processor, the controller must make sure to only appoint such processors who can provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject (article 28(1) of the GDPR).

15. **Is the transfer of PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (for example, does cross-border transfer of PII require notification to or authorization from a regulator?)**

Yes, the transfer of personal data outside the EU and European Economic Area (EEA) is restricted. Such transfer is only permitted if:

- There is a decision from the European Commission that, for example, a certain country outside the EU/EEA ensures an adequate level of protection;
- Appropriate protection measures has been taken, for example Binding Corporate Rules (BCR) or Standard Contractual Clauses (SCC); or
- Special situations and single cases.

Among the countries that, according to the European Commission, have an adequate level of protection, the European Commission has also assessed that the level of protection is adequate in US if the recipient has joined the so-called



Privacy Shield Network. This is however currently being tried by the European Court of Justice.

There are no requirements to notify or obtain consent for the cross border transfer from the Swedish Data Protection Authority.

16. **What security obligations are imposed on PII owners and on service providers, if any, in your jurisdiction?**

According to article 32 of the GDPR, both the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

In addition to the above, the NIS Act requires operators of essential services (in relation to networks and information systems that they use to provide essential services) and digital service providers (in relation to networks and information systems that they use), to take appropriate and proportionate technical and organisational measures to manage risks that threaten the security as well as take measures to prevent and minimize the impact of incidents.

The NIS Ordinance stipulates that when digital service providers assess whether a security measure ensures a level of security in networks and information systems that is appropriate in relation to the risk, they must take into account inter alia the security in systems and installations, incident management as well as monitoring, auditing and testing.

17. **Does your jurisdiction impose requirements of data protection by design or default?**

Yes, the GDPR impose requirements of data protection by design or default. The requirements imply, amongst others, that the controller shall through the whole life cycle of a product/solution implement appropriate technical and organisational measures which are designed to implement data protection principles and integrate the necessary safeguards into the processing.

18. **Do the laws in your jurisdiction address security breaches and, if so, how does the law define “security breach”?**

The term security breach is not used. Instead, the term personal data

breach is used in the GDPR and the term incident is used in the NIS Act.

The term “personal data breach” is defined in article 4 of the GDPR as *“a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”*.

The term “incident” is defined paragraph 2 of the NIS Act as *“an event having an actual adverse effect on the security of network and information systems”*.

19. **Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?**

According to article 33 of the GDPR, the controller is required to notify a personal data breach to the Swedish Data Protection Authority no later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The controller is typically also required to communicate the personal data breach to the data subject without undue delay, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons (article 34 of the GDPR).

Further, the NIS Act and the NIS Ordinance require operators of essential services to, without undue delay, notify incidents having a significant impact on the continuity of the essential services they provide and digital service providers to, without undue delay, notify incidents having a substantial impact on the provision of a digital service which they offer within the EU. Such incident reports shall be reported to the Swedish Civil Contingencies Agency. The time limits to report such incidents has been further specified by the Swedish Civil Contingencies Agency, according to the following:

- The operators of essential services/digital service providers shall within six (6) hours from identification of an incident which must be reported, report it and include information about inter alia concerned service, description of the incident, the disorder and consequences.
- The operators of essential services/digital service providers shall within 24 hours from identification of an incident which must be reported, provide the Swedish Civil Contingencies Agency with information about measures to minimise the consequences of the incident.
- The operators of essential services/digital service providers shall within four (4) weeks provide the Swedish Civil Contingencies Agency with information about measures that have been taken and how they will prevent future incidents.

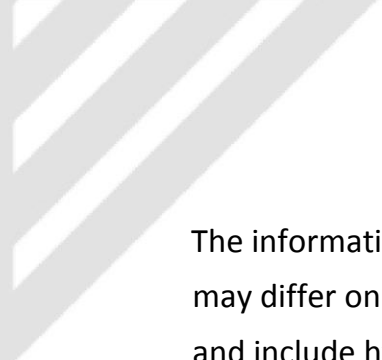
20. **Do the laws in your jurisdiction provide individual rights, such as the right to access and the right to deletion? If so, please provide a general description on what are the rights, how are they communicated, what exceptions exist and any other relevant details.**

Yes, the data subject has several rights under GDPR such as:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restriction of processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

Right to be informed (articles 13 and 14 of the GDPR)

The controller is required to provide data subjects with certain information, such as identity and contact details of the controller and the purposes as well as the legal basis for the processing. The information to provide the data subjects with varies to some extent depending on whether the personal data have been obtained from the data subject or not. When personal data is obtained directly from the data subject, then the data subject shall be informed immediately, i.e. at the time the personal data is collected. Otherwise, the data subject shall be informed within a reasonable period of time, but at latest after one (1) month. If the data are to be used for communication with the data subject or if a disclosure to another recipient is envisaged, then the data subject shall be informed at the latest at the time of the first communication to that data subject or when the personal data are first disclosed.



