USS

SOCIALE SECRETARIATEN • SECRÉTARIATS SOCIAUX

Guidelines for applying GDPR in social secretariats

1. Definitions

1.1. The definitions used in the GDPR can be found in Annex 1.

1.2. ESS/SSA: Erkend Sociaal Secretariaat (Dutch) / Secrétariat Social Agréé (French) is a Payroll Office, accredited according to Belgian law

1.3. GDPR: General Data Protection Regulation

1.4. DPA: Data protection authority, i.e. the authority that supervises the protection of personal data in Belgium.

1.5. Subprocessor: the processor appointed by the social secretariat to take on part of the ESS/SSA's processing activities on behalf of the controller, including the processing of personal data.

1.6. USS: Union of Social Secretariats

2. Introduction

2.1. 90% of private sector employers in Belgium use an ESS/SSA for their social administration. The ESS/SSA processes personal data in the course of its work and believes it is vital to process this personal data in a careful, confidential manner. For this reason, the USS intends to use guidelines to formalise the manner in which GDPR is concretely implemented by social secretariats as processors. These guidelines will lay out a framework to ensure that the personal data of workers employed by the clients of the social secretariats is processed in a consistent way and is all subject to the same strict protective measures.

2.2. The sector-specific guidelines (hereafter 'guidelines') relating to the processing of personal data within the framework of the GDPR clearly list the main elements of the data protection strategy implemented by the USS.

2.3. This document:

- will describe the guidelines for processing personal data within the context of service provision;
- will increase transparency regarding the methods of processing personal data used within the sector;
- will provide the Data Protection Authority ('DPA') the means to evaluate whether personal data is being processed in accordance with the legislation and regulations in force;
- aims to meet clients' legitimate expectations regarding the correct processing of their employees' personal data.

3. Scope of application

These guidelines apply to any ESS/SSA established in Belgium for the performance of its main functions in Belgium.
The guidelines apply exclusively to the processing of personal data within the context of the ESS/SSA's main tasks, namely:

- pay calculations and documents relating thereto
- declarations to the authorities and other third parties
- collection and payment of social security contributions and withholding tax on earned income
- legal advice in the field of social and labour law relating to the employer's social administration

As a processor, the purpose of the ESS/SSA's processing is to carry out its main tasks stated below.

When carrying out these main tasks, the ESS/SSA does not process special categories of personal data as described in Article 9 GDPR.
Data provided by the client/employer which is not necessary for the ESS/SSA to carry out its main tasks does not fall within the scope of these sector-specific guidelines.

4. ESS/SSA – client/employer relations

4.1 The ESS/SSA is always a processor when carrying out its main functions. The controller is always the client/employer.

4.2 The legal basis for the ESS/SSA is the contract with the client/employer and the legal obligations that apply to the ESS/SSA in its role as an authorised representative.

5. Impact analysis relating to data protection

As a processor, the ESS/SSA does not have to carry out a Data Protection Impact Assessment (hereafter 'DPIA'). The obligation to carry out a DPIA rests solely with the controller.

In addition, the USS emphasises the fact that the DPA states that the administration of pay and staff are processing activities that do not require a DPIA (Annex 3 of Recommendation 01/2018 of 28 February 2018).

However, the ESS/SSA undertakes to:

- assist its clients, upon request, to comply with their DPIA obligations on the basis of Article 35 GDPR

- carry out a risk analysis of the processing activities undertaken for its clients to ensure that sufficient, necessary technical and organisational measures can be taken (see also Article 12 of these Guidelines).

6. Records of Processing Activities

In accordance with Article 30.2 GDPR, the ESS/SSA keeps an internal record of its processing activities.

7. Sub-processors

The ESS/SSA makes use of sub-processors to carry out its main tasks and thus:

- concludes a processing contract with the sub-processor which covers at least the same data protection obligations as the respective processing contract concluded between the ESS/SSA and its client(s);
- ensures that the client gives their prior written authorisation for the use of sub-processors. This authorisation may take the form of a general or specific written authorisation;
- has a working process to inform each client in advance when they add or replace sub-processors;
- has a working process to deal with client complaints;
- maintains an up-to-date list of its sub-processors. This list is available upon request, as a minimum.

The ESS/SSA does not consider the following third parties to be sub-processors, although these parties receive personal data from the ESS/SSA:

- Social Security authorities;
- the Federal Public Finance Service;
- regional authorities;
- organisations to which the ESS/SSA transfers the personal data of the client's employees on the instructions of the client, but with which the ESS/SSA does not have a contractual relationship, such as meal voucher providers, leasing companies, group insurance and welfare funds.

