Global Data and Cyber Handbook - Sweden

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# What's new?

## Recently Updated Topics

*Last review date: 27 December 2024*

Updates to this chapter for the 2025 edition of the Global Data Privacy and Security Handbook primarily consists of the Swedish regulators' enforcement during 2024 and future supervision for 2025, and additional information on processing of personal data in the employment context, relating to use of AI tools, profiling and automated decision-making, and within the transactional context. Furthermore, the Swedish Authority for Privacy Protection has issued Regulation IMYFS 2024:1 enabling processing of personal data relating to criminal offences and convictions for the purposes of conducting screening against third country sanctions lists. There are also minor changes to sections on certain provisions and applicability.

The implementation of the NIS 2 directive has been postponed in Sweden and will most likely not be entered into force until the summer of 2025. The Swedish DPA issued three administrative fines in 2024. Further, the Swedish DPA issued a number of decisions that did not result in any administrative fines, but where the controller was left with, e.g., a reprimand or ban on the non-compliant processing activity.

# Key Data & Cyber Contacts

# Key Data & Cybersecurity Laws

## How are data and cybersecurity laws/regulations implemented?

*Last review date: 27 December 2024*

☒   omnibus – all personal data

☒   sector-specific

E.g., telecoms/electronic communications, healthcare sector, camera surveillance, credit reference agencies and debt recovery agencies

☒   constitutional

## What are the key data privacy laws and regulations?

*Last review date: 27 December 2024*

*Please refer to the* [*EU Chapter*](https://resourcehub.bakermckenzie.com/en/en/resources/global-data-and-cyber-handbook/emea/eu)*for detailed information regarding EU-wide legislation.*

[EU General Data Protection Regulation](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679)

[Swedish Personal Data Protection Act](https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218)

[Swedish Personal Data Protection Regulation](https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2018219-med-kompletterande_sfs-2018-219)

[Swedish Criminal Data Act](https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsdatalag-20181177_sfs-2018-1177)

The Swedish Criminal Data Act (implementing the EU Data Protection Law Enforcement Directive) applies to personal data processing within law enforcement activities such as the Swedish Police Authority and hospitals if someone is sentenced to compulsory psychiatric care.

[Swedish Camera Surveillance Act](https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/kamerabevakningslag-20181200_sfs-2018-1200)

The Swedish Camera Surveillance Act supplements the EU GDPR and applies to processing of personal data in connection with camera surveillance.

[Swedish Patient Data Act](https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/kamerabevakningslag-20181200_sfs-2018-1200)

The Swedish Patient Data Act stipulates requirements for public and private healthcare providers' personal data processing in relation to healthcare activities, including the obligation to keep medical records.

[Swedish Police Data Act](https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181693-om-polisens-behandling-av_sfs-2018-1693)

The Swedish Police Data Act supplements the Swedish Criminal Data Act in relation to personal data processing carried out by the Swedish Police Authority, the Swedish Economic Crime Authority, and the Swedish Security Service.

[Swedish Electronic Communications Act](https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2022482-om-elektronisk-kommunikation_sfs-2022-482/)

The Swedish Electronic Communications Act covers electronic communications networks, services imposing certain extended legal requirements for companies with significant market power and influence. The act includes certain provisions to enhance the security and integrity of electronic communications requiring operators to take appropriate measures to manage risks. The act also outlines the responsibilities of the Swedish Post and Telecom Authority, which is the supervising authority.

The act regulates the use of cookies. For example, the law states that operators must obtain user consent before storing or accessing information on a user’s device, such as through cookies. Users must be informed about the purpose of the data collection and given the option to refuse. Storage and access of data is, however, permitted without consent if it is needed for the transmission of electronic messages or necessary for the providing of a service that has been explicitly requested by the user.

## What are the key cybersecurity laws and regulations?

*Last review date: 27 December 2024*

*Please refer to the* [*EU Chapter*](https://resourcehub.bakermckenzie.com/en/en/resources/global-data-and-cyber-handbook/emea/eu) *for detailed information regarding EU-wide legislation.*

[Swedish Act on Information Security for Essential Services and Digital Services](https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174)

The Swedish Act on Information Security for Essential Services and Digital Services (implementing the EU Directive on Security of Network and Information Systems, the **NIS Directive**) stipulates cybersecurity requirements for essential services and digital services. The Swedish Act on Information Security for Essential Services and Digital Services applies to providers of essential transport with its primary establishment in Sweden, and to providers of digital services with its primary establishment in Sweden, e.g., online marketplaces, search engines and cloud services. Please see below for further information on the Swedish implementation of the NIS2 Directive.

Note that the **EU Dual-Use Regulation** may be applicable to cybersecurity solutions. This means that in the event that a cybersecurity solution is subject to control under the Dual-Use Regulation, and export controls subsequently apply, a license would be required in order to export the solution.