The information shall be provided to the data subject in a suitable manner, which may differ on a case-by-case basis. Many chose to post an online privacy notice and include hyperlinks to the notice in for example its email signatures and marketing messages.

The information to the data subject shall be provided in an easily accessible, written form in a clear and simple language.

Right of access (article 15 of the GDPR)

The data subject has the right to request a register extract from a controller that processes the data subject's personal data. The controller shall inform the data subject whether it processes personal data or not, and if so, the register extract shall, among other things, include information on the purposes of the processing, the categories of personal data processed, the recipients or categories of recipients etc. The information must be provided without undue delay but at latest within one (1) month if there is not an exception.

Right to rectification (article 16 of the GDPR)

The data subject has the right to contact the controller and request that information that is inaccurate shall be rectified. Furthermore, this also means that the data subject has the right to add such personal data that is missing and that is relevant taking into account the purpose of the processing of personal data.

Right to erasure (article 17 of the GDPR)

The right is also known as “the right to be forgotten” and the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay. This right is not an absolute right, the personal data is to be erased only if one of the grounds stipulated in article 17 of the GDPR applies, such as for example if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed or the personal data have been unlawfully processed.

Right to restriction of processing (article 18 of the GDPR)

The data subject has the right to demand the controller to restrict the processing of their personal data in some cases. The right to restriction applies, among other things, when the data subject considers that the data is inaccurate and has requested rectification. In such cases, the data subject may request to restrict the processing of their personal data during the investigation of the accuracy of the data. Where the processing has been restricted, the personal data may only be processed for certain limited purposes.

Right to data portability (article 20 of the GDPR)

The data subject shall in certain cases have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, e.g. from a social media service to another where the data subject him- or herself has provided the controller with its personal data.

Right to object (article 21 of the GDPR)

In certain cases, the data subject has the right to object to his or her personal data being used. The controller may only continue to process the personal data if it can demonstrate compelling legitimate grounds for the processing which override the interest, right and freedoms of the data subject or if the processing is carried out for the establishment, exercise or defence of legal claims.

Furthermore, the data subject always has the right to object to his or her personal data being used for direct marketing and such objections can be made at any time. If such objection is made, the personal data may no longer be processed for such purposes.

Where personal data is processed for scientific, historical or statistical research purposes, other rules apply.

Rights in relation to automated decision making and profiling (article 22 of the GDPR)

The data subject shall have the right to not be subject of a decision solely based on some form of automated decision-making, including profiling, if the decision produces legal effects concerning him or her or similarly significantly affects him or her. However, automated decision-making may be permitted if it is necessary to enter into or performance of an agreement between the data subject and the controller or if the data subject has given its explicit consent. There may also be special legislation that permits such automated decision-making.

The controller shall inform the data subject if automated decision-making is used.

21. **Are individual rights exercisable through the judicial system or enforced by a regulator or both? When exercisable through the judicial system, does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances? Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury of feelings sufficient?**

Yes, individual rights are exercisable both through the judicial system and enforced by the Swedish Data Protection Authority.

Each natural and legal persons have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (article 78 of the GDPR).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (article 79 of the GDPR).

The possibility to bring private claims against controllers and processor appear from article 82(1) of the GDPR which stipulates that any person who has suffered "material or non-material damage" because of a breach of the GDPR have the right to receive compensation from the controller or processor. The inclusion of "non-material" damage means that it is possible to also claim compensation for distress although no financial loss can be proven.

Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (article 80 of the GDPR).

Data subjects also enjoy the right to lodge a complaint with a supervisory authority (article 77 of the GDPR). This right is without prejudice to any other administrative or judicial remedy.

Finally, the Swedish Data Protection Authority can also initiate a supervisory matter and within the framework of such matter enforce data subjects' rights.

22. How are the laws governing privacy and data protection enforced? What is the range of fines and penalties for violation of these laws? Can PII owners appeal to the courts against orders of the regulators?

The Swedish Data Protection Authority can impose administrative fines of up to EUR 20 million, or in the case of an undertaking, up to four (4) percent of the total worldwide annual turnover of the preceding financial year, whichever is higher.

For less serious violations, the Swedish Data Protection Authority can impose administrative fines of up to EUR 10 million or, in the case of an undertaking, up to two (2) percent of total worldwide turnover of the preceding year, whichever is the higher.

