Data Protection in Sweden: Overview

by Anna Fernqvist Svensson, Hellström Advokatbyrå, with Practical Law Data Privacy & Cybersecurity

Country Q&A | Law stated as of 01-Jan-2024 | Sweden

A Q&A guide to data protection in Sweden.

This Q&A guide gives a high-level overview of the data protection laws, regulations, and principles in Sweden, including the main obligations and processing requirements for controllers, processors, or other third parties. It also covers data subject rights, the supervisory authority's enforcement powers, and potential sanctions and remedies. It briefly covers rules applicable to cookies and spam.

To compare answers across multiple jurisdictions, visit the Data Protection Country Q&A Tool.

Regulation

Legislation

1. What national laws regulate the collection, use, and disclosure of personal data?

Data Protection Law

The European Union (EU) General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) governs data protection in the EU and applies directly to each European Union (EU) member state, including Sweden. The GDPR replaced the EU Data Protection Directive (Directive 95/46/EC) and the prior Swedish data protection law, introducing a single legal framework across the EU. However, several GDPR provisions allow EU member states to enact national legislation specifying, restricting, or expanding the scope of some requirements.

Sweden enacted the Data Protection Act (2018:218) (Swedish Act) and Data Protection Regulation (2018:219) (both in Swedish) (Swedish Regulation), which supplement the GDPR. The Swedish Act and Swedish Regulation also change some of the GDPR's requirements. Prior to the Swedish Act's passage, the Swedish government prepared Proposition 2017/18:105 (February 15, 2018) (in Swedish), which includes additional background information on certain provisions in the Swedish Act.

Sweden also:

- Signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) (Convention 108) on January 28, 1981 and September 29, 1982, respectively. Convention 108 was effective October 1, 1985.
- Signed and ratified the Additional Protocol to Convention 108 on supervisory authorities and transborder data flows (Additional Transborder Protocol) on November 8, 2001. The Additional Transborder Protocol was effective July 1, 2004.
- Signed the Protocol amending Convention 108 (CETS No. 223) (Convention 108+) on October 10, 2018. Sweden has not ratified Convention 108+ as of the date of this Q&A.

(See Council of Europe: Treaty List for Sweden.)

For more on Sweden's implementation of the GDPR, see Practice Note, Swedish Implementation of the GDPR. For GDPR guidance from the Swedish Authority for Privacy Protection, see GDPR Data Protection Authority Guidance Tracker by Country (EEA): Sweden.

Other Relevant Laws

Several other Swedish laws apply to personal data processing, including:

- The Electronic Communications Act (2003:389) (in Swedish), which regulates, among other things, cookie use (see Question 18).

- The Marketing Act (2008:486) (in Swedish), which regulates, among other things, the use of direct marketing (see Question 9).
- The Patient Data Act (2008:355) (in Swedish), which regulates healthcare providers' personal data processing.
- The Act on Names and Images in Advertising (1978:800) (in Swedish), which regulates personal data use in advertising.
- The Credit Information Act (1973:1173) and Debt Recovery Act (1974:182) (both in Swedish), which regulate the use of credit information.
- The Camera Surveillance Act (2018:1200) (in Swedish), which regulates the use of camera surveillance in accordance with the GDPR.

Additional laws may govern the use of personal data in the public sector, for example, relating to law enforcement authorities' activities. The details of all of these other laws are outside the scope of this Q&A, which focuses on the GDPR and the Swedish Act. For more on other relevant EU laws that apply in Sweden, but that are outside the scope of this Q&A, see Country Q&A, Data Protection in the EU: Overview: Question 1.

Scope of Legislation

2. To whom do the laws apply?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1). Both the GDPR and the Swedish Data Protection Act (2018:218) (in Swedish) (Swedish Act) apply to:

- Controllers**.** A controller, formerly known as a data controller, is any natural or legal person, public authority, agency, or any other body that determines the purposes and the means of the data processing alone or jointly with others (Article 4(7), GDPR).
- Processors**.** A processor, formerly known as a data processor, is any natural or legal person, public authority, agency, or any other body that processes personal data on the controller's behalf (Article 4(8), GDPR).
- Data subjects**.** Data subjects are individuals to whom personal data relates (Article 4(1), GDPR; for more on what constitutes personal data, see Question 3).

The Swedish Act incorporates the GDPR's definitions set out above (Chapter 1, Section 1, Swedish Act). For more on the GDPR's definitions, see Practice Note, Overview of EU General Data Protection Regulation: GDPR: definitions.

3. What personal data does the law regulate?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1). Both the GDPR and Sweden's Data Protection Act (2018:218) (in Swedish) (Swedish Act) regulate personal data processing (Articles 2(1) and 4(2), GDPR; Chapter 1, Section 2, Swedish Act).

The GDPR:

- Defines personal data as information relating to an identified or identifiable natural person, called a data subject. An identifiable natural person is one who can be identified, directly or indirectly, by reference to identifiers such as the person's:
  - name;
  - identification number;
  - location data;
  - online identifiers like IP addresses, cookies, and radio frequency identification tags (see Recital 30, GDPR); or
  - physical, physiological, genetic, mental, economic, cultural, or social identity.

  (Article 4(1), GDPR.)
- Imposes additional limitations on and requires more rigorous protection for special categories of personal data (Article 9(1), GDPR; see Question 11).
- Defines genetic data, biometric data, and health data (Article 4(13) to (15), GDPR).
- Allows EU member states to enact national laws specifying, restricting, or expanding the requirements for processing special categories of personal data (Article 9(4), GDPR).