## What are the key laws and regulations relating to non-personal data?

*Last review date: 27 December 2024 Please refer to the* [*EU Chapter*](https://resourcehub.bakermckenzie.com/en/en/resources/global-data-and-cyber-handbook/emea/eu)*for detailed information regarding EU-wide legislation.*

[The Swedish Accounting Act](file:///C:/Users/gsbmam/AppData/Roaming/iManage/Work/Recent/Knowledge.KNOWLEDGE%20_%20IPTech%20and%20CG_R%20Content%20Development%20Team.10000000495%20_%20EMEA/The%20Accounting%20Act%20(1999:1078)) (1999:1078)

The Swedish Accounting Act regulates accounting, financial record keeping and reporting in Sweden. The act mandates an accurate collection and systematic recording of all business transaction. The Act also mandates that companies share relevant accounting information with auditors and relevant authorities.

## Are new or material changes to those key data and cybersecurity laws anticipated in the near future?

*Last review date: 27 December 2024*

*Please refer to the* [*EU Chapter*](https://resourcehub.bakermckenzie.com/en/en/resources/global-data-and-cyber-handbook/emea/eu) *for detailed information regarding EU-wide legislation.*

The **NIS2 Directive**, which in particular broadens the scope of application and also extends the relevant obligations in comparison to NIS, requires Member States to apply implementing measures from 17 October 2024. For Sweden, the government has through an inquiry presented its proposal for Swedish implementation of the NIS2 Directive with the proposed date of entry into force set to 1 January 2025. However, the new regulation in Sweden, following delays in the legislative procedure, will most likely not be entered into force until the summer of 2025.

# Regulators, Enforcement Priorities and Penalties

## Who are the main data privacy, non-personal data and/or cybersecurity regulator(s) in the jurisdiction?

*Last review date: 27 December 2024*

Sweden has one national data protection authority. For the Electronic Communications sector and with respect to Cybersecurity, there are  additional authorities:

Data protection - [The Swedish Authority for Privacy Protection](https://www.imy.se/en/) ("**Swedish DPA**")

Electronic communication - [The Swedish Post and Telecom Authority](https://pts.se/en/)

Cybersecurity – The Swedish Civil Contingencies Agency

## How active is each of the regulator(s)?

*Last review date: 27 December 2024*

**The Swedish DPA**

With respect to key enforcement activities, the Swedish DPA issued three administrative fines in 2024 for a total amount of SEK 60,000,000 (approx. USD 5,400,000). Further, the Swedish DPA issued a number of decisions that did not result in any administrative fines, but where the controller was left with, e.g., a reprimand or ban on the non-compliant processing activity. All of the decision issued by the Swedish DPA in 2024 were issued on the basis of personal data being transferred via an analytics tool used by the affected companies on their websites.

The three supervisory cases in which the Swedish DPA issued administrative fines during 2024 concerned  failure in implementing appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR Regulation. Two of the cases of breach resulting in fines involved the transfer of information regarding customers’ orders. The companies had, among other things, transferred data containing information about purchases of over certain sensitive information (resulting in administrative fines of SEK 8,000,000 (approx. USD 725,000), and SEK 37,000,000 (approx. USD 3,360,000) respectively). Furthermore, a Swedish bank was issued an administrative fine on similar legal grounds. The bank had also used an analytics tool on its website and app, which resulted in the transfer of information pertaining to customers’ securities holdings and account numbers to a third party. According to the banks own report of the incident, personal data of up to one million individuals were improperly transferred to a third party, resulting in an administrative fine of SEK 15,000,000 (approx. USD 1,360,000).

Lastly, three companies were subject to reprimands from the Swedish DPA following breaches pertaining to the usage of analytic tools. For these three companies, however, no fines were issued by the Swedish DPA following the authority's conclusion that the violations were to be characterized as minor, taking into account that the companies after the discovery of the breach subsequently implemented various measures to enhance their IT security

In particular, in comparison to 2023 (where eleven administrative fines for a total amount of SEK 120  million (approx. USD 11,000,000) were issued), 2024 saw a relative decrease in not only the Swedish DPA's willingness to issue administrative fines, but in overall activity and the total monetary amount imposed in fines as well.

**The Swedish Post and Telecom Authority**

During 2024, the Swedish Post and Telecom Authority has conducted two focused reviews resulting in injunctions and/or fines. The authority has stated that two Swedish companies have  failed to provide adequate contractual informationto consumers and has ordered that each company pay a fine of SEK 250,000 (approx. 23,000 USD). The supervisory body has specified that the upcoming implementation of NIS 2 will bring about substantial modifications for companies under its jurisdiction, and that certain interim regulations must already be complied with by these entities.

**The Swedish Civil Contingencies Agency**

The Swedish Civil Contingencies Agency (**“MSB”**) has given notice of a response to the legislative consultation concerning the Swedish implementation of the NIS2 Directive, emphasizing the importance of coordinated regulation to make efforts to increase resilience more effective for all actors in the system. In particular, the agency has highlighted that it is particularly important that:

The requirements for those covered are clear and cohesive,

NIS 2 and CER are implemented as a unified regulation, and

The work with NIS 2-CER is coordinated with the existing civil preparedness system, into a common structure to strengthen total defense.

