

# **DATA PROTECTION LAWS OF THE WORLD**

Sweden



Downloaded: 14 May 2024

## SWEDEN



Last modified 22 January 2024

### LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

### Territorial Scope

Primarily, the application of the GDPR turns on whether an organisation is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organisation that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "to the offering of goods or services" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "the monitoring of their behaviour" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

In addition to the GDPR, the Data Protection Act (2018:218) (the "**Data Protection Act**") and the Data Protection Ordinance (2018:219) apply. The Data Protection Act regulates general aspects of data protection where the GDPR allows, e.g. processing of personal identity numbers and processing of data relating to criminal convictions and offences. The Data Protection Act applies from 25 May 2018 (i.e. the same date as the GDPR).

In addition to the Data Protection Act and the Data Protection Ordinance, there are sector and processing specific regulations.

The Camera Surveillance Act (2018:1200) contains provisions regarding camera surveillance. The Camera Surveillance Act applies *inter alia* where camera surveillance is carried out with equipment located in Sweden and where the one carrying out the surveillance is established in Sweden or in a third country. The Camera Surveillance Act applies from 25 May 2018 (i.e. the same date as the GDPR).

The Whistleblowing Act (2021:890) entered into force on 17 December 2022 and implements the EU Directive 2019/1937 (the Whistleblowing Directive). Chapter 7 of the Whistleblowing Act contains *inter alia* provisions on permitted purposes of processing personal data, internal access to personal data and retention periods.

Moreover, a vast number of sector specific acts apply in Sweden, for example relating to the healthcare, ethical review of research, finance, education, referendums / elections, enterprise, communication, certain aspects of the labor market, etc.

For example, the Credit Information Act (1973:1173) applies to credit reference agencies and contains specific provisions regarding the processing of personal data.

The Patient Data Act (2008:355) and the Patient Data Ordinance (2008:360) regulates healthcare providers' processing of personal data. As of 1 January 2023, the new the Act (2022:913) on shared health and care documentation applies. It contains further provisions regarding the processing of personal data.

Furthermore the Electronic Communications Act (2022:482) (the "**Electronic Communications Act**") and the Electronic Communications Ordinance (2022:511) apply to inter alia electronic communications networks and electronic communications services and associated facilities and services as well as other radio use. The Electronic Communications Act implements Directive (EU) 2018/1972 (the Electronic Communications Code) and Directive 2002/58/EC (the so called ePrivacy Directive). The Electronic Communications Act applies to providers of public electronic communications networks and publicly available electronic communications services' processing of personal data, and regulates the use of so-called cookies.

## DEFINITIONS

"**Personal data**" is defined as *"any information relating to an identified or identifiable natural person"* (Article 4). A low bar is set for "identifiable" &#8211; if the natural person can be identified using &#8220;all means reasonably likely to be used&#8221; (Recital 26) the information is personal data. A name is not necessary either &#8211; any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who *"alone or jointly with others, determines the purposes and means of the processing of personal data"* (Article 4). The processor *"processes personal data on behalf of the controller"*, acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

## NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).



However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

In Sweden, the Swedish Authority for Privacy Protection (Sw: Integritetsskyddsmyndigheten) is the supervisory authority.

## Postal address

Box 8114  
104 20 Stockholm  
Sweden

## Visiting address

Fleminggatan 14, 7th Floor  
112 26 Stockholm  
Sweden

## Phone number

+46 8 657 61 00

## E-mail

[imy@imy.se](mailto:imy@imy.se)

## Website

[www.imy.se](http://www.imy.se)

## REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases (Article 36 prior consultation) following a data protection impact assessment (Article 35) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

In Swedish national law, there are no indiscriminate general notification obligations. However, there are sector and processing specific provisions requiring notification and / or requiring a permit from the relevant supervisory authority, *inter alia*:

- A permit from the Swedish Authority for Privacy Protection is required for camera surveillance of publicly accessible areas carried out by authorities (and under limited circumstances private entities tasked with similar duties as authorities) under the Camera Surveillance Act (2018:1200).
- With a limited number of exceptions, the processing of personal data relating to criminal convictions and offences (Article 10 of the GDPR) by others than public authorities requires a permit from the Swedish Authority for Privacy Protection under the Data Protection Act and the Data Protection Ordinance (2018:219). The Swedish Authority For Privacy Protection has proposed a new regulation to allow for companies in the financial sector and in the defence industry to process personal data relating to criminal convictions and offences.
- Sector specific requirements exist under *inter alia* the Credit Information Act (1973:1173). A license from the supervisory authority is generally required to carry out credit information activities. From 1 January 2024, the responsibility for issuing licences and supervising credit information activities will be transferred from the Swedish Authority for Privacy Protection to the Swedish Financial Supervisory Authority (Sw: *Finansinspektionen*).

## DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "expert knowledge" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must report directly to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

There are no derogations in Swedish national law, except that under the Data Protection Act, a DPO performing tasks under to Article 37 GDPR shall not unauthorisedly disclose what has come to their knowledge in the performance of their tasks. The Swedish Public Access to Information and Secrecy Act (2009:400) applies in relation to the confidentiality obligation of a DPO within the public sector.

## COLLECTION & PROCESSING

## Data protection principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimisation principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organisational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organisations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

## Legal basis under article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

## Special category data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;

- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

## Criminal convictions and offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

## Processing for a secondary purpose

Increasingly, organisations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose;
- the context in which the data have been collected;
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible);
- the possible consequences of the new processing for the data subjects; and
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

## Transparency (privacy notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;

- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

## Rights of the data subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

### Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

### Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

### Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

### Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

### Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xml).

### Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate compelling legitimate grounds; for processing which override the rights of the data subject.



In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

*The right not to be subject to automated decision making, including profiling (Article 22)*

Automated decision making (including profiling) "which produces legal effects concerning [the data subject] &#8230; or similarly significantly affects him or her" is only permitted where:

- a. necessary for entering into or performing a contract;
- b. authorised by EU or Member State law; or
- c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

## Personal identity numbers

In Sweden, personal identity numbers may be processed without consent only where manifestly justified with regard to the purpose of the processing, the importance of secure identification or some other substantial reason.

## Personal data relating to criminal convictions and offences

Personal data relating to criminal convictions and offences (Article 10 of the GDPR) may be processed by other parties than public authorities if the processing is necessary to (i) establish, exercise or defend legal claims or (ii) to fulfil a legal obligation under law or regulation. Furthermore, the Swedish Authority for Privacy Protection may upon application in an individual case grant a permit to process personal data relating to criminal convictions and offences.

## Rights of the data subject

Swedish law may prohibit controllers to disclose certain data to data subjects. This applies to the rights in Articles 13-15 of the GDPR.

For personal data in running text which has not taken on its final form when the request was made (e.g. drafts) or that is a note or similar, the right under Article 15 of the GDPR does not apply. This exemption may however not be relied on by a data controller if such personal data (i) has been disclosed to a third party, (ii) is processed solely for archiving purposes in the public interest or for statistical purposes, or (iii) has been processed over a period of more than one year in running text that has not taken on its final form.

## Other derogations for specific processing situations or sectors

Furthermore, in regards to data subjects' rights, there are a number of sector specific derogations (e.g. healthcare and credit reference agencies, etc.).

## TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). On 10 July 2023, the European Commission adopted its adequacy decision for the EU-US Data Privacy Framework, in which an adequate level of protection for personal data transferred from the EU to US companies that have joined the framework

is ensured in accordance with GDPR Art. 45. Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, Republic of Korea, Eastern Republic of Uruguay, the United Kingdom, United States (if certified under the EU-US Data Privacy Framework) and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules and standard contractual clauses. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

On 16 July 2020, the Court of Justice of the European Union's ("CJEU") invalidated the EU-US Privacy Shield in the so called *Schrems II* case (judgement of the CJEU in Case C-311/18). Moreover, the CJEU clarified that exporters of personal data to third countries may continue to rely on standard contractual clauses. When doing so, however, exporters need to carry out a so-called transfer impact assessment and implement supplementary measures as necessary in each individual case, in order to be able to ensure that a level of protection essentially equivalent to that which is guaranteed within the EU can be upheld.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

- explicit informed consent has been obtained;
- the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
- the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation. Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

For more information, please visit our [Transfer - global data transfer methodology website](#).

## SECURITY

### Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

- a. the pseudonymisation and encryption of personal data;
- b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

There are no specific security requirements set out in the Data Protection Act. However, it should be noted that certain security related provisions are prescribed under the Patient Data Act (2008:355) when processing personal data, regarding e.g. confidentiality, access and disclosure.