The Swedish Act incorporates the GDPR's definitions (Chapter 1, Section 1, Swedish Act).

4. What acts are regulated?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1). Subject to certain exemptions, both the GDPR and Sweden's Data Protection Act (2018:218) (in Swedish) (Swedish Act) apply to personal data processing:

- Wholly or partly by automated means.
- Other than by automated means if the personal data forms or is intended to form part of a filing system.

(Article 2(1), (2), GDPR; Chapter 1, Section 2, Swedish Act.)

The Swedish Act does not separately define processing, so the GDPR's definition applies. The GDPR defines processing as any operation or set of operations that is performed on personal data or sets of personal data, whether automated or not, such as:

- Collection.
- Recording.
- Organization.
- Structuring.
- Storage.
- Adaptation or alteration.
- Retrieval.
- Consultation.
- Use.
- Disclosure by transmission.
- Dissemination or otherwise making available.
- Alignment or combination.
- Restriction, erasure, or destruction.

(Article 4(2), GDPR.)

Material Scope

The GDPR includes a material scope provision stating that it does not apply to:

- Activities that fall outside the scope of EU law.
- Processing by EU member states under Title V, Chapter 2 of the Treaty on European Union relating to foreign and security policy.
- Processing for purely personal or household activities.
- Processing by competent authorities to prevent, investigate, detect, or prosecute criminal offenses and execute criminal penalties, including safeguarding against and preventing threats to public safety.

(Article 2(2), GDPR.)

The Swedish Act has a somewhat broader material scope than the GDPR and also applies to personal data processing:

- Not covered by EU law.

- Covered by Title V, Chapter 2 of the Treaty on European Union, which relates to foreign and security policy.

(Chapter 1, Section 2, Swedish Act.)

The Swedish Act also states that the provisions on the age of child consent for online services directed to children only apply to children residing in Sweden, regardless of the controller's or processor's location (Chapter 1, Section 5, Swedish Act; see Question 9).

If another Swedish law or regulation applies to the processing that conflicts with the Swedish Act, the other Swedish law applies (Chapter 1, Section 6, Swedish Act).

Derogations for Specific Processing Situations

GDPR Articles 85 to 91 permit EU member states to enact further rules in seven specific processing situations. The Swedish Act introduces further rules that apply to processing:

- For journalistic purposes and academic, artistic, or literary expression under GDPR Article 85 (Chapter 1, Section 7, Swedish Act).
- Personal data in official documents under GDPR Article 86 (Chapter 1, Section 7, Swedish Act).
- Personal identification numbers under GDPR Article 87 (Chapter 3, Section 10, Swedish Act).
- In the employment context under GDPR Article 88 (Chapter 3, Section 2, Swedish Act).
- For archiving in the public interest, scientific or historical research, or statistical purposes under GDPR Article 89 (Chapter 4, Sections 1 to 3, Swedish Act). The Swedish government released Proposition 2017/18:298 on processing personal data for research purposes (September 6, 2018) (in Swedish), which resulted in the amendment of several acts related to personal data processing for research purposes.

The Swedish Act does not expressly address the GDPR's other specific processing situations under Article 90 and 91. However, other Swedish laws may apply. For more on the Swedish Act's derogations for specific processing situations, see Practice Note, Swedish Implementation of the GDPR: Derogations for Specific Processing Situations.

The rules applicable to processing under GDPR Articles 85 and 89 may also affect data subject rights (see Question 12 and Question 13).

For more on:

- The jurisdictional scope of the GDPR and the Swedish Act, see Question 5.
- The GDPR's and the Swedish Act's exemptions, see Question 6.
- The GDPR's definitions, see Practice Note, Overview of EU General Data Protection Regulation: GDPR: definitions.

5. What is the jurisdictional scope of the rules?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1). For more on the GDPR's jurisdictional scope and when the requirement to designate a representative in the EU applies, see Country Q&A, Data Protection in the EU: Overview: Question 5.

Some EU member states have passed national laws that include a territorial scope provision that mirrors GDPR Article 3. Other member states' laws include different applicability language or do not include a territorial scope provision. The Data Protection Act (2018:218) (in Swedish) (Swedish Act) applies to:

- Controllers and processors established in Sweden that process personal data in the context of that establishment.
- Controllers and processors not established in Sweden that process personal data about data subjects in Sweden when the processing activities relate to:
    - supplying goods or services to data subjects in Sweden; or
    - monitoring data subjects' behavior that takes place in Sweden.
- Controllers not established in Sweden that process personal data and that are subject to Swedish law under international law.

(Chapter 1, Section 5, Swedish Act.)

For more on the GDPR's territorial scope, see Practice Notes:

- Overview of EU General Data Protection Regulation.
- Determining the Applicability of the GDPR.

6. What are the main exemptions (if any)?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1). For more on the GDPR's main exemptions, see Country Q&A, Data Protection in the EU: Overview: Question 6.

The Data Protection Act (2018:218) (in Swedish) (Swedish Act) does not apply in the following circumstances:

- When the processing is contrary to:

- the Freedom of the Press Act (1949:105) (in Swedish), specifically personal data disclosures in official documents held by public authorities or bodies under GDPR Article 86 or
- the Fundamental Law on Freedom of Expression (1991:1469) (in Swedish).

(Chapter 1, Section 7, Swedish Act.)

- When personal data is processed by:
  - The Armed Forces for defense intelligence activities and military security under Law (2007:258) (in Swedish).
  - The Defense Radio Agency's radio intelligence and development activities under Law (2007:259) (in Swedish).
  - The Security Police under Law (2019:1182) (in Swedish).