Public authorities may also be fined, up to SEK 10 million for serious infringements and SEK 5 million for less serious infringements.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (article 83(1) of the GDPR). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be taken into consideration, among other things, how serious the

infringement is, how much harm has been caused, if sensitive personal data is involved, and if the infringement is intentional.

Fines can be imposed in combination with other corrective powers.

The decisions of the Swedish Data Protection Authority may be appealed to the Swedish Administrative Court.

23. **Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.**

Yes, the Data Protection Act stipulates certain further limitations on how processing of personal data may be carried out, namely in relation to processing of personal data relating to criminal convictions and offences as well as personal identity numbers and coordination numbers.

The general rule is that only authorities may process personal data relating to criminal convictions and offences. Others than authorities must have a lawful basis in the Data Protection Ordinance or in regulations or decision from Swedish Data Protection Authority to be able to process personal data. It is currently unclear if criminal convictions and offences also includes suspicion of a crime and the Swedish Data Protection Authority has expressed that it will provide more guidance on this later.

Personal identity numbers and coordination numbers may only be processed if the data subjects have given their consent or when it is clearly motivated taking into consideration the purpose of the processing, the importance of an accurate identification or any other considerable reason.

24. **Please describe any restrictions on monitoring or profiling in your jurisdiction including the use of tracking technologies such as cookies – how are these terms defined and what restrictions are imposed, if any?**

The term monitoring is not used. Nevertheless, the term profiling is used and it is defined in article 4 of the GDPR as *“any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements”*.

According to article 22 of the GDPR, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, unless the decision.

- is necessary for entering into, or performance of, a contract between the data subject and a controller;
- is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- is based on the data subject's explicit consent.

Further, the decision may typically not be based on special categories of personal data and the controller must under certain circumstances implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests to express his or her point of view and to contest the decision.

Not all profiling falls however under article 22 of the GDPR. Regarding such profiling that falls outside article 22 of the GDPR's scope it is debated whether consent must be obtained or not from the data subject.

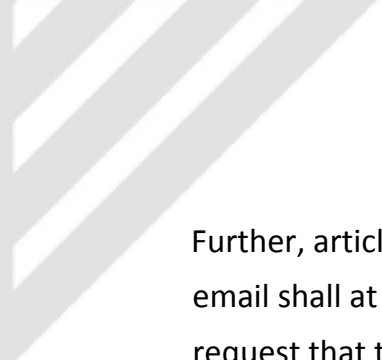
Finally, chapter 6 paragraph 18 of the Cookie Act stipulates that data from cookies may only be stored in or retrieved from a visitor of a website's terminal equipment if the visitor is provided with information about the purpose of the processing and consents to it. This does however not prevent such storage or access that as is necessary to transmit an electronic message via an electronic communications network or provide a service explicitly requested by the visitor.

25. **Please describe any laws addressing email communication or direct marketing?**

Apart from the GDPR's rules on processing of personal data, the Swedish Marketing Act (*sw. Marknadsföringslag (2008:486)*) is applicable when sending direct marketing. Most of the Swedish Marketing Act's rules on direct marketing only apply to marketing to natural persons (i.e. individuals and private companies, as they are not legal entities). Direct marketing business-to-business (except private companies), including where a person is contacted in his or her occupational role, is however mainly regulated by ethical rules.

According to article 19 of the Swedish Marketing Act marketing via electronic communication (i.e. e-mail, fax, SMS, MMS or an automatic calling device or any other similar automatic system for individual communication) to natural persons without prior consent is prohibited. An exception exists in the case of contact information that was received by the natural person in connection with a purchase or service, if the following requirements are fulfilled:

- such natural person has not objected to the use of the e-mail address information for marketing purposes by means of e-mail;
- the marketing pertains to the trader's own, similar products; and
- the natural person has been clearly and explicitly provided the opportunity to object, simply and without charge, to the use of such information for marketing purposes when it is collected and in conjunction with each subsequent marketing communication.



Further, article 20 of the Swedish Marketing Act stipulates that marketing via email shall at all times contain a valid address to which the recipient may send a request that the marketing practice cease. This provision apply in respect of marketing to both natural persons (individuals and private companies) and legal persons.

A trader may use other methods of individual remote communication than those referred to in article 19 unless the natural person clearly objects to the use of such methods.

Recipients that do not want to receive advertisement by post can attach a sticker to their mailbox and/or front door declaring “No advertising please” or a similar statement. In addition, “Nix-Telefon” and “Nix adresserat” are two lists individuals who does not want to receive direct marketing via phone or physical post can registered at.