Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: Sweden

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 discussing obligations for private-sector data controllers in Sweden to notify, register with, or obtain authorization from the data protection authority under Sweden's comprehensive data protection law before processing personal data. It also discusses any requirements for data controllers to appoint a data protection officer (DPO) and any applicable notification or registration obligations relating to DPO appointments. This Q&A does not cover notification, registration, or authorization requirements for data processors or arising under sectoral laws. For an overview of the data protection law in Sweden, see Country Q&A, Data Protection in Sweden: Overview.

Data Protection Authority

1. What is the name and contact information of the country's data protection authority or supervisory authority responsible for data protection?

Name

Swedish Authority for Privacy Protection (IMY)

DPA Contact Information

W: imy.se

English Home Page

E: imy@imy.se

Agency Contact Webpage

For a chart with key GDPR guidance from the IMY, see GDPR Data Protection Authority Guidance Tracker by Country (EEA): Sweden.

Notification or Registration

> 2. Does the country's comprehensive data protection law require private-sector data controllers to notify or register with the data protection authority before processing personal data?

In certain circumstances. The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Country Q&A, Data Protection in Sweden: Overview: Question 1). Like the GDPR, the Data Protection Act (2018:218) (in Swedish) (Swedish Act) does not distinguish between different kinds of private- and public-sector controllers regarding notification or registration requirements. For the GDPR's requirements, including notification requirements for cross-border data transfers, see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: EU: Question 2.

General Notification or Registration Requirements

The Swedish Act does not require private-sector controllers to notify or register with the Swedish Authority for Privacy Protection (IMY) when carrying out personal data processing activities. The GDPR requires prior consultation with or authorization from the IMY in certain circumstances (Article 36, GDPR). For more on prior authorization requirements, see Question 3.

Prior Consultation Requirements

Controllers must consult with the IMY if a data protection impact assessment (DPIA) indicates that the processing would result in a high risk to natural persons' rights and freedoms if the controller fails to take measures to mitigate the risk (Article 36, GDPR).

The IMY has released guidance (in English and Swedish) and a non-exhaustive list of data processing activities that require a DPIA, which complements the list endorsed by the European Data Protection Board (Article 35(4), GDPR; see IMY: List of When a Data Protection Impact Assessment Is to Be Made (in Swedish) and EDPB Opinion 20/2018 on the draft list of the competent supervisory authority of Sweden regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR) (Oct. 3, 2018)).

The IMY is developing a process for submitting requests for prior consultations online. However, in the meantime, it offers a form on its website for controllers to use to submit requests (for more information on prior consultations, including the request form, see IMY: Prior consultation (in Swedish)).

Cross-Border Data Transfers

The Swedish Act does not impose any additional notification or registration requirements for cross-border data transfers.

However, controllers must inform the IMY when transferring data to non-adequate countries on the basis that the transfer is necessary for the controller's compelling legitimate interests, where the controller is not able to base the transfer on an adequacy decision, appropriate safeguards, binding corporate rules, or the GDPR Article 49(1) derogations. Transfers under these circumstances must be non-repetitive, concern only a limited number of data subjects, and be necessary for the controller's compelling legitimate interests, which are not overridden by the data subject's interests or rights and freedoms. (Article 49(1), second paragraph and Recital 113, GDPR.)

For more on cross-border data transfers in Sweden, see Country Q&A, Data Protection in Sweden: Overview: Question 20.

Authorization

> 3. Does the country's comprehensive data protection law require private-sector data controllers to seek authorization from the data protection authority before processing personal data?

In certain circumstances. The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Country Q&A, Data Protection in Sweden: Overview: Question 1). For more on the GDPR's general authorization requirements, see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: EU: Question 3.

Prior Authorization Requirements

Sweden's Data Protection Act (2018:218) (in Swedish) (Swedish Act) does not impose requirements for controllers to obtain authorization from the Swedish Authority for Privacy Protection (IMY) before processing personal data. Controllers may have obligations based on GDPR Article 36. For more information on prior consultation requirements, see Question 2.

Cross-Border Data Transfers

The Swedish Act does not impose additional authorization requirements for cross-border data transfers. For the GDPR's cross-border authorization requirements, see Country Q&A, Data Protection in the EU: Overview: Question 20.