The Swedish Civil Contingency Agency (**“MSB”**) has highlighted that it is not yet clear what the new regulation will look like. Organizations not currently covered by NIS and wishing to prepare for the legislative changes can, according to the agency, benefit from reviewing existing regulations on information security and security measures.

## What are each of the regulator's anticipated enforcement priorities for the next 12 months?

*Last review date: 27 December 2024*

**The Swedish DPA**

With respect to priorities anticipated for the near future, the Swedish DPA has stated that the authority has received increased funding from the Swedish government with the aim of enhancing its capacity to adapt its operations to a changing legal landscape regarding complaint handling, new responsibilities arising from EU regulations, an increased need for oversight of camera surveillance due to amendments in the Swedish Camera Surveillance Act, and a growing demand for guidance from various sectors concerning data protection related to technological development and innovation. According to the Swedish DPA's Strategic Target Plan for 2022-2025, the DPA will increase its support for individuals and will continue to carry out its supervision primarily on the basis of complaints from individuals. The DPA will also aim to improve data protection compliance across private and public organizations by, e.g., providing clear legal positions on various legal issues and increasing supervisory activities, as well as observe technological development and provide guidance and support to this end.

Note that the Swedish DPA has seen a significant increase in its budget for the second year in a row, which may consequently lead to higher enforcement activity. Following the previous increase in funding a trend in increased enforcement activity during 2024, however, has not been observed.

It is currently unclear if the supervision of adherence of the EU AI regulation will fall under the DPA’s supervising authority, though this is a potential future development. The authority has affirmed that it will strive to make sure the AI regulation is not viewed as a burden by offering guidance and advocating for enhanced transparency and predictability.

**The Swedish Post and Telecom Authority**

The Swedish Post and Telecom Authority is as of 2 August 2024, the competent authority for the supervision of the sections of the European Data Governance Act that govern providers of data intermediation services and data altruism organizations. The authority has also been given a certain mandate regarding the reuse of protected data. According to the authority's own statement, the authority is to ensure compliance with the regulations and to receive and process complaints within this domain.

## What trends are you seeing in regulatory investigations relating to data & cyber?

*Last review date: 27 December 2024*

Regulatory investigations or direct enforcement activity by data or cyber regulators are:

☒         Rare

☒         Staying the same

Class actions/group actions under data or cyber regulation are:

☒         Rare

☒         Staying the same

## What are the potential penalties/remedies for non-compliance with the key data and cybersecurity laws in the jurisdiction?

*Last review date: 27 December 2024*

There are:

☒   administrative remedies / civil penalties applied by regulators and law enforcement

These amount to up to EUR 20 million or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

☒   private remedies

Individuals may, for example:

Individuals may, for example:

file complaints with the data protection authorities

claim damages for material or non-material damages

## If data subjects have private remedies, what form can these remedies take?

☒   individual personal actions

☒   representative actions (e.g., brought by a consumer / data privacy body or the supervisory authority)

☒   class actions

# Key Definitions

## Personal data

*Last review date: 27 December 2024*

"Personal data" means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

## Sensitive/special personal data (including personal data subject to additional protections/ restrictions/breach notification obligations)

*Last review date: 27 December 2024*

Sensitive data includes:

☒   personal data revealing racial or ethnic origin

☒   personal data revealing political opinions

☒   personal data revealing religious or philosophical belief

☒   personal data revealing trade / professional union or association membership

☒   genetic data

☒   biometric data for the purpose of uniquely identifying a natural person or biometric templates

☒   data concerning health/medical information

☒   data concerning a natural person's sex life or sexual orientation

☒   financial information

☒   government identity card or number information

☒   personal data regarding an individual's criminal convictions or record

☒   other

Processing of national personal identity numbers is subject to additional requirements for processing. Where there is no consent, the processing needs to be clearly justified by its purpose, the importance of positive identification, or another noteworthy reason.

Note that there are other categories of personal data that are particularly worthy of protection, which may require the same security measures as sensitive personal data. Such personal data may include:

financial information

information about a person having committed a crime

•valuating data such as information from performance reviews, results of personality tests or profiles

information relating to a person's private sphere

information about social conditions

## Controller vs Processor

*Last review date: 27 December 2024*

**Do the privacy laws distinguish between controllers/owners and processors/agents? Whereby:**

the controller/owner is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

the processor/agent is natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

**Answer:** Yes.

The concepts of controller and processor are defined in the GDPR.

# Territorial Scope

## What is the territorial reach of the data privacy and cybersecurity laws?

*Last review date: 27 December 2024*

☒   applies to organizations located in the jurisdiction

☒   applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction

☒   applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction

# Legal Bases for Processing of Personal Data

## Is an identified legal basis required in order to collect or process non-sensitive personal data?

*Last review date: 27 December 2024*

Yes.

The following are potential legal bases for processing personal data:

☒   the data subject has provided consent to the processing for the identified purposes

☒   the personal data is necessary to perform a contract with the data subject

☒   the personal data is necessary to comply with a legal obligation

☒   the personal data is necessary to protect the vital interests of a natural person

☒   the personal data is necessary for a public interest

☒   the personal data is necessary to fulfil a legitimate interest of the controller or third party (provided that the interest is not overridden by the data subject's privacy interests and the data subject has not made use of his/her right to object)

☒   other

Please see section 8 regarding personal data or sensitive personal data in the employment context.