(Chapter 1, Section 3, Swedish Act.)

The following provisions are also exempt under the Swedish Act:

- GDPR Articles 33 and 34 do not apply to certain personal data security breaches covered by the Security Protection Act (2018:585) or the Security Protection Act (2019:109) in the Riksdag and its authorities (both in Swedish) and their regulations (Chapter 1, Section 4, Swedish Act).
- GDPR Articles 5 to 30 and 35 to 50 and Swedish Act Chapters 2 to 5 do not apply to processing for journalistic purposes and academic, artistic, or literary expression (Chapter 1, Section 7, Swedish Act; see Question 13). The IMY has released guidance (in Swedish) on what is meant by "journalistic purposes" including examples of different types of personal data publications that would fall under the exception.

If another Swedish law or regulation applies to the processing that conflicts with the Swedish Act, the other Swedish law applies (Chapter 1, Section 6, Swedish Act).

Notification

7. Is notification or registration with a supervisory authority required before processing data?

Notification, registration, or authorization may be required in certain circumstances. For information on the Swedish Authority for Privacy Protection's (IMY) notification, registration, or authorization requirements, see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: Sweden: Question 2 and Question 3.

For the IMY's contact details, see Regulator Details.

Main Data Protection Rules and Principles

Main Obligations and Processing Requirements

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1) and sets out the following six principles that govern personal data processing:

- **Lawful, fair, and** transparent **processing.** Controllers must process personal data lawfully, fairly, and in a transparent manner in relation to the data subject. The European Data Protection Board has endorsed Article 29 Working Party guidelines on transparency (see European Commission: Guidelines on transparency under the GDPR (WP260) (April 11, 2018)).
- Purpose limitation**.** Controllers:
  - may only collect personal data for specified, explicit, and legitimate purposes; and
  - may not further process personal data for an incompatible purpose, however, processing for archiving in the public interest, scientific or historical research, or statistical purposes under GDPR Article 89(1) is not considered incompatible.
- Data minimization**.** Controllers may only process personal data that is adequate, relevant, and limited to what is necessary for the purposes of their processing.
- **Accuracy.** Personal data must be accurate and up to date. Controllers must take every reasonable step to erase or rectify inaccurate data without delay.
- **Storage limitation.** Controllers generally may not store personal data in a form that permits identification of data subjects for longer than is necessary for the purposes of their processing. With appropriate technical and organizational measures to safeguard data subjects' rights and freedoms, there are limited exceptions under GDPR Article 89(1) for:
  - archiving in the public interest;
  - scientific or historical research; or
  - statistical purposes.
- **Integrity and confidentiality.** Controllers must process personal data in a manner that ensures appropriate security, using appropriate technical and organizational measures to protect against:
  - unauthorized or unlawful processing;

- accidental loss;
- destruction; or
- damage.

(Article 5(1), GDPR; see Question 15.)

For more on accountability and GDPR compliance, see Practice Note, Demonstrating Compliance with the GDPR: Accountability and Demonstrating Compliance.

In addition to complying with these six principles, controllers must also, among other things:

- Take appropriate measures to provide processing-related information to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language (Article 12, GDPR; see Question 12).
- Facilitate the exercise of data subjects' rights (see Question 13).
- Properly secure personal data (see Question 15).
- Record all personal data breaches and report relevant breaches to the relevant supervisory authority and data subjects in certain circumstances (Articles 33 and 34, GDPR; see Question 16).
- Meet certain obligations when engaging processors (see Question 17).
- Keep written or electronic records with specified information about their processing activities, depending on the number of their employees and the nature of the processing (Article 30, GDPR).
- Designate an EU representative in certain circumstances (Articles 3(2) and 27(1), GDPR).
- Carry out a data protection impact assessment (DPIA) when necessary (Article 35, GDPR). The Swedish Authority for Privacy Protection (IMY) has published a list (in Swedish) of processing operations that require a DPIA.
- Consult the supervisory authority before processing if a DPIA under GDPR Article 35 indicates that the processing would result in a high risk if the controller fails to take measures to mitigate the risk (Article 36, GDPR).
- Designate a data protection officer (DPO) if:
    - a public authority or body carries out the processing, except for courts acting in their judicial capacity;
    - the controller's core activities are processing operations that require regular and systematic monitoring of data subjects on a large scale by virtue of their nature, scope, or purposes;
    - the controller's core activities are processing special categories of data or personal data relating to criminal convictions and offenses on a large scale; or
    - an EU member state stipulates by national regulation that a DPO is required.

  (Article 37(1), GDPR.)
- Publish the DPO's contact details and communicate them to the supervisory authority (Article 37(7), GDPR).

Data Protection Officers

The GDPR allows EU member states to require DPO appointments in additional situations (Article 37(4), GDPR). For information on whether controllers operating in Sweden are required to appoint a data protection officer, see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: Sweden: Question 4 and Question 5.

Purpose Limitation

The GDPR generally restricts data processing to the original collection purpose unless an exception applies, for example:

- The data subject consents to processing for a secondary purpose.
- An EU or EU member state law, which is a necessary and proportionate measure to safeguard certain important objectives, permits the processing for a secondary purpose.

(Article 6(4), GDPR.)

Without data subject consent or an EU or member state law permitting the secondary processing, any secondary processing purpose must both:

- Remain compatible with the original processing purpose.
- Satisfy the conditions in GDPR Article 6(4).

To determine the secondary processing purpose's compatibility, the controller should consider the criteria specified in GDPR Article 6(4) (see Practice Note, Overview of EU General Data Protection Regulation: Further compatible processing).

