

Data protection policy of Statistics Sweden 240903

Data protection policy of Statistics Sweden



Statistics Sweden’s data protection policy sets out the agency’s interpretation of legal grounds for processing personal data at the agency pursuant to the General Data Protection

POLICY	1
Data protection policy of Statistics Sweden.....	1
Introduction	2
Application of the GDPR	2
Personal data.....	2
Sensitive personal data.....	3
Principles for processing personal data	3
Personal identity number	5
Protection by design and by default	5
Organisation.....	7

Introduction

The GDPR¹ is law throughout the EU and other EEA countries. It is directly applicable to all automated and some manual processing of personal data in the EU, and thus also at Statistics Sweden. To enable Statistics Sweden to fulfil certain certification requirements, the agency's interpretation of aspects such as the legal grounds for processing personal data pursuant to the GDPR must be set out in a policy.

Application of the GDPR

The GDPR applies to processing personal data that is performed in a fully or partly automated manner, and to other non-automated processing of personal data that are included or will be included in a register. It essentially applies within all types of operations and irrespective of the processing party, for government agencies, private enterprises, and organisations.

A natural person who processes personal data as part of a purely personal activity, or who has connections with the subject's household, is exempted from application of the regulation. Exemptions also apply for statements within the bounds of freedom of speech and for releasing documents according to the principle of public access to information.

The GDPR shall be applied to processing of personal data within the bounds of the activity carried out by a personal data controller or a personal data processor that is established in the EU, irrespective of whether the processing is performed in the EU or not.

For Statistics Sweden, this means that the agency's entire processing of personal data is governed by the GDPR, including within operations that form part of international cooperation outside of the EU. Statistics Sweden's publication of journals, online publications and release of documentation according to the principle of public access to information, however, are carried out pursuant to the Freedom of the Press Act and the Fundamental Law on Freedom of Expression, in which the GDPR does not apply.

Rules concerning this can be found in Art. 2, 3, 85 and 86 of the GDPR and Chapter 2, Section 7 of the Act on supplementary provisions to the EU General Data Protection Regulation (2018:218).

Personal data

Personal data is defined as every piece of information concerning an identified or an identifiable natural person. It is crucial that the data, alone or in combination with other data, can be linked to a living person. Common personal data include personal identification numbers, names and addresses. Images and recordings of people can also constitute personal data, if the people are identifiable. Information that has been coded, encrypted or pseudonymised but that can be assigned to a natural person using supplementary information is also personal data. Electronic data such as IP addresses and cookies can also constitute personal data. Information regarding a group of people constitutes the

¹ Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

personal data of any person who is an identifiable member of that group.

Statistics Sweden often uses personal data in its operations to produce statistics. Personal data are also present in the operations conducted by Statistics Sweden besides statistical operations.

The term “personal data” is defined in article 4.1 of the GDPR.

Sensitive personal data

Some personal data are by nature particularly sensitive and thus have stronger protection in the GDPR. These are known as ‘sensitive data’ under Swedish law.

² As a rule, processing such data is prohibited, unless there are special provisions that permit processing.

Sensitive data are defined as such information that discloses racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation of a natural person. Sensitive data also include personal data relating to criminal convictions and offences.

As stated in the second sentence of recital 51 of the GDPR, the use of the term ‘racial origin’ in this policy does not imply an acceptance by Statistics Sweden of theories which attempt to determine the existence of separate human races.

Sensitive data are used in some cases to produce statistics at Statistics Sweden. They also occur in HR administration and can occur in other operations.

Rules concerning this can be found in Art. 9 and 10 of the GDPR, Chapter 3 of the Data Protection Act, Section 15 of the Official Statistics Act (2001:99) and Section 8 and the Annex to the Official Statistics Ordinance (2001:100).

Principles for processing personal data

The GDPR contains some fundamental principles that shall be fulfilled in all processing of personal data and throughout the entire period in which processing takes place. The following principles exist:

- *Lawfulness, fairness and transparency* means that there must be legal grounds for the processing, that the processing must be reasonable and proportionate in relation to data subjects and that it should be clear and obvious to the data subjects how their personal data are processed.

- *Purpose limitation* means that personal data may only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is permitted. The rule regarding statistical purposes is often applicable in Statistics Sweden’s operations and for respondents to Statistics Sweden’s statistics.

- *Data minimisation* means that personal data shall be adequate, relevant and

² For these data, the GDPR uses the term ‘special categories of personal data’.

limited to what is necessary in relation to the purposes.

- *Accuracy* means that personal data shall be accurate and up to date.
- *Storage limitation* means that personal data may not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes.
- *Integrity and confidentiality* means that the controller shall take appropriate measures to protect the data against unlawful access, destruction or damage.
- *Accountability* means that the controller shall be responsible for compliance with the fundamental principles and be able to demonstrate the way in which the principles are fulfilled.

Each person working at or for Statistics Sweden in operations pertaining to personal data shall be aware that there are adopted principles for personal data processing. At Statistics Sweden, storage limitation means, for instance, that temporary files must be removed.

Rules concerning this can be found in Art. 5 of the GDPR.

Legal grounds for personal data processing In order for personal data processing to be permitted, there must be at least one legal ground for the processing. The following legal grounds for processing exist:

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

The legal ground according to point f does not apply to processing carried out by authorities in the performance of their tasks.

For Statistics Sweden as an agency, the majority of all personal data processing has its legal ground according to e. Data of public interest must be set out in EU law or national law, and where Statistics Sweden is concerned, this is set out in the Official Statistics Act, the Official Statistics Ordinance, the Statistics

Sweden Instructions Ordinance (2016:822), and other special provisions.