## Is an identified legal basis required in order to collect or process sensitive personal data?

*Last review date: 27 December 2024*

Yes.

The following are potential legal bases for processing special categories of personal data:

☒  the data subject has given consent to the processing, where consent is measured to a higher standard than for non-sensitive personal data (for example, additional requirement for consent to be "explicit")

☒   processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law

☒   processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

☒   processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and further conditions

☒   processing relates to personal data which are manifestly made public by the data subject

☒   processing is necessary for the establishment, exercise or defense of legal claims

☒   processing is necessary for reasons of substantial public interest

☒   processing is necessary for the purposes of medicine, the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

☒   processing is necessary for reasons of public interest in the area of public health

☒   processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

☒   other

Note that processing of special categories of personal data (sensitive personal data) requires both a legal basis under Article 6 of the GDPR and a separate condition / exception for processing under Article 9 of the GDPR.

Private bodies may process special categories of personal data for health and social care purposes, archiving in the public interest if prescribed by law, and statistics, where the statistical purpose clearly outweighs the risk of intrusion of the data subject's integrity.

Processing of national personal identity numbers is subject to additional requirements for processing. Where there is no consent, the processing needs to be clearly justified by its purpose, the importance of positive identification, or another noteworthy reason.

According to Sections 6 and 7 of the The Swedish DPA regulations on the processing of personal data related to criminal offenses (IMYFS 2024:1), which was admitted in November 2024, certain companies are permitted to process such personal data as referred to in Article 10 GDPR (personal data related to criminal offenses) for the purpose of screening, for example, customers, suppliers, and employees against third country sanctions lists.

Following IMYFS 2024:1, companies under the inspection of the Swedish Inspectorate of Strategic Products or the [Swedish Radiation Safety Authority](https://bing.com/search?q=Str%c3%a5ls%c3%a4kerhetsmyndighetens+in+english)  are in some instances permitted to screen and process personal data, with certain limitations, against third countries sanction lists.

Furthermore, companies under the supervision of the Swedish Financial Supervisory Authority (FI) have also been granted the ability to process personal data related to criminal offenses for screening against sanctions lists. However, in order for the data processing to be deemed permissible, such processing must be necessary to comply with the Swedish Act (2017:630) on Measures against Money Laundering and Terrorist Financing, other regulations, or rules in the financial market area issued by foreign authorities, EU bodies, or intergovernmental organizations.

It should be noted that, in order for the exemptions set out in IMYFS 2024:1 to be applicable, the processing of the data must be necessary to comply with mandatory regulations and rules. The evaluation concerning if the data processing is to be deemed necessary, should be conducted taking into account the same variables as set out in Article 6.1GDPR.

Lastly, the regulation also stipulates that sanctions lists against which the screening is conducted has to have been established through a democratic process and made publicly available on the websites of issuing authorities or intergovernmental organizations in order for the data processing to be deemed permissible. Internal lists created by individual companies or corporate groups are therefore not covered by the provisions.

## Are there special requirements that apply to the collection or processing of personal data from minors?

*Last review date: 27 December 2024*

Yes.

In accordance with the UN Convention on the Rights of the Child (ratified by all EU Member States), a child is a person under the age of 18 years. However, in the case of the special provision on consent to the processing of personal data for the use of information society services, a child of 13 years may give valid consent.

## In what circumstances do these special requirements apply?

*Last review date: 27 December 2024*

☒   in the context of information society services (e.g., a commercial website) only if processing is based on consent

## What are the special requirements that apply to collecting or processing personal data from minors?

*Last review date: 27 December 2024*

☒   consent must be given or authorized by the parent/ guardian of the minor

☒   additional data subject rights are granted to minors (e.g., deletion, access, transparency)

Note that data controllers have an obligation in accordance with the transparency measures addressed to children (Article 12(1) of the GDPR and Recitals 38 and 58).

# Information Requirements, Data Subject Rights, Accountability and Governance

## What information needs to be included in a privacy notice to data subjects?

*Last review date: 27 December 2024*

☒   the identity and the contact details of the controller and, where applicable, of the controller's representative

☒   the contact details of the data protection officer, where applicable

☒   the purposes of the processing for which the personal data is intended

☒   the legal basis for the processing

☒   the categories of personal data concerned

☒   the source from which the personal data originates, and if applicable, whether it came from publicly accessible sources

☒   the legitimate interests pursued by the controller or by a third party if processing is based on the legitimate interests ground

☒   the recipients or categories of recipients of the personal data, if any

☒   information regarding data transfers to third countries, where applicable, and reference to appropriate or suitable safeguards and the means by which by to obtain a copy of them or where they have been made available

☒   the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period

☒   the existence of data subjects' rights, such as the right to access, rectification, erasure, data portability, etc.