8. Transferring personal data to third parties

The ESS/SSA only transfers data in the context of its main functions or if formally instructed to do so by the client. These instructions may be included in a contract or delivered in another form (e.g. via an online tool).

9. Retention period

9.1. Retention period for the client/employer as the controller, regarding the retention of documents for which the client/employer is subject to a legal retention obligation:

The ESS/SSA retains the documents listed in Annex 2.1, which it processes as part of its main functions, for at least the retention period stated in Annex 2.1, counting from the year after the period covered by the document, unless otherwise agreed with the client/employer.

9.2. Retention period for the ESS/SSA as the processor, regarding the retention of documents for which the ESS/SSA is subject to a legal retention obligation:

The ESS/SSA retains the documents listed in Annex 2.2, which it processes as part of its main functions, for the retention period stated in Annex 2.2, counting from the year after the period covered by the document.

9.3. Data retention policy

The ESS/SSA has a data retention policy that takes into account the principles of Article 5.1 (e) GDPR (storage limitation). This policy states, as a minimum, that the ESS/SSA will delete/anonymise the data no later than 7 years after the termination of the work contract between the client and its employee, and no later than 7 years after the termination of the contract between the ESS/SSA and the client, unless otherwise agreed with the client.

This 7-year period begins on the first day of the year following the term of the employee's work contract or the contract with the client. Upon the expiry of the retention period, this data shall be deleted or made anonymous within a reasonable period of time.

This data retention policy includes at least the following elements:

- Whether the client can or cannot manage the deletion or anonymisation of the personal data themselves;
- How the ESS/SSA manages the retention/deletion/anonymisation of the personal data
- The retention periods per category of employee personal data

10. Data protection officer

The ESS/SSA undertakes to appoint a data protection officer and to comply with these guidelines. This officer is also the contact person for data protection matters. The ESS/SSA will publish this person's contact details.

The USS undertakes to create a data protection steering group consisting of data protection officers from social secretariats that are members of the USS. The aims of this steering group will include:

- monitoring new developments in the field of data protection;
- promoting the exchange of best practices within the sector;
- carrying out an annual review of these guidelines and the self-assessment questionnaire.

11. Personal data breach

As soon as the ESS/SSA becomes aware of a data leakage, it must inform the affected client/employer (controller) as soon as possible. The ESS/SSA has put standard procedures in place for notifying the client and managing data leakages.

Based on the information available, the ESS/SSA will provide reasonable assistance to the controller when dealing with a data leakage.
It is the responsibility of the controller (client/employer) to check whether the data subjects/DPAs should be informed of any data leakage. Therefore, the ESS/SSA will not inform the data subjects/DPA of a data leakage unless an explicit agreement to the contrary has been made with the client.

12. IT security – Technical and organisational measures

The ESS/SSA has the necessary security measures in place to protect personal data, as described in Annex 3. This annex gives an overview of the main measures guaranteed by the ESS/SSA as a minimum.

13. Data subject rights

If the ESS/SSA receives requests from data subjects to exercise their rights, the ESS/SSA will pass them on to the client/employer within 14 calendar days.

The ESS/SSA provides reasonable assistance to its client/the employer to allow the employer to respond to the data subjects in a suitable manner.

The ESS/SSA has put standard procedures in place for applying data subject rights if requested.

14. Compliance with the guidelines

The ESS/SSA uses a questionnaire, which can be found in Annex 4, to carry out an annual self-assessment regarding the implementation of these guidelines and, on the basis of this self-assessment, confirms to the USS in writing that it complies with the guidelines.

In the event of issues of compliance with these guidelines, the USS will inform the affected ESS/SSA.

Annex 1: definitions

In these guidelines, the following definitions apply:

(Definitions copied from the GDPR)

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

Special categories of personal data:
Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data and biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person's sex life or sexual orientation.

- **Genetic data:** personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- **Biometric data:** personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- **Data concerning health:** personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Data subject: an identified or identifiable natural person

Controller: the 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Third party: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

Data protection officer (DPO):
The data protection officer monitors data processing within their organisation.

Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

DPIA (Data Protection Impact Assessment): is an instrument to pre-emptively identify any privacy risks associated with data processing and then take measures to reduce the risks.