The Data Protection Act (2018:218) (in Swedish) (Swedish Act) does not include any clauses permitting secondary processing. In the preparatory work to the Swedish Act, Proposition 2017/18:298 on processing personal data for research purposes (September 6, 2018) (in Swedish), the Swedish government discusses secondary uses of personal data for research purposes (see Question 13). Further discussion of this proposition is outside the scope of this Q&A.

9. Is the consent of data subjects required before processing personal data?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1) and sets out six lawful bases for processing personal data. One of those bases is obtaining the data subject's consent for one or more specific processing purposes. (Article 6(1)(a), GDPR.) For more on:

- When the GDPR requires data subject consent, including valid consent elements, documentation, and withdrawing consent, see Country Q&A, Data Protection in the EU: Overview: Question 9 and Practice Notes:

- Overview of EU General Data Protection Regulation: Consent requirements; and
- Demonstrating Compliance with the GDPR.

- The other legal grounds for processing personal data:
  - in Sweden, see Question 10.
  - under the GDPR, see Country Q&A, Data Protection in the EU: Overview: Question 10.

The Data Protection Act (2018:218) (in Swedish) (Swedish Act) does not specify, restrict, or expand the GDPR's requirements for consent.

Explicit Consent

The GDPR requires controllers relying on consent as the legal basis for processing personal data to obtain explicit consent in certain circumstances (see Country Q&A, Data Protection in the EU: Overview: Question 9). GDPR Article 9(2)(a) permits EU or member state law to prohibit the use of explicit data subject consent as a legal basis for processing special categories of personal data. The Swedish Act does not prohibit this.

The Swedish Act requires controllers to obtain data subjects' explicit consent before disclosing special categories of personal data to fulfill obligations and exercise rights under labor laws or for social security or social protection purposes (Chapter 3, Section 2, Swedish Act). For more on these requirements, see Practice Note, Swedish Implementation of the GDPR: Swedish Act Exceptions That Permit Processing Special Categories of Personal Data.

Consent by Minors

For online service providers offering services directly to children (called information society services in the GDPR), the GDPR permits EU member states to lower the age of child consent below 16 years old, if the age is not lower than 13 (Article 8(1), GDPR). The Swedish Act reduces the age of child consent to 13 for service providers offering online services to children residing in Sweden (Chapter 2, Section 4, Swedish Act). The Swedish Act does not otherwise change the requirements for obtaining valid consent from children or impose any additional requirements or restrictions or processing personal data about children.

10. If consent is not given, on what other grounds (if any) can processing be justified?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1). The GDPR permits personal data processing without data subject consent if at least one of the following other legal bases for processing applies:

- The processing is necessary to enter into or perform a contract with the data subject or to take pre-contractual steps at the data subject's request.

- The processing is necessary for the controller to comply with a legal obligation.
- The processing is necessary to protect the vital interests of the data subject or another natural person.
- The processing is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the controller.
- The processing is necessary to pursue the controller's or a third party's legitimate interests, unless the data subject's interests or fundamental rights and freedoms override those interests.

(Article 6(1), GDPR.)

The Data Protection Act (2018:218) (in Swedish) (Swedish Act) permits controllers to base processing on GDPR Article 6(1)(c) if the processing is necessary to comply with a legal obligation applicable to the controller under:

- Applicable laws or regulations.
- Collective agreements.
- Decisions granted based on applicable laws or the Constitution, for example, legal judgments.

(Chapter 2, Section 1, Swedish Act.)

Controllers may base processing on GDPR Article 6(1)(e) if the processing is necessary:

- To perform a task of general interest based on:
  - applicable laws or regulations;
  - collective agreements; or
  - decisions granted based on applicable laws or the Constitution, for example, legal judgments.
- To exercise the controller's official authority based on applicable laws or regulations.

(Chapter 2, Section 2, Swedish Act.)

For more on consent as a legal basis to process data, see Question 9. For more on lawful bases for processing, see Practice Note, Demonstrating Compliance with the GDPR: Lawfulness of Processing.

Special Rules

11. Do special rules apply for certain types of personal data, such as sensitive data?

The EU General Data Protection Regulation (Regulation (EU) 2016/679 (GDPR) applies directly in Sweden (see Question 1) and:

- Prohibits processing special categories of personal data, unless an exception applies (Article 9, GDPR).
- Allows EU member states to introduce further conditions and limitations on processing genetic, biometric, and health data (Article 9(4), GDPR).
- Limits who may process personal data relating to criminal conviction and offenses and when this processing may occur (Article 10, GDPR).

For more on the GDPR's special rules for certain types of personal data, such as sensitive data or criminal conviction and offense data, see Country Q&A, Data Protection in the EU: Overview: Question 11.

Special Categories of Personal Data

Under the GDPR, special categories of personal data include personal data revealing any of the following:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data to uniquely identify a natural person.
- Data concerning a natural person's:
    - health;
    - sex life; or
    - sexual orientation.

(Article 9, GDPR.)

On August 1, 2022, the EU Court of Justice (ECJ) ruled that processing personal data liable to indirectly reveal sensitive information concerning an individual is prohibited unless an exception applies, highlighting how broadly special categories of personal data are defined (Case C-184/20: OT v Vyriausioji tarnybin#s etikos komisija (Chief Official Ethics Commission, Lithuania); see Legal update, Information indirectly disclosing sexual orientation is special category personal data (ECJ)). For more on processing special categories of personal data, see Practice note, Overview of EU General Data Protection Regulation: Special Categories of Personal Data.