The Swedish Act does not provide limitations on the cross-border transfer of personal data under GDPR Article 49(5). Under the GDPR, controllers must obtain prior authorization from the IMY to transfer personal data to a non-European Economic Area (EEA) country without an adequacy decision when relying on:

- Contractual clauses that deviate from:
    - the European Commission's (EC) standard contractual clauses (SCCs); or
    - the standard clauses that a supervisory authority has adopted and the EC has approved.

Binding corporate rules (BCRs). The IMY must approve an organization's BCRs before controllers may rely on them as a mechanism to provide adequate protection for non-EEA cross-border data transfers. However, once approved, controllers do not need to obtain the IMY's authorization for each cross-border transfer that is subject to the BCRs.

- Codes of conduct. Associations and other similar bodies representing certain categories of controllers may prepare codes of conduct according to GDPR Article 40's requirements. These require the IMY's approval before:
    - adoption; or
    - amendment of existing documents.

(Articles 40, 46(3)(a), (4), 47(1), and 63, GDPR.)

The 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 Danish SCCs approved by the European Data Protection Board (EDPB) (see IMY: Danish standard contractual clauses may be used in Sweden (in Swedish)). From June 27, 2021, controllers may also use the new SCCs the EC adopted as appropriate safeguards for cross-border transfers based on GDPR Article 46. For more information on the EC's implementing decision and annex with the new SCCs, see Legal update, European Commission adopts final versions of standard contractual clauses under EU GDPR.

Controllers should regularly monitor guidance from the IMY and the EDPB as specific recommendations on responding to the EU Court of Justice's (ECJ) July 16, 2020 decision on the validity of SCCs as a mechanism to provide adequate protection for transferred personal data may continue to evolve (Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Case C-311/18) EU:C:2020:559 (*Schrems II*); see Legal Update, Schrems II: controller to processor standard contractual clauses valid but EU-US Privacy Shield invalid (ECJ) and EU Cross-Border Data Transfers: Regulatory Guidance Post Schrems II Tracker). On June 18, 2021, the EDPB adopted its Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. For more information on EDPB recommendations, see Legal Update, EDPB adopts final version of recommendations on supplementary measures for data transfers to third countries in response to Schrems II (50th Plenary). On 10 July 2023, the European Commission adopted its adequacy decision for the EU-US Data Privacy Framework. This enables data transfers between EU entities and certified US entities, concluding that the United States ensures an adequate level of protection for personal data transferred from EU to companies participating in the Framework.

Data Protection Officers

4. Does the country's comprehensive data protection law require private-sector data controllers to appoint a data protection officer?

In certain circumstances. The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Country Q&A, Data Protection in Sweden: Overview: Question 1). For the GDPR's requirements for appointing a data protection officer (DPO), see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: EU: Question 4.

Sweden's Data Protection Act (2018:218) (in Swedish) does not:

- Deviate from the GDPR's requirements on when private-sector controllers must appoint a DPO and notify the Swedish Authority for Privacy Protection (IMY) of the DPO's contact details.
- Require appointing a DPO under additional circumstances.

(Article 37(1), (4), (7), GDPR.)

5. If the comprehensive data protection law requires private-sector data controllers to appoint a data protection officer (DPO), do data controllers have any obligations to notify or communicate the DPO's contact details to the data protection authority or register with the data protection authority?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Sweden (see Country Q&A, Data Protection in Sweden: Overview: Question 1). For the GDPR's requirements on notifying the Swedish Authority for Privacy Protection (IMY) about data protection officer (DPO) appointments, see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: EU: Question 5.

Sweden's Data Protection Act (2018:218) (in Swedish) does not set out any specific requirements about how to notify the IMY about DPO appointments. The IMY has released guidance on how controllers may submit the DPO notification and a form for controllers to use (see IMY: Data Protection Officers).

For the IMY's contact information, see Question 1.

Contributor Profiles

Anna Fernqvist Svensson, Partner

Hellström Advokatbyrå

T +46 (0) 709 55 09 15

E anna.fernqvist@hellstromlaw.com

W hellstromlaw.com

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.