Annex 2: Legal retention periods for categories of personal data processed in the context of the main tasks:

2.1. Legal obligations for the client/employer:

The ESS/SSA retains the following documents for at least the following retention periods:

- general data:
  - fixed worker data (identification, address, gross salary, etc.): 5 years
  - overview of pay and hours worked: 5 years
  - all correspondence between the client/employer and the ESS/SSA that contains personal data: 5 years

- wage calculations:
  - worker data that has been calculated (wage calculation details): 5 years
  - payslip: 5 years
  - individual earnings record: 5 years
  - accounting documents relating to payroll: 7 years

- supplementary documents relating to wage calculations:
  - company car certificate: 5 years
  - general staff register: 5 years
  - documents relating to attachment of earnings: 5 years
  - documents relating to wage transfer: 5 years
  - documents relating to wage delegation: 5 years
  - documents at the end of the employment contract (certificate of employment, holiday certificate, etc.): 5 years
  - 281.XX tax form: 7 years
  - social balance sheet: 7 years

- declarations to the authorities and other third parties:
  - quarterly DmfA declaration: 3 years
  - welfare fund declarations: 3 years
  - Dimona declaration: 5 years
  - Social Risk Declaration for unemployment: 5 years
  - Social Risk Declaration for illness: 5 years
  - declaration regarding withholding tax on earned income: 7 years

2.2. Specific legal obligations for the ESS/SSA:

The legal basis of the specific legal obligations for the ESS/SSA features in Article 48 of the Royal Decree (RD) of 1 July 2006:

Art.48 § 1.3°: The ESS/SSA is required to compile and keep, in a location in Belgium, a complete file for each of the affiliated employers regarding the application of the social laws for all the staff of the affiliated employers. This file will enable the accuracy of the declarations to be verified, and the officials and agents referred to in Article 31 of the law may use this file for reference; the contents of this file are stated in the instructions for social secretariats. (Translated from the French version of the article)

The implementation of Article 48 of the RD of 1 July 2006 is featured in the instructions from the National Social Security Office (NSSO) regarding the employer file:

Overview of the components of the 'single employer file':
In accordance with the provisions of Article 48 § 1.3° of the RD of 28/11/1969, the single employer file shall contain the following documents or information on paper and/or in electronic form for all staff members of the affiliated employers:

a) The affiliation agreement between the employer and the ESS/SSA;
b) The power of attorney assigned to the ESS/SSA;
c) One sheet per employee giving individual details (= information sheet);
d) Written and/or automated pay data with information regarding the services provided by the workers; in order to check whether the employer's input has been correctly converted into the DmfA declaration and whether the social contributions have been correctly calculated;
e) Salary statements as defined in the Pay Protection Act (12 April 1965);
f) The individual earnings records of all employees (employee identification data) in accordance with the RD of 8 August 1980 on managing administrative records;
g) All correspondence between the employer and the ESS/SSA which has or could have an impact on the obligations for which a social secretariat has been commissioned by the employer (also in electronic form);
h) Where applicable, if the ESS/SSA has been instructed to pay net wages to employees via the employer's bank, the documents evidencing this transfer;
i) Holiday bonus documents received, upon which basis the holiday pay with the new employer is calculated (if necessary, these documents can be requested via a set deadline);
j) An overview of the various codes used along with details of these codes (which still needs to be finalised);
k) A copy of the contract concluded with the relevant employer(s) or ESS/SSA house rules regarding its affiliated members.
In concrete terms, this means that the ESS/SSA statutory retention periods for the categories of personal data processed in the performance of their main tasks, and for which they have a specific retention obligation of 5 years, are as follows:

- fixed worker data (identification, address, gross pay, etc.)
- overview of pay and benefits
- all correspondence between the client/employer and the ESS/SSA that contains personal data
- worker data that has been calculated (wage calculation details)

- payslip
- individual earnings record
- documents showing payment transfer (if the ESS/SSA pays net wages)
- documents at the end of the employment contract (certificate of employment, holiday certificate, etc.)

Annex 3: IT security – Technical and organisational measures

The ESS/SSA has the necessary security measures in place to protect personal data. An overview of the main measures guaranteed by the ESS/SSA, as a minimum, can be found below.

1. **Area:**

Security policy and organisation of IT security

Practical measures:

Ownership of security and data protection. The ESS/SSA has designated a person who is jointly responsible for coordinating and monitoring rules and procedures regarding data protection.

Responsibilities. Responsibilities regarding IT security are defined and assigned to employees. The management requires all employees and contractors to implement IT security that complies with the policy in effect and the organisation's procedures.

2. **Area:**

Safe human resources policy

Practical measures:

Confidentiality obligations. The ESS/SSA employees are subject to confidentiality obligations and these obligations are formally stated in work contracts and/or the work rules.