Under the Data Protection Act (2018:218) (in Swedish) (Swedish Act) controllers may be permitted to process special categories of personal data when necessary for the purposes set out in GDPR Article 9(2)(b), (g), (h), and (j) (Chapter 3, Sections 2 to 7, Swedish Act). This includes processing:

- When necessary for the controller or data subject to fulfill obligations and exercise rights under labor laws or for social security or social protection purposes, if:
    - applicable labor, social security, or social protection laws require the disclosure; or
    - the data subject explicitly consents.

  (Chapter 3, Section 2, Swedish Act.)
- When an authority processes the personal data for public interest purposes, and:
    - the information was submitted to the authority and applicable law requires the processing;
    - the processing is necessary for handling a case; or
    - the processing is necessary for important public interest reasons and does not infringe the data subject's privacy.

  (Chapter 3, Section 3, Swedish Act.) The Swedish Government may issue additional regulations on processing special categories of personal data for public interest purposes (Chapter 3, Section 4, Swedish Act).
- When necessary for:
    - preventive health care and occupational medicine;
    - assessing an employee's working capacity;
    - medical diagnosis;
    - providing healthcare, treatment, or social care; or
    - managing healthcare services, social care, and their systems.

  (Chapter 3, Section 5, Swedish Act.)
- For archiving in the public interest to comply with archiving regulations. The Swedish Act permits the government, or an authority named by the government, to issue regulations on processing for general archival purposes by controllers not subject to archiving regulations. The authority named by the government can also permit processing for general archival purposes on a case-by-case basis by controllers not subject to archiving regulations. (Chapter 3, Section 6, Swedish Act.)
- When necessary for statistical purposes and the public interest in the statistical project clearly outweighs the risk of undue intrusion into the data subject's privacy (Chapter 3, Section 7, Swedish Act).

All other processing relating to special categories of personal data must comply with GDPR Article 9.

Genetic, Biometric, and Health Data

The GDPR permits EU member states to introduce further conditions and limitations on processing genetic, biometric, and health data (Article 9(4), GDPR). The Swedish Act does not address this type of processing.

The Patient Data Act (2008:355) (in Swedish) regulates healthcare providers' personal data processing. The details of this law are outside the scope of this Q&A.

Criminal Conviction and Offense Data

The GDPR only permits processing personal data relating to criminal convictions and offenses when either:

- Carried out under the control of official authority, for example, the police.
- EU or EU member state law authorizes the processing and provides for appropriate safeguards for data subjects' rights and freedoms.

(Article 10, GDPR.)

The Swedish Act permits processing criminal conviction or offense data when processed by either:

- The authorities.
- Other entities, to comply with archiving regulations.

(Chapter 3, Section 8, Swedish Act.)

When controllers other than authorities process criminal conviction and offense data, the processing must be both:

- Necessary to comply with the controller's legal obligations under GDPR Article 6(1)(c).
- For the purpose of complying with archiving regulations.

(Chapter 3, Section 8, Swedish Act.)

The Swedish Act permits the government, or a government-named authority, to issue regulations on processing criminal conviction and offense data by entities other than authorities. The government-named authority can also authorize non-authorities to process criminal conviction or offense data on a case-by-case basis. (Chapter 3, Section 9, Swedish Act.) The Swedish Authority for Privacy Protection has issued a regulation on processing of personal data concerning criminal offenses (DIFS 2018:2) (in Swedish). The Swedish Authority for Privacy Protection issued a proposal for a new regulation concerning criminal offenses (in Swedish), to replace the current regulation (DIFS 2018:2). The new regulation is proposed to enter into force 1 March 2024.

Data Protection Regulation (2018:219) (in Swedish) (Swedish Regulation) authorizes non-authorities to process criminal conviction and offense data if the processing is necessary to:

- Establish, exercise, or defend legal claims under GDPR Article 6(1)(f).
- Comply with a legal obligation under GDPR Article 6(1)(c).

(Section 5, Swedish Regulation.)

Rights of Individuals

12. What information rights do data subjects have?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1) and requires controllers to provide data subjects with certain information at the point of collection depending on whether they collect the personal data directly from the data subject or from a third party (Articles 13 and 14, GDPR). The information controllers must provide in each case is similar, but not identical. For more on what information the GDPR requires in each of these circumstances, see Country Q&A, Data Protection in the EU: Overview: Question 12 and Practice note, Data Subject Rights Under the GDPR: Information Right.

EU member states may restrict the scope of data subjects' information rights and controllers' related obligations under GDPR Articles 13, 14, and 5 (as it relates to the rights and obligations in Articles 13 and 14) when the restriction is a necessary and proportionate measure to safeguard certain objectives in GDPR Article 23 or in other specific processing situations (Articles 23 and 85, GDPR; for more on other specific data subject rights and the GDPR Article 23 objectives, see Question 13).

The Data Protection Act (2018:218) (in Swedish) (Swedish Act) provides that data subjects' information rights under GDPR Articles 13 and 14 do not apply:

- To processing for journalistic purposes and academic, artistic, or literary expression (Chapter 1, Section 7, Swedish Act).
- When applicable laws or regulations prevent the controller from providing the information to the data subject (Chapter 5, Section 1, Swedish Act). For controllers that are not authorities, this exception also applies to information that would have been classified by an authority under the Public Access and Secrecy Act (2009:400) (in Swedish) (Chapter 5, Section 1, Swedish Act).

Data Subject Rights When Processing for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes

Personal data that is processed solely for archiving in the public interest or research or statistical purposes may be only be used to take certain measures affecting data subjects when there are extraordinary reasons with regard to the data subject's vital interests (Chapter 4, Swedish Act).