☒   the existence of the right to withdraw consent if processing is based on consent

☒   the right to lodge a complaint with a supervisory authority

☒   whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

☒   if applicable, information regarding automated decision making, including profiling

Note that the Swedish DPA issued an administrative fine to a bank for the amount of SEK 7.5 million (approx. USD 719,000) for its failure to fulfil its information and transparency requirements in relation to its data subjects. The Swedish DPA's decision includes comments on how a data controller should fulfil the basic principle of transparency and the data subjects' right to information.

## Do data subjects have specific privacy rights that must be operationalized?

*Last review date: 27 December 2024*

Yes.

Data subjects have the following data privacy rights, although the specifics of the scope and conditions for each of these vary depending on the circumstances and local law:

☒   right to access the data subject's own personal data

☒   right to rectify/correct the data subject's own personal data where inaccurate or incomplete

☒   right to erasure of personal data

☒   right to restrict data processing

☒   right to data portability

☒   right to object to the processing of personal data

☒   right to withdraw consent

☒   other

right to claim damages

Note that the Swedish DPA has issued a large administrative fine for non-compliance with the data subject's right of access under Art. 15 of the GDPR.

## Are there accountability and governance requirements?

*Last review date: 27 December 2024*

Yes.

There are accountability and governance requirements to:

☒   take privacy by default and design measures for all processing of personal data

☒   perform and document data protection impact assessments (DPIAs) for high-risk processing:

The Swedish Authority for Privacy Protection issued a list of examples of processing activities for which DPIAs shall be made (available only in Swedish [here](https://www.imy.se/globalassets/block/verksamhet/dataskydd/forteckning---konsekvensbedomningar.pdf)).

☒   maintain a record of processing activities

☒   implement appropriate measures to comply with data privacy and cybersecurity

☒   demonstrate compliance with data privacy and cybersecurity

☒   identify a specific individual as the data privacy contact for data subject or data protection authority inquiries

☒   provide training to employees

☒   audit or supervise data processors

☒   appoint a local representative in the jurisdiction (if the controller or processor is not located in the jurisdiction)

# DPOs and Notification Requirements

## Is the concept of data protection officer (DPO) recognized in the jurisdiction?

*Last review date: 27 December 2024*

Yes.

## Are there circumstances in which it is mandatory to appoint a DPO or similar position?

Yes.

If yes, under what circumstances?

☒   the processing is carried out by a public authority or body, except for courts acting in their judicial capacity

☒   the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale

☒   the core activities of the controller or the processor consist of processing on a large scale of special categories of data

## Where a DPO is appointed, does the DPO have to meet specific requirements?

*Last review date: 27 December 2024*

Yes.

If yes, what are these requirements?

☒   legal qualifications / experience

☒   other professional qualifications / experience

According to the GDPR, a DPO shall possess the professional qualities and expert knowledge of data protection law and practice enabling them to fulfil their role.

According to the WP29 guidelines, the level of expertise depends on the sensitivity, volume and complexity of data processed and whether data transfers are systematic or occasional. The DPO shall have an in-depth understanding of the GDPR and expertise in national and EU laws, knowledge of the business sector of the organization and sufficient understanding of processing operations, information security and information systems.

## Are there obligations to notify, submit filings to, register with or obtain approval from local data protection authorities to collect and/or process personal data generally?

*Last review date: 27 December 2024*

No.

# Data Processors

## Are there obligations for controllers to establish controls with respect to data processors?

*Last review date: 27 December 2024*

Yes.

The obligations are as follows:

☒   controllers must conduct due conduct diligence on the processor to ensure it will provide appropriate security and processing of the personal data

☒   controllers must only use processors subject to a written agreement that complies with specific requirements

## Are there any direct regulatory or statutory requirements on processors?

*Last review date: 27 December 2024*

Yes.

The following provisions apply directly to processors:

Art. 28, 29, 30(2), 31, 32, 33(2), 37 et seq., 44 et seq. GDPR.

# International Data Transfer

## Are there restrictions on the transfer of personal data to third countries?

*Last review date: 27 December 2024*

Yes.

Third country is not defined in the GDPR but means countries (1) outside of the European Union, and (2) countries outside of the European Economic Area.

Transfers of personal data to third countries are only permissible if there is a legal basis for the processing/transfer and one of the following applies:

☒   approved adequate/whitelisted jurisdictions

☒   to holders of specific certifications or followers of specific code of conduct programs each approved by the relevant data protection and cybersecurity authority (e.g., EU-US Data Privacy Framework)

☒   approved standard contractual clauses

☒   binding corporate rules

☒   derogations, such as consent, contract performance, necessity to establish, exercise or defend legal claims

☒   other solutions

***Please see separate question for information on data localization provisions that are not restricted to personal data.***

In case of a singular transfer that only affects a limited number of data subjects and where legitimate interests can be demonstrated following a balancing test, the data subject and the Data Protection Authority shall also be informed about the transfer. Please note that the transfer also requires that the controller has assessed all the circumstances surrounding the data transfer and has, based on that assessment, provided suitable safeguards with regard to the protection of personal data.

