ESS RULES FOR PERSONAL DATA PROTECTION

	Name
Owner	Clara San Inocencio, Enterprise Architecture function
Reviewer	Agneta Nestenborg, Director for Project Support and Administration Ari Benderly, Chief Information Security Officer
Approver	John Womersley, Director General

TABLE OF CONTENTS **PAGE**

1. INTRODUCTION

In order to fulfil certain legal obligations and legitimate business interests, ESS gathers personal data from its Staff, potential Staff, suppliers, business partners and contacts, and visitors.

These ESS Rules for Personal Data Protection (Rules) describe how personal data should be collected, handled, and stored by ESS in order to comply with the General Data Protection Regulation (GDPR) and meet ESS' own personal data protection standards.

This document is subordinate to the ESS Policy for Safety, Health, and Security.

2. SCOPE

These Rules apply to personal data processing activities undertaken by ESS or on behalf of ESS that form or intend to form part of a filing system, searchable by specific criteria.

3. PRINCIPLES FOR PROCESSING PERSONAL DATA

3.1. Privacy notice

a) At the time of processing, the data controller shall provide the data subject with the following information in a stand-alone electronic format:

   i. Identity and contact details of the data controller's representative;

   ii. Purpose of and grounds for processing;

   iii. Possible consequences of failure to comply;

   iv. Recipients or categories of recipients of the personal data;

   v. Information about transfers of personal data to a third country or international organisation, if relevant;

   vi. The period for which the personal data will be stored or the criteria used to determine that period;

   vii. Data subject rights; and

   viii. Existence of automated decision-making.

b) If the data controller receives personal information about a data subject from a third party, then the data controller shall provide the data subject similar[1] information within one month after obtaining the personal data.

[1] In addition to relevant information in Article 4.1(a), ESS will also be required to inform the data subject about: which source the personal data originated, if data came from publicly accessible sources, inter alia, unless so informing the data subject meets one of the exceptions laid out in GDPR Article 14(5).

c) The data controller shall only transfer personal data to a third country or international organisation if it has been provided appropriate safeguards (e.g., adequacy decision by the European Commission, legally binding agreement, code of conduct, etc.).

3.2. Purpose of and grounds for processing

a) The data controller shall only process personal data without the data subject's consent if it has a specified[2], explicit[3], and legitimate purpose[4] for collecting personal data.

b) If the data controller does not have a legitimate purpose to collect personal data, then it shall only collect personal data if the data subject gives his or her consent[5].

3.3. Consent

If the data controller does not have a specified, explicit, and legitimate purpose for processing personal data, then it shall request consent from the data subject prior to processing personal data by way of a consent form.

The data controller shall request consent from the data subject

a) In writing,

b) In a stand-alone electronic document,

c) Using clear and plain language, and

d) Acknowledge the data subject's right to withdraw his or her consent at any time.

The data controller shall decide whether consent is necessary for processing and draft the consent form when appropriate.

3.4. Sensitive data

The data controller shall only process sensitive data under one of the following conditions, which will be further specified in a privacy notice:

a) The data subject gives explicit consent;

[2] "Specified" means ESS must inform the data subject the reason why his or her personal data must be collected.
[3] "Explicit" means ESS must explain the reason why personal data must be collected in a clear and unambiguous way.
[4] "Legitimate purpose" means the processing is necessary to: comply with a legal obligation, perform under a contract to which the data subject is a party, perform internal administrative duties, ensure network and information security, etc.

b) Processing sensitive data is necessary for the purpose of carrying out legal or employment obligations under law or collective agreement;

c) Processing relates to sensitive data manifestly made public by the data subject;

d) Processing is necessary for the establishment, exercise, or defence of legal claims;

e) Processing is necessary for preventative or occupational medicine, for assessment of the working capacity of the employee, medical diagnosis, prevention of health or social care or treatment or management of health or social care systems;

f) Processing is necessary to protect the vital interests of a data subject or other natural person incapable of giving consent;

g) Processing is carried out in the course of legitimate activities, with appropriate safeguards, by a non-profit or other on the condition that processing relates solely to its own or former members and personal data is not disclosed to third parties without the consent of the data subject;

h) Processing is necessary for substantial public interest based on Swedish law; or

i) Processing is necessary for archiving purposes in the public interest, scientific, or historical research or statistical purposes.

4. PROCESSING

a) Only the data processor is authorised to process personal data on behalf of ESS.

   i. A list of individuals and divisions who perform the data processor function and the types of personal data allowed to be processed will be posted on the internal ESS IT systems.

   ii. Individuals who are not authorised to perform the data processor function may not process personal data on behalf of ESS. If this occurs, the individual may face administrative or legal consequences.

   iii. The data processor should be consulted before selection of an external processor.

   iv. Additional guidelines for the data processor may be found in the Appendix to these Rules.

b) Regardless of whether the data controller collects personal data by relying on a legitimate purpose or consent, ESS shall only keep personal data that:

i. Is relevant and limited[6] to the purpose communicated to the data subject;

ii. Is accurate, up-to-date, and not kept longer than necessary; and

iii. Does not override the fundamental rights and freedoms[7] of the data subject.