13. Other than information rights, what other specific rights are granted to data subjects?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1). For more on individual rights under the GDPR and handling data subject requests, see:

- Country Q&A, Data Protection in the EU: Overview: Question 13.
- Practice Notes:
  - Complying with the GDPR's Transparency Obligation to Data Subjects; and
  - Data Subject Rights Under the GDPR.
- Responding to Data Subject Requests Under the GDPR Checklist.
- Handling Data Subject Requests Under the GDPR Toolkit.

Data Subject Rights Derogations

EU member states may restrict the scope of data subjects' rights and controllers' related obligations in GDPR Articles 12 to 22, 34, and 5 (as it relates to the rights and obligations in Articles 12 to 22) when the restriction is a necessary and proportionate measure to safeguard:

- National security.
- Defense.
- Public security.
- The prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties.
- Other important economic or financial public interests of the EU or EU member state, including:
  - monetary, budgetary, and taxation matters;
  - public health; and
  - social security.
- Judicial independence and proceedings.
- The prevention, investigation, detection, and prosecution of ethics breaches for regulated professions.
- Monitoring, inspection, or regulatory functions connected to the exercise of official authority regarding:
  - national or public security;
  - defense;
  - other important public interests;
  - crime prevention; or
  - breaches of ethics for regulated professions.

- Protection of the individual or the rights and freedoms of others.
- Enforcing civil law matters.

(Article 23(1), GDPR.)

Under the Data Protection Act (2018:218) (in Swedish) (Swedish Act), data subjects' GDPR Article 15 access rights do not apply:

- When applicable laws or regulations prevent the controller from providing the relevant information to the data subject. For controllers that are not authorities, this exception also applies to information that would have been classified by an authority under the Public Access and Secrecy Act (2009:400) (in Swedish). (Chapter 5, Section 1, Swedish Act.)
- To personal data contained in unfinished materials, memorandums, or similar items in unfinished form at the time of the access request unless the controller:
    - disclosed the personal data to a third party;
    - processes the personal data for archiving in the public interest or statistical purposes (see Personal Data Use Limitations When Processing for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes); or
    - the personal data has been processed in the unfinished materials for longer than one year.

    (Chapter 5, Section 2, Swedish Act.)

Data Subject Rights When Processing for Journalistic Purposes or Academic, Artistic, or Literary Expression

When controllers process personal data for journalistic purposes or academic, artistic, or literary expression, certain data subject rights under the GDPR do not apply, including:

- Transparency rights (Article 12, GDPR).
- Information rights (Articles 13 and 14, GDPR).
- Access rights (Article 15, GDPR).
- Rectification rights (Article 16, GDPR).
- Erasure rights (Article 17, GDPR).
- Processing restriction rights (Article 18, GDPR).
- The obligation to notify personal data recipients of rectification, erasure, or processing restriction requests and the data subject's right to be informed about those data recipients (Article 19, GDPR).
- Data portability rights (Article 20, GDPR).
- Objection rights (Article 21, GDPR).

(Chapter 1, Section 7, Swedish Act.)

The Swedish Authority for Privacy Protection has released guidance (in Swedish) on what is meant by "journalistic purposes" including examples of different types of personal data publications that would fall under the exception.

Personal Data Use Limitations When Processing for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes

Controllers that process personal data solely for the following reasons may only take certain measures affecting data subjects if necessary to protect the data subject's vital interests:

- Archiving in the public interest.
- Research purposes.
- Statistical purposes.

(Chapter 4, Swedish Act.)

This limitation does not prevent authorities from processing personal data contained in public documents (Chapter 4, Section 1, Swedish Act).

14. Do data subjects have a right to request the deletion of their data?

See Question 13.

Security Requirements

15. What security requirements are imposed in relation to personal data?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1). For more on the GDPR's security requirements for controllers and processors, see Country Q&A, Data Protection in the EU: Overview: Question 15.

The Data Protection Act (2018:218) (in Swedish) does not specify, restrict, or expand the GDPR's data security requirements. Other Swedish sector-specific laws may impose additional security requirements. Those laws are outside the scope of this Q&A.

16. Is there a requirement to notify data subjects or the supervisory authority about personal data security breaches?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1). For more on the GDPR's requirements to notify supervisory authorities and data subjects of certain personal data breaches, see Country Q&A, Data Protection in the EU: Overview: Question 16.

The Data Protection Act (2018:218) (in Swedish) (Swedish Act) does not limit or change the GDPR's data breach notification requirements. The Swedish Authority for Privacy Protection maintains an e-service for reporting personal data security breaches.

GDPR Articles 33 and 34 do not apply to personal data breaches that must be reported in accordance with:

- The Security Protection Act (2018:585) (in Swedish).
- The Security Protection Act (2019:109) in the Riksdag and its authorities (in Swedish).
- Any regulations issued in connection with the above laws.

(Chapter 1, Section 4, Swedish Act.)

These laws are outside the scope of this Q&A.

Processing by Third Parties

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1). For more on the GDPR's requirements when engaging processors, see Country Q&A, Data Protection in the EU: Overview: Question 17.

The Data Protection Act (2018:218) (in Swedish) (Swedish Act) does not specify, restrict, or expand the GDPR's requirements for engaging third-party processors. However, controllers may need to meet additional requirements when engaging third-party processors for cross-border data transfers (see Question 20).

Electronic Communications

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), which applies directly in Sweden (see Question 1), does not expressly address the use of cookies or equivalent devices.