# Cookies, Online Tracking and Direct Marketing

## Are there specific requirements for the use of cookies and other online tracking technologies?

*Last review date: 27 December 2024*

Yes.

Cookies are regulated by Chapter 9 Section 28 of the Swedish Electronic Communications Act. The provision states that cookies are only allowed to be used if the user of the electronic communication service has been informed of the purpose for the use of cookies and consented to that use.

## Are there specific requirements related to the use of personal data for direct marketing activities?

*Last review date: 27 December 2024*

Yes.

**☒   email marketing**

☒   prior opt-in consent

☒   prior existing business relationship (and subject to other requirements) with opt-out consent

**☒   telephone marketing**

☒   opt-out or implied consent

**☒   SMS/text message marketing**

☒   prior opt-in consent

☒   prior existing business relationship (and subject to other requirements) with opt-out consent

**☒   postal marketing**

☒   opt-out or implied consent

**☒   online behavioral advertising targeting/social media targeting/ad personalization marketing**

☒   prior opt-in consent

# Data Processing in the Employment Context

## Is an identified legal basis required in order to collect or process personal data or sensitive personal data in the employment context?

*Last review date: 27 December 2024*

Yes.

According to the Swedish Data Protection Act, processing of sensitive personal data within the employment context is permitted on the basis of 9.2 (b) of the GDPR if:

it is necessary to exercise rights or comply with legal obligations derived from labour law, social security and social protection law

Such sensitive personal data within the employment context is only allowed to be transferred to a third party if:

it is required by law or if the data subject has given its explicit consent thereto.

## Can consent be validly obtained in the employment context?

*Last review date: 27 December 2024*

☒   Yes, but this consent is typically more difficult to establish in an employment context (specify details below)

Even though it is not expressly stated that consent cannot be validly obtained in the employment context, it shall be noted that recital 43 states: "consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller". This could be the case in the employment relationship, which is also explicitly mentioned by the Swedish DPA in its online guidance.

That being said, a valid consent can be obtained in the employment context in some cases, e.g., for the purposes of processing personal data in order to manage voluntary extracurricular activities at the workplace.

When asking for consent, the controller must do so in a clear manner. This means that it must explain in detail what the data subject agrees to regarding the category of data that is to be processed, the purpose of the processing and who will conduct the processing. When asking for consent, it must not be bundled with requirements of the data subject. Furthermore, the consent must be voluntary and should allow the data subject to withdraw without negative consequences.

## Has the data privacy regulator issued guidance on use of artificial intelligence, automated decision making or profiling in an employment context – for example, relating to use in employee monitoring or hiring?

*Please refer to the* [*EU Chapter*](https://resourcehub.bakermckenzie.com/en/en/resources/global-data-and-cyber-handbook/emea/eu) *for detailed information regarding EU-wide guidance.*

☒         No

No guidance on this specific issue has been produced at a national or European level.

# Artificial Intelligence, Profiling and Automated Decision Making

## Are there any restrictions or requirements related to creating profiles of data subjects or utilizing automated decision-making for decisions related to data subjects, including with respect to artificial intelligence?

*Last review date: 27 December 2024*

Yes.

The restrictions or requirements are as follows:

☒   qualified right not to be subject to a decision based solely on automated decision making, including profiling – for example, only applicable if the decision produces legal effects concerning them or similarly significantly affects them

☒  right to information / transparency requirement

☒  right to request human review of the automated decision making

☒  other

Note that the right to request human review of the automated decision-making consists of the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision, where the decision (i) is necessary for a contract between the data subject and the controller, or (ii) is based on the data subject's consent.

## If such restrictions or requirements exist, are they subject to any exceptions?

*Last review date: 27 December 2024*

Yes.

The exceptions are as follows:

If the decision:

is necessary for entering into, or performance of, a contract between the data subject and a data controller

is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights/freedoms and legitimate interests

is based on the data subject's explicit consent

## Has the data privacy regulator issued guidance on data privacy and artificial intelligence, automated decision-making or profiling?

*Last review date: 27 December 2024*

Yes. *Please refer to the* [*EU Chapter*](https://resourcehub.bakermckenzie.com/en/en/resources/global-data-and-cyber-handbook/emea/eu)*for detailed information regarding EU-wide guidance.*

## Has the data privacy regulator taken enforcement action in relation to artificial intelligence, including automated decision-making or profiling?

*Last review date: 27 December 2024*

☒         No enforcement activity to date

## Do other (non-personal data or cybersecurity) laws or regulations impose restrictions on use of artificial intelligence, automated decision-making or profiling?

*Last review date: 27 December 2024*

☒   Yes, laws in force

☒  Draft legislation in progress

*Please refer to the* [*EU Chapter*](https://resourcehub.bakermckenzie.com/en/en/resources/global-data-and-cyber-handbook/emea/eu) *for detailed information regarding EU-wide legislation.*

# Data privacy and cybersecurity in a transactional context

## Has the data privacy authority issued any guidance on data privacy compliance in the context of transactional activity (including, but not limited to, share sales, asset sales, reorganizations or spinouts)?