5. BREACH NOTIFICATION

5.1. If the data processor discovers a personal data breach, the processor shall notify the data controller without undue delay by written communication.

5.2. The data controller shall notify the Swedish supervisory authority (*Sw:* Datainspektionen) with the following information if the breach is likely to result in a risk to the rights and freedoms of the data subjects:

a) The nature of the personal data breach, including the categories of data subjects, the approximate number of data subjects, and the approximate number of personal data records concerned;

b) The name and contact details of a person from whom more information can be obtained;

c) The likely consequences of the breach; and

d) The measures taken or proposed to be taken by ESS to address the breach (e.g., mitigation).

5.3. The data controller shall notify the data subject of the breach if the breach is likely to result in a high risk to the rights and freedoms of natural persons. This notification shall include the information in Article 5.2 above.

5.4. However, the data controller shall not notify the data subject of the breach if it:

a) implemented measures that rendered the personal data unintelligible to any person with unauthorised access;

b) took measures to ensure the risks associated with the breach are unlikely to materialise; or

c) finds it a disproportionate effort to notify individual data subjects[8] of the breach.

[6] "Relevant and limited" means the data subject may not be asked for more personal data than necessary to fulfill the purpose.
[7] "Fundamental rights and freedoms" generally refer to the data subject's right to a private life, which must be weighed against the employer's interest, how personal data was collected, and the amount of personal data collected.
[8] In this case, the data controller may mass-communicate (e.g., send one e-mail to many recipients) to the data subjects affected or similar measure whereby the data subjects are informed in an equally effective manner.

6. DATA SUBJECT RIGHTS

The data subject may exercise his or her rights by written communication to the data controller via internal ESS IT systems.

ESS retains the right under the GDPR to refuse data subject requests to exercise his or her rights if ESS finds the request manifestly unfounded or excessive. Should this situation occur, ESS will inform the data subject of the reasons behind the refusal to fulfil the data subject's request to exercise his or her right.

In most cases, ESS shall seek to fulfil the rights of the data subject within one month. However, this one month period may be extended by two more months should ESS receive a high number of requests or requests requiring more resources.

6.1. Right of access by the data subject

a) The data subject has the right to know if ESS is processing his or her personal data.

b) If the data subject's personal data is being processed, then the data subject may request a copy of his or her personal data and the relevant privacy notice.

c) ESS requires verification of identity before proceeding with requests for access to personal data. A designated member of ESS Staff will set up an in-person meeting with the requester whereby the requester will verify his or her identity by showing the designated member of ESS Staff his or her valid ID (e.g., passport or Swedish ID-card).

d) If the data subject requests a copy of his or her personal data and this copy includes the personal data of another individual, then ESS shall:

   i. redact the personal data of the other individual from the copy, or

   ii. request consent from the other individual to include his or her personal data.

   However, if neither redaction nor consent from the other individual is possible, ESS may deny the request.

e) An electronic copy of the data subject's personal data will be e-mailed to the data subject in a ZIP file.

6.2. Right to rectification

The data subject has the right to request correction of inaccurate personal data concerning him or her currently stored in internal ESS IT systems. Once the correction has been made, the data controller will send a written verification.

6.3. Right to erasure ('right to be forgotten')

The data subject has the right to request his or her personal data be deleted or otherwise destroyed if one of the following applies:

a) Personal data is no longer necessary for the purpose it was collected or processed;

b) Data subject withdrew consent and there is no other legal grounds for the processing;

c) Personal data was unlawfully processed;

d) Personal data must be erased in order to comply with a legal obligation to which the data controller is subject; or

e) Data subject objects and ESS cannot demonstrate compelling legitimate grounds to override the objection.

If ESS approves the request for erasure, then the personal data subject to erasure shall be moved to the ESS backup servers until ESS establishes a solution supporting erasure.

6.4. Right to object

The data subject has the right to object to ESS processing his or her personal data at any time if:

a) ESS processed the personal data in order to perform a task that was in the public interest; or

b) ESS processed the personal data because of its legitimate interests or the legitimate interests of a third party.

If the data subject objects, then ESS shall no longer actively process this data unless ESS can demonstrate compelling legitimate grounds that either override the interests, rights, and freedoms of the data subject or is related to establishment, exercise, defence of legal claims. If such grounds exist, then ESS will send the data subject a written communication explaining its grounds for overriding his or her objection.

However, if the data subject objects and ESS approves, then ESS will move the objectionable personal data to its backup servers where it will be stored and neither changed nor used.

6.5. Right to restrict

The data subject has the right to request ESS limit[9] processing of his or her own personal data if:

a) The data subject disputes the accuracy of his or her personal data being processed by ESS;

b) Processing by ESS has been determined to be unlawful but the data subject requests restriction instead of erasure;

c) ESS no longer needs the personal data but the data subject demands ESS hold some of his or her personal data in order to establish, exercise, or defend legal claims; or

d) The data subject objects to ESS processing his or her personal data.

If the data subject's request to restrict is approved, then ESS will move the restricted personal data to its backup servers where it will be stored and neither changed nor used.