For more on:

- The GDPR's requirements regarding cookies, including the need for a legal basis for processing, see Country Q&A, Data Protection in the EU: Overview: Question 18.
- The status of the Proposed EU E-Privacy Regulation, see Digital Single Market Strategy: Regulation on Privacy and Electronic Communications (ePrivacy Regulation): legislation tracker.
- How EU member states regulate cookies, see EU Member State Cookie Directive Implementation Chart.

The Electronic Communications Act (2003:389) (in Swedish) (ECA) regulates the use of cookies and equivalent technologies in Sweden. Organizations cannot store information on, or retrieve information from, a subscriber's or user's terminal equipment unless:

- They have informed the subscriber or user of the cookies' use purpose.
- The subscriber or user consents.

(Chapter 6, Section 18, ECA.)

These requirements do not apply to storage or access solely to transmit an electronic message through an electronic communications network or provide a service the subscriber or user explicitly requested (Section 18, Chapter 6, ECA).

The Swedish Post and Telecom Agency has provided guidance (in Swedish) on the use of cookies.

19. What rules regulate sending commercial or direct marketing communications?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), which applies directly in Sweden (see Question 9), does not expressly address the sending of unsolicited electronic commercial communications (spam). However, it

does give data subjects the right to object to personal data processing for direct marketing purposes (Article 21(3), GDPR). For more on sending spam under the GDPR and the requirement for a legal basis for processing, see Country Q&A, Data Protection in the EU: Overview: Question 19.

The Marketing Act (2008:486) (in Swedish) (Marketing Act), which implements part of the EU E-Privacy Directive (Directive 2002/58/EC), as amended by the EU Citizens' Rights Directive (Directive 2009/136/EC), regulates sending direct marketing communications. Under the Marketing Act, natural or legal persons acting for their own business activities (traders) cannot use email, fax, or similar automatic-dialing machines or systems for marketing to individuals without their prior consent (Section 19, Marketing Act).

However, if the trader obtained an individual's email address in connection with the sale of a product, the consent requirements do not apply if all the following conditions are met:

- The individual has not objected to the use of their email address for marketing purposes.
- The marketing concerns the trader's own similar products.
- The individual is clearly given an opportunity to freely and easily oppose the use of their email address for marketing purposes when the email address is collected and in every subsequent marketing message.

(Section 19, Marketing Act.)

Marketing emails, including those sent to a legal person, must always contain a valid address recipients can contact to opt-out of marketing messages (Section 20, Marketing Act).

Traders may use other methods of communication, such as telemarketing, unless an individual has clearly opted out (Section 21, Marketing Act). Individuals who do not want to receive marketing calls can register in the NIX-Telefon system.

International Transfer of Data

Transfer of Data Outside the Jurisdiction

20. What rules regulate the transfer of data outside the jurisdiction?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1). The GDPR allows controllers and processors to transfer personal data within the European Economic Area (EEA) if a lawful basis for the processing exists (see Question 9 and Question 10). Otherwise, it only allows for transfers of personal data outside of the EEA to third countries and international organizations based on:

- Adequacy decisions.

- Appropriate safeguards, such as standard contractual clauses and binding corporate rules.
- Derogations from the general prohibition.
- Nonrepetitive transfers.

(Articles 44 to 49, GDPR.)

For more on cross-border transfers under the GDPR, see Country Q&A, Data Protection in the EU: Overview: Question 20.

The GDPR allows EU member states, for important public interest reasons, to enact national laws limiting the cross-border transfer of specific categories of personal data if the destination country has not been deemed to provide an adequate level of data protection (Article 49(5), GDPR). The Data Protection Act (2018:218) (in Swedish) does not address GDPR Article 49(5).

For more on:

- Cross-border data transfer agreements, see Question 22.
- Regulatory guidance after the EU Court of Justice's (ECJ) ruling in Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (Case C-311/18) EU:C:2020:559 (Schrems II), see EU Cross-Border Data Transfers: Regulatory Guidance Post Schrems II Tracker.
- General and country-specific resources to help organizations comply with data protection laws when transferring personal data across borders, see Cross-Border Personal Data Transfers Toolkit.

21. Is there a requirement to store any type of personal data inside the jurisdiction?

Neither the EU General Data Protection Regulation (Regulation (EU) 2016/679) nor Sweden's Data Protection Act (2018:218) (in Swedish) require controllers to store any type of personal data in any specific jurisdiction.

Sweden's Bookkeeping Act (1999:1078) (in Swedish) imposes limited data localization requirements (see Country Q&A, Data Localization Laws: Sweden). Other sectoral laws may impose additional data localization requirements, but are outside the scope of this Q&A.

Data Transfer Agreements

22. Are data transfer agreements contemplated or in use? Has the supervisory authority approved any standard forms or precedents for cross-border transfers?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1). For cross-border data transfers to third countries without an adequacy decision, controllers can meet the GDPR's requirements by using data transfer agreements, such as:

- Standard contractual clauses that the European Commission (EC) has adopted.
- Standard contractual clauses that a national supervisory authority has adopted and the EC has approved.
- Other contractual clauses that a competent national supervisory authority has approved.

(Article 46(2), (3), GDPR.)

The Swedish Authority for Privacy Protection (IMY) has not approved any standard data protection clauses for cross-border transfers under GDPR Article 46(2)(d), but has stated that controllers in Sweden may use the standard contractual clauses developed by the Danish Data Protection Authority (see IMY: Danish standard contractual clauses may be used in Sweden (in Swedish)).

For more on rules regulating cross-border data transfers in Sweden and the EU respectively, including other possible mechanisms to legally transfer data, see Question 20 and Country Q&A, Data Protection in the EU: Overview: Question 20 and Question 22.