*Last review date: 27 December 2024:*

☒   No

No guidance on this specific issue has been produced at a national or European level.

## In the context of an asset sale (the sale of a separate business unit as a going concern), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the assets that are the subject of the asset sale)?

*Last review date: 27 December 2024*

☒  It depends (for example, on the way the asset sale is structured, and/or the assets being acquired)

## If so, how would any regulatory fines be calculated?

*Last review date: 27 December 2024*

☒  Unclear

## In the context of a share sale (where the acquiring entity acquires 100% of the shares of a target company), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the target company)?

*Last review date: 27 December 2024*

☒  Yes

## If so, how would any regulatory fines be calculated?

*Last review date: 27 December 2024*

☒  Unclear

# Security Requirements and Breach Notification

## Do data privacy laws or regulations impose obligations to maintain information security controls to protect personal data from unauthorized access or processing?

*Last review date: 27 December 2024*

Yes.

☒   general obligation to take appropriate / reasonable technical, physical and/or organizational security measures

☒   reasonable security controls

☒   encryption

Encryption is considered by the GDPR as an example of what can constitute an appropriate technical and organizational measure. According to the Swedish Post and Telecom Authority's binding regulation PTSFS 2014:1, art. 9, the following applies when data is processed when providing an electronic communication service: If the data is transferred over the internet, encryption is a requirement. This does not apply if the transfer is made to the user himself or to another party to whom the user has agreed that the data may be transferred.

Encryption is also a requirement for the processing of patient data in accordance with the regulations of the Swedish National Board of Health and Welfare.

## Do other laws or regulations impose obligations to protect systems from cyberattack?

*Last review date: 27 December 2024*

☒   health regulatory requirements

☒  financial services requirements

☒   telecommunication requirements

☒   providers of critical infrastructure

☒         digital or connected (IoT) products

## Has there been regulatory activity – including enforcement action, investigations, regulatory guidance or other public statements by the regulator – relating to cybersecurity by the following regulators in the last 12 months?

☒  Data privacy

☒   Securities or public company

☒   health

☒   financial services

## Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last review date: 27 December 2024*

Yes.

"Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

## Controllers/Owners have to notify:

*Last review date: 27 December 2024*

☒   data protection authorities

in case of a personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons

without undue delay and, where feasible, not later than 72 hours after having become aware of it

☒  cybersecurity authorities

In the new interim report on new cybersecurity regulations announced by Swedish authorities, it is proposed that the notification of “significant incidents” should, for efficiency reasons, be made directly to the CSIRT unit. This unit should promptly make the information in incident reports available to supervisory authorities. An incident is considered significant according to Article 23.3 if:

(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;

(b)  it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

The report also states that It will be the responsibility of the Swedish Civil Contingencies Agency (MSB) to specify in regulations the detailed meaning of a significant incident.

☒   affected individuals

in accordance with Article 34 of the GDPR: "when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject *without undue delay*."

if a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, unless any of the following conditions are met:

the controller has implemented technical and organizational protection measures and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption; or

the controller has taken subsequent measures that ensure that the high risk to the rights and freedoms of the data subjects is no longer likely to materialize.

☒   other

There shall be public communication or similar measure whereby the data subjects are informed in an equally effective manner (instead of informing the data subjects) if the communication to the data subject would involve disproportionate effort. The GDPR does not stipulate a precise timeline for such public communication.

## Processors/Agents have to notify:

*Last review date: 27 December 2024*

☒   controller/ owner

in case of a personal data breach irrespective of a risk to the rights and freedoms of the data subjects

without undue delay after becoming aware of it

## Are there any additional sector-specific or non-personal data security breach notification requirements?

*Last review date: 27 December 2024*

Yes.

☒  cybersecurity authorities

☒   health regulatory requirements (e.g., to notify incidents affecting safety of medical devices)

☒   telecommunication requirements

☒   providers of critical infrastructure

☒   other

**Details regarding the identified data security breach notification requirements**

**Additional requirements to report incidents for ECS providers**

**Integrity incidents**

An integrity incident is an event that leads to the unintentional or unauthorized destruction, loss or modification of, or unauthorized disclosure of or unauthorized access to, any personal data that is processed in connection with the provision of a publicly available electronic communication service.

A breach must be reported to the supervisory authority PTS without undue delay. According to Article 2 (2) EU Regulation 611/2013, the authorities have to be informed within 24 hours after detection of the breach.

If the breach can be assumed to have had a negative effect on the individual user whose personal data has been processed, or if the supervisory authority requests it, then "notification to the subscriber or individual shall be made without undue delay after the detection of the personal data breach", in accordance with Article 3 (3) EU Regulation 611/2013.

The supervisory authority or a court of law can issue a prohibitory injunction against the service provider if it does not comply with the provision to report a data breach. Such a prohibitory injunction can be combined with a fine.

**Disruptions or interruptions of a significant scale**

In addition, where there is a disruption or interruption of a significant scale, PTS shall be notified the day after the disruption or interruption has been solved and no later than three days after qualifying as an incident that should be notified.