Personal data processing also occurs at Statistics Sweden based on b, c or d. Very rarely, personal data are processed at an authority pursuant to a, and this should be avoided, wherever possible, by first of all establishing whether some other legal ground is applicable. Multiple legal grounds can exist simultaneously, but there must always be at least one legal ground to apply.

In all production of statistics, personal data processing must have its legal ground in one of the points above. There are special exemptions, e.g., for statistics, in terms of the purposes for which data may be processed (see the previous section). These exemptions do not affect the need to have a legal ground for processing personal data.

Rules concerning this can be found in Art. 6 of the GDPR.

Personal identity number

The GDPR permits Member States to decide more precisely the special terms on which a national identification number or other accepted identification method may be processed. Such an identification number shall, in that case, only be used subject to appropriate safeguards for the rights and freedoms of data subjects.

Where Sweden is concerned, a personal identity number counts as a national identification number. Personal identity numbers may be processed without consent only when it is clearly motivated in light of the purpose of the processing, the importance of reliable identification or other compelling reason. A statistical agency may process personal identity numbers to produce statistics.

As a rule, Statistics Sweden uses personal identity numbers when producing statistics. Coordination numbers and other temporary identifiers are also used. This is clearly motivated for several reasons. Personal identity numbers are used to enable following people in time series and for straightforward age determination, and for breaking down statistics by sex. Statistics Sweden's procedures for preparing register extracts according to Art. 15 of the GDPR are based on searches on personal identity numbers.

Rules concerning this can be found in Art. 87 of the GDPR, Chapter 3 Section 10 of the Act on supplementary provisions to the EU General Data Protection Regulation (2018:218), and Section 14, second paragraph of the Official Statistics Act.

Protection by design and by default

A controller shall implement appropriate technical and organisational measures which will meet the requirements of the GDPR and to protect the rights of the data subject. This applies both in determining the methods used to perform the processing, and in the processing itself. Pseudonymisation of personal data is one such measure. The measures shall be designed to implement data protection principles, such as data minimisation, in an effective manner. The necessary safeguards shall be integrated into the processing. These measures shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks, of varying likelihood and severity, for the rights and freedoms of natural persons.

The controller shall implement appropriate technical and organisational measures to ensure that, normally, only personal data that are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of the processing, the period of storage and its accessibility. In particular, such measures shall ensure that, by default, personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Statistics Sweden processes a great deal of personal data electronically. It is therefore important that IT systems are designed in such a way that, from the very start, they have sufficient protection by design. There should be protection by default in all development work. Statistics Sweden's organisation shall also be designed to limit access to personal data by means of active and up-to-date authorisation management. People who do not need access to certain personal data to perform their work duties shall not have such access. Statistics Sweden performs regular and annual audits of its authorisation management systems.

Rules concerning this can be found in Art. 25 of the GDPR.

Personal data controller and personal data processor

Statistics Sweden is usually the personal data controller for the processing of personal data conducted by the agency. Statistics Sweden can also be a personal data processor. This can be the case when Statistics Sweden produces statistics on behalf of other statistical agencies, and this is the case when Statistics Sweden releases large volumes of data to external recipients that gain access thereto via user interfaces provided by Statistics Sweden. When Statistics Sweden appoints a personal data processor or acts as a personal data processor for another party, a personal data processor agreement is always entered. Statistics Sweden's personal data processor agreement template includes an annex in which technical requirements for the processor are specified.

Rules concerning this can be found in Art. 4.7, 4.8, 24 and 28 of the GDPR and Section 14, first and third paragraphs of the Official Statistics Act.

Transfers of personal data to a third country Any transfer of personal data which is undergoing processing or is in-tended for processing after transfer to a third country or to an international organisation shall take place only under specific conditions. A third country means any country outside of the EU and EEA.

The European Commission can decide that a third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Otherwise, there are detailed rules for ensuring that transferring personal data is done securely as well as exemption rules for special cases.

As a rule, Statistics Sweden only transfers personal data to recipients in a third country when the European Commission has decided that there is an adequate level of protection for that country, or according to exemption rules for special cases.

Rules concerning this can be found in Art. 44–50 of the GDPR.

Organisation

An administrative authority that processes personal data shall appoint a data protection officer. In certain cases, other personal data controllers and personal data processors shall also appoint a data protection officer. This is the case for instance if their principal activity consists of processing extensive amounts of sensitive data. The data protection officer shall have an autonomous position and be bound by confidentiality rules. With due consideration for the organisational structure and size, a data protection officer can be appointed for multiple agencies.

Statistics Sweden, as a large agency with extensive processing of personal data, has appointed its own data protection officer.

Rules concerning this can be found in Art. 37 and 38 of the GDPR.

The data protection officer shall inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the GDPR and other Union or Member State data protection provisions. Furthermore, the data protection officer shall monitor compliance with the GDPR and other regulations in the EU, Sweden or at the controller, provide advice where requested as regards the data protection impact assessment and monitor its performance, cooperate with the Swedish Authority for Privacy Protection as the supervisory authority, as well as acting as the contact point for the supervisory authority on issues relating to processing and consulting as needed with regard to any other matter.

Statistics Sweden's data protection officer reports directly to the Director General but provides support for the entire agency. The data protection officer can be contacted by e-mailing dataskyddsbud@scb.se.

Rules concerning this can be found in Art. 39 of the GDPR.