Moreover, a two-factor authentication when accessing special categories of data over an open network and encryption when sending special categories of data are examples of previous recommendations from the Swedish Authority for Privacy Protection.

## BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "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" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation's data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

There are no derogations under Swedish law, except that personal data breaches that fall under the Criminal Data Act (2018:1177) (which implements the Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data) shall be reported by public authorities separately in accordance certain provisions of the Criminal Data Act.

## ENFORCEMENT

### Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking'; and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

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)).

Fines can be imposed in combination with other sanctions.

## Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

## Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of 'non-material' damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, 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).



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

## Fines

Under the Data Protection Act, infringements of Article 10 of the GDPR may render administrative fines. As regards the amount of such fines, the higher of the two levels for legal maximum fines prescribed in the GDPR applies (Article 83(5) of the GDPR). As such, fines may be up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher.

In relation to public authorities, violations of the GDPR may render administrative fines under the Data Protection Act. Fines imposed on public authorities adhere to the system of the two levels of fines depending on the violated Article set out in the GDPR, may amount to maximum SEK 5 000 000 (in relation to the lower level of fines, set out in Article 83(4) of the GDPR) and SEK 10 000 000 (in relation to violations set out in Articles 83(5) and 83(6) of the GDPR).

Moreover, the Data Protection Act regulates procedural matters relating to decisions on administrative fines and how to appeal such decisions made by authorities (for example, the right to appeal to the Swedish Administrative Court).

## Right to damages

The right for data subjects to claim damages from a controller or processor under Article 82 of the GDPR also applies to violations of provisions in the Data Protection Act and other Swedish regulations that supplement the GDPR.

## ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

There is no provision in the Data Protection Act which particularly concerns the processing of personal data in relation to electronic marketing.

There is, however, other legislation in Sweden (such as the Marketing Act (2008:486) that regulates electronic marketing in Sweden.

Under the Marketing Act, unsolicited automated electronic marketing (by *inter alia* email) to natural persons generally requires prior consent. It is, however, allowed to conduct email marketing to natural persons without prior consent provided that the person has not objected to such, if the trader has received the email address of the individual in

connection with sales of a similar product. In these cases, the addressee must be given the option to opt out of marketing both when the email address is collected and subsequently along with each marketing email.

The Marketing Act also states that, in the case of email marketing, the email message must always contain a valid address to which the recipient can send a request for the marketing to cease. This applies to marketing to natural persons as well as to legal entities.

Note that certain provisions relating to electronic marketing under Swedish law may be amended in the future due to the upcoming ePrivacy Regulation which will become immediately enforceable as law in all EU member states.

## ONLINE PRIVACY

Pursuant to the Electronic Communications Act (implementing *inter alia* the e-Privacy Directive), data may be stored in or retrieved from a subscriber's or a user's terminal equipment only if the subscriber or user has been provided with information about the purpose of the processing and consents to it, i.e. the user must give its prior ☐opt-in☐ consent before a cookie is placed on the user's computer. In its judgment of 1 October 2019, the Court of Justice of the European Union (the "**CJEU**") decided on cookie consent requirements and stated that cookie consent must be given by a statement or clear affirmative action (consent cannot be validly obtained through pre-ticked checkboxes).

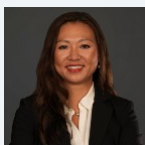
Consent is however not required for storage or access that is:

- necessary for the transmission of an electronic message over an electronic communications network; or
- necessary for the provision of a service explicitly requested by the user or subscriber.

In the event of a wilful or negligent breach of the now relevant provision in the Electronic Communications Act are criminalised. As such, a fine may be imposed provided that the offence is not sanctioned by the Swedish Criminal Code (1962:700). However, if the breach is deemed to be minor, no fine shall be imposed. To our knowledge there has not yet been any cases where a website operator has been fined for a breach of the cookie provision in the Electronic Communications Act.

Sweden has set the digital age of consent as 13 in relation to consent to processing of personal data in the context of offering information society services.

## KEY CONTACTS



**Jennie Nilsson**

Advokat / Partner, Head of Digital, Data & Cyber

T +46 73 867 67 87

jennie.nilsson@se.dlapiper.com

## DATA PRIVACY TOOL

You may also be interested in our [Data Privacy Scorebox](#) to assess your organization's level of data protection maturity.

## Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at [www.dlapiper.com](http://www.dlapiper.com).

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.