The initial report shall be provided the day after the disruption has been solved, but no later than three days after the disruption/interruption qualified as being mandatory to report. Follow up report shall be provided as soon as possible. The supervisory authority may, if it is in the public interest, order the ECS provider to inform the public about the disruption or interruption.

**Providers of essential services and providers of digital services**

The breach notification requirement to the competent authority stipulated in sections 18 and 19 of the Swedish the Act on Information Security for essential services and digital services applies (i) to operators of essential services and digital service providers and (ii) for breaches that substantially affect the continuity of essential or digital services.

A data breach occurs when an event has a negative effect on the security of a network or an information system. When a service provider does not comply with the breach notification requirement, then the supervisory agency shall issue an administrative fine.

The fine cannot be less than EUR 500 or exceed EUR 1,000. The individual must not be notified.

Incidents shall be reported to the Swedish Civil Contingencies Agency.

First notification shall be made within six hours from when the incident has been identified as being mandatory to report. Follow-up reporting shall then be made within 24 hours and four weeks.

**NIS 2 directive implementation in Sweden**

As stated above, the Swedish government has through an inquiry presented its proposal for Swedish implementation of the NIS 2 Directive with the proposed date of entry into force set to 1 January, 2025. However, the new regulation in Sweden, following delays in the legislative procedure, will most likely not enter into force until summer 2025. The proposed changes include, *inter alia*, requirements for notification obligations, risk management measures, and incident reporting for the operators covered by the regulation. According to the Swedish Government Official Reports, the number of operators that will be covered by the new regulation is expected to increase significantly compared to those currently covered.

The Swedish government will be given authority to decide what government agencies will be tasked with the supervision of the new regulation. It is currently unclear if The Swedish Contingency Agency (MSB), which currently is the coordinating supervising authority of the NIS Directive, will continue in its role after the implementation of the NIS 2 Directive. According to the Swedish Government Official Report, the upcoming decision should be based on the current existing regulatory framework. Therefore, the investigation concludes that a supervisory authority should be appointed for each sector, following the pattern currently in place in Sweden, during the implementation of the NIS 2 Directive. The investigation further suggests that an existing supervisory authority should be assigned oversight responsibility for any new sector included in the NIS 2 Directive. Ultimately, as outlined, the decision will rest with the Swedish government once the law comes into effect.

# Data localization and regulation of non-personal data

## Are there data localization/data residency or other types of laws that may require the retention and storage of data in the local jurisdiction, or prohibit the transfer of data out of the jurisdiction?

*Last review date: 27 December 2024*

Yes.

☒   other laws that may require the retention and storage of personal data (including, for example, where such data is part of another type of record or dataset) in the local jurisdiction or otherwise prohibit the transfer or disclosure of the personal data outside of the local jurisdiction:

☒   tax or financial record laws

As a general rule, all bookkeeping data necessary to fulfil the documentation requirements under the Swedish Bookkeeping Act shall be stored in Sweden. There is also an ongoing public discussion about data (including but not limited to personal data) that is subject to the statutory duty of confidentiality and whether such data can lawfully be processed by cloud service providers that may be obliged to provide data to foreign governments. The US CLOUD Act is of particular concern.

## Does law or regulation impose mandatory requirements to share or make accessible non-personal data?

*Last review date: 27 December 2024*

☒         Obligation for public sector organizations to share or make accessible non-personal data

☒         Obligation for private organizations to share or make accessible data generated by connected or "IoT" devices

☒         Obligation for private organizations to share or make accessible non-personal financial data

☒         Obligation for private organizations to share or make accessible other non-personal data

[The Swedish Accounting Act](https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/bokforingslag-19991078_sfs-1999-1078/) regulates accounting, financial record keeping and reporting in Sweden. The act mandates an accurate collection and systematic recording of all business transaction. The Act also mandates that companies share relevant accounting information with auditors and relevant authorities. As mentioned above the principle of public access to information is a fundamental aspect of Sweden's governance, hence official documents held by the public authorities are accessible to the public with exceptions for certain documents i.e. to protect sensitive information. For example, the annual reports of limited companies registered in Sweden are always publicly available through the Swedish Companies Registration Office.

Please see the EU Chapter for the description of Data Governance Act, Data Act, and Regulation (EC) No 1049/2001 which are all applicable in Sweden. For Sweden the complementary Swedish law Data Governance act applies. The Swedish Post and Telecom Authority is responsible for supervising parts of the Data Governance act in Sweden.

There is also an ongoing investigation in preparation for the Swedish Data Act through which the investigator is tasked with proposing the legislative amendments and other measures necessary for the relevant authorities to exercise their powers and take the required actions under the EU Data Regulation. The assignment is to be reported by October 15, 2025, after which further steps in the legislative process follow before a new law can be admitted. The new legislation is therefore not expected to be entered into force in the immediate future.

## What specific obligations do these data-sharing rules impose on private organizations?

*Last review date: 27 December 2024*

☒         Obligation to share data on request

☒         Obligation to share data proactively

☒         Obligation to (re)design products or services to facilitate data accessibility

☒         Obligation to standardize products or services to facilitate data portability or interoperability

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.