Awareness. The ESS/SSA regularly carries out activities to raise sufficient awareness among its employees.

End. Access rights are withdrawn in a timely manner when the employment relationship ends, and this is carried out in accordance with the administrative procedures regarding security.

3. **Area:**

Economic asset management

Practical measures:

Inventory of economic assets. The ESS/SSA keeps an up-to-date inventory of all the hardware and media it uses.

Processing economic assets

- Rules for acceptable use of information and economic assets are identified and implemented
- Workers and external parties return all economic assets in their possession after their employment or contract has come to an end
- The ESS/SSA has procedures in place to safely destroy media and printed materials containing confidential data

4. **Area:**

Access control

Practical measures:

Access authorisation

- The ESS/SSA implements and maintains an authorisation management system to control access to the systems containing client data.
- Every individual with access to the systems containing client data has a specific, unique user ID/username.
- The ESS/SSA limits access to client data to persons who require this access to carry out their jobs.

Authentication

- The ESS/SSA uses standard practices that comply with industry standards to identify and authenticate users attempting to access the ESS/SSA network systems or IT systems.
- If the authentication methods are password-based, the ESS/SSA requires passwords to consist of at least eight characters.
- The ESS/SSA follows these practices to ensure the confidentiality and integrity of passwords when they are assigned and provided, as well as during storage.

Network access. The ESS/SSA implements the necessary control mechanisms (e.g. firewalls, security appliances, etc.) to increase security and provide adequate protection when its network is accessed.

5. Area:

Cryptography

Practical measures:

Confidential data is encrypted in accordance with recognised cryptographic standards (e.g. Transport Layer Security).

6. Area:

Physical security and securing the environment

Practical measures:

Physical access to the facilities.

- The ESS/SSA restricts access to facilities where confidential information is handled to employees responsible for this task.
- Physical access to the data centres is only granted in accordance with a formal authorisation procedure, and access rights are reviewed periodically.

Protection against disruptions/outages. The ESS/SSA uses different systems that comply with industry standards to protect its data centres against data loss resulting from power outages or fires.

7. Area:

Security of business activities (operational security)

Practical measures:
Data recovery

- The ESS/SSA periodically backs up its client data for recovery purposes in accordance with its agreed backup policy.
- The ESS/SSA retains copies of client data and data recovery procedures in a different location to that in which the primary computing device that processes client data is situated.

Malware. The ESS/SSA carries out anti-malware checks to prevent this malicious software accessing client data without authorisation.

Security update. Security updates are monitored and installed.

Recording in a logbook. The ESS/SSA keeps a record of the access to and use of its IT systems that contain client data, including user IDs, when it occurred and the activity in question.

8. Area:
Communication security

Practical measures:
Transferring outside its own network. The ESS/SSA encrypts client data that is sent via non-secure public networks.

Information transfer. Client data is only transferred to third parties on the client's instructions.

9. Area:
Acquisition, development and maintenance of IT systems

Practical measures:
Security requirements. Data protection requirements are analysed and implemented from the early stages of the development process (security and privacy by design).

Separation of development and production. Production access rights are limited to social secretariat employees who need access to the production environment as part of their job.

Change control. The ESS/SSA (or its IT service provider) has put in place a change management process to ensure that changes to the operational systems and applications are made in a controlled manner.

10. Area:
Supplier relations

Practical measures:

Supplier selection. The ESS/SSA has a selection process in which it assesses the security and privacy practices of a supplier/partner when processing data.

Contractual obligations. Suppliers with access to client data are subject to data protection obligations and these are formally included in the suppliers' contracts.

11. Area:
Managing IT security incidents

Practical measures:
Incident reporting. If an IT security incident occurs which affects the confidentiality or integrity of the clients' data, the ESS/SSA will inform the client without unreasonable delay.

12. Area:
Continuity of the company

Practical measures:
Emergency recovery. The ESS/SSA ensures that there is an emergency recovery plan in place for the data centres where the ESS/SSA IT systems used for processing client data are located.

Redundancy. The ESS/SSA has redundant storage and procedures for data recovery. These are designed to recover client data in the state in which it was last backed up just before it was lost or destroyed.

13. Area:
Compliance

Practical measures:
Security evaluations. Compliance with IT security controls is assessed periodically.

USS

SOCIALE SECRETARIATEN • SECRÉTARIATS SOCIAUX

Annex 4: Annual evaluation questionnaire on compliance with the guidelines

See Word document