23. For cross-border transfers, is a data transfer agreement sufficient, by itself, to legitimize transfer?

See Question 20 and Question 22.

24. Must the relevant supervisory authority approve the data transfer agreement for cross-border transfers?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1). The Swedish Authority for Privacy Protection (IMY) does not need to approve a data transfer agreement that uses unamended Standard Contractual Clauses (SCCs). However, the IMY must approve data transfer agreements that amend or supplement the SCCs in a way that directly or indirectly contradicts the measures provided for in the SCCs (Article 46(3), GDPR). For more information on the IMY's notification, registration, or authorization requirements before transferring personal data cross-border,

see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: Sweden: Question 2 and Question 3. For the IMY's contact information, see Regulator Details.

Enforcement and Sanctions

25. What are the enforcement powers of the supervisory authority?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1). For more on the enforcement powers supervisory authorities have under the GDPR, see Country Q&A, Data Protection in the EU: Overview: Question 25.

GDPR Article 54 requires each EU member state to establish a supervisory authority. Section 2a of Ordinance (2007:975) on Instructions for the Swedish Authority for Privacy Protection (in Swedish) (Ordinance 2007:975) establishes the Swedish Authority for Privacy Protection (IMY) as the supervisory authority under the GDPR. The IMY has:

- The powers specified in GDPR Article 58(1) to (3) (Chapter 6, Section 1, Data Protection Act (2018:218) (in Swedish)).
- Additional powers set out in Ordinance (2007:975).

26. What are the sanctions and remedies for non-compliance with data protection laws?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Question 1). For more on the GDPR's enforcement and applicable sanctions, see Country Q&A, Data Protection in the EU: Overview: Question 26 and Practice Note, Enforcement, Sanctions, and Remedies under the GDPR.

The GDPR permits EU member states to specify whether and to what extent supervisory authorities may impose administrative fines on public authorities and bodies (Article 83(7), GDPR). The Data Protection Act (2018:218) (in Swedish) (Swedish Act) grants the Swedish Authority for Privacy Protection (IMY) the authority to impose the following administrative fines on public bodies:

- Up to SEK5 million for violations set out in GDPR Article 83(4).
- Up to SEK10 million for violations set out in GDPR Article 83(5) and (6).

(Chapter 6, Section 2, Swedish Act.)

GDPR Article 83(1) to (3) applies to the IMY when determining the amount of any administrative penalty for public authorities and bodies (Chapter 6, Section 2, Swedish Act).

In addition to the fines applicable under GDPR Article 83, the GDPR permits EU member states to specify penalties applicable to GDPR violations that are not subject to administrative fines under this article (Article 84, GDPR). The Swedish Act makes use of this derogation and imposes administrative fines for violations of GDPR Article 10, the penalty to be determined by the application of GDPR Article 83(5) (Chapter 6, Section 3, Swedish Act).

Regulator Details

Swedish Authority for Privacy Protection (IMY)

W www.imy.se (in Swedish)

Main areas of responsibility. The IMY's primary responsibility is to detect and prevent threats to personal integrity. Its operations are focused on areas expected to be particularly sensitive from an integrity perspective, new technological phenomena and applications, and areas where the risk of abuse or faulty use could be particularly significant.

The IMY is responsible for enforcing, among other things:

- The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR).
- Sweden's Data Protection Act (2018:218) (in Swedish) supplementing the GDPR.
- Other relevant laws with data protection implications (see Question 1).

Contributor Profile

Anna Fernqvist Svensson, Partner

Hellström Advokatbyrå
T +46 709 55 09 15
E anna.fernqvist@hellstromlaw.com
W www.hellstromlaw.com/en/

Professional qualifications. Sweden, Advokat, 2001

Areas of practice. Commercial law; competition and markets; employment and data protection.

END OF DOCUMENT

RESOURCE HISTORY

Law stated date updated following periodic maintenance.

This document has been reviewed by the author as part of its periodic maintenance to ensure it reflects the current law and market practice on January 1, 2024.

Review Completed on December 7, 2022.

We reviewed this resource on December 7, 2022 to ensure it reflects the most current law and market practice. We did not make any substantive changes to this document.

ECJ Decision Expanding the Scope of GDPR Article 9.

On September 6, 2022, we updated Question 11 to reflect the EU Court of Justice decision in Case C-184/20: OT v Vyriausioji tarnybin#s etikos komisija (Chief Official Ethics Commission, Lithuania), which held that processing personal data that may indirectly reveal sensitive information concerning an individual is prohibited under GDPR Article 9(1), unless a GDPR Article 9(2) exception applies.

Review Completed July 21, 2020.

We reviewed this resource on June 21, 2020 to ensure it reflects the most current law and market practice. We have made significant revisions for clarity and readability, including supplementing each answer with relevant statutory links to the GDPR and Sweden's data protection laws.

Related Content

Practice note: overview

Global Data Protection Authorities Chart: Overview • Law stated as of 13-Nov-2023
Personal Data Definitions Global Comparison Chart: Overview • Law stated as of 30-Jun-2023
Global Data Breach Notification Laws Chart: Overview • Law stated as of 28-Dec-2023

Practice notes

Swedish Implementation of the GDPR • Law stated as of 01-Dec-2023

Country Q&A

Data Localization Laws: Sweden • Law stated as of 02-Feb-2023
GDPR Derogations: Sweden • Law stated as of 01-Dec-2023
Records Retention: Sweden • Law stated as of 30-Jun-2022

Toolkit

Cross-Border Personal Data Transfers Toolkit • Maintained
GDPR National Implementation Legislation Toolkit • Maintained