6.6. Right to data portability

The data subject has the right to receive an electronic copy of his or her own personal data, which he or she has provided to ESS, in a ZIP file and request this file be transmitted to another data controller if:

a) ESS processed the personal data because the data subject consented or in order to perform under a contract; and

b) The processing was carried out by automated means.

ESS currently does not use automated means to carry out processing for personal data required to perform under a contract; therefore, it is unlikely a request for portability will be approved.

6.7. Right to not be subject to automated processing

Automated decision-making is a decision made by automated means without any human involvement that produces legal effects on data subjects or similarly significantly affects data subjects.

Currently, ESS does not engage in automated processing decision-making.

[9] Limited processing restricts processing to only storage of personal data and the establishment, exercise, or defence of legal claims or protection of the rights of another natural or legal person, or for reasons of public interest in Sweden.

6.8. Right to remedy

a) **Against ESS**

Data subjects have the right to lodge a complaint against ESS with a supervisory authority or court located in the data subject's habitual residence, place of work, or place of the alleged infringement if the data subject believes processing by ESS violated the GDPR.

b) **Against the supervisory authority**

Data subjects also have the right to lodge a complaint against the supervisory authority if the supervisory authority did not handle the data subject's complaint or inform the data subject within three months on the progress or outcome of his or her complaint in the courts of the member state where the supervisory authority is established.

7. FURTHER INFORMATION

Questions regarding these Rules or on personal data protection at ESS should be submitted by ticket in the internal ESS IT systems or by e-mail to privacy@esss.se.

8. GLOSSARY

Data controller is ESS, but in practice will refer to the designated and authorised group of ESS employees who are responsible for determining how to process personal data. Currently, the Enterprise Architecture (EA) function has the mandate to perform such duties.

Data processor is ESS, but in practice will refer to the designated and authorised group of ESS employees and business partners who process personal data on behalf of ESS. Internal data processors will be selected by the data controller and the selection of external data processors will require data controller input.

Data subject refers to a natural person whose personal information is being processed.

Personal data refers to information relating to an identified or identifiable natural person (data subject); for example: name, identification number, location data, online identifier, genetic or social identity of a data subject, etc.

Process(ing) refers to any action performed on personal data: such as collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying, regardless of whether it was performed by automated or manual means.

Sensitive data refers to personal data that includes the characteristics of a data subject revealing 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 a data subject's sex life or sexual

orientation.

Staff refers to persons working as employees, consultants, interns, secondees, in-kind, visiting professors, and any other title whereby the person performs work on behalf of ESS.

Supervisory authority refers to a public entity appointed and authorised by a member state to monitor GDPR compliance; in Sweden, the supervisory authority is Datainspektionen.

_____

REFERENCES

	Title	Reference number
[1]	General Data Protection Regulation (GDPR)	Regulation 2016/679
[2]	Opinion 2/2017 on data processing at work	17/EN WP249
[3]	Guidelines on Consent under Regulation 2016/679	17/EN WP259
[4]	ESS Policy for Safety, Health, and Security	ESS-0019190
[5]	ESS Rules for Handling Confidential Information	ESS-0021313
[6]	IT Security Plan	ESS-0009026
[7]	IT Policy	ESS-0000964

9. DOCUMENT REVISION HISTORY

Revision	Reason for and description of change	Author	Date
1	First issue	Johan Långberg	2015-06-23
2	Updated to comply with GDPR	Clara San Inocencio	2018-05-25

APPENDIX: ESS DATA PROCESSOR

10. ORGANISATION

As stated in the Rules above, the data controller will designate and authorise a limited number of ESS employees, divisions, or groups to perform the data processor function at ESS. The data controller is also responsible for investigating and participating in the selection process of the external processor.

Membership in the data processor function requires proper adherence to these Rules and other instruction from the data controller.

11. CONSENT AND SENSITIVE DATA

11.1. After consultation with the data processor, the data controller shall decide if processing of personal data or sensitive data requires consent or if such processing falls within the scope of a privacy notice.

11.2. If processing requires consent, the data controller shall create a tailored consent form for the specific processing.

12. RECORD

12.1. The data controller, with support from the data processor, shall maintain one record of all personal data processing activities at ESS.

12.2. The data processor shall update the data controller on existing and potential future processing activities as these activities arise.

12.3. Any processing activity not included in the record is therefore not authorised by ESS and may result in disciplinary action against the responsible party.

13. DATA PROTECTION IMPACT ASSESSMENT

The data controller shall ensure a data protection impact assessment (DPIA) is performed each time ESS uses new technology to process personal data or if the data controller determines processing has a high risk of infringing data subjects' rights. The DPIA will be carried out by the data controller/data processor before the new technology is used for processing.

A DPIA shall contain:

a) a description of the intended processing operations systems,

b) the purpose of the processing,

c) the legitimate interests of ESS,

d) the rights and freedoms of the data subjects,

e) an assessment of the necessity and proportionality of the processing in relation to the data subject's rights,

f) measures in place to address the risks to the data subject's rights, and

g) a description of any mechanisms in place to ensure protection of the personal data.

The data controller may involve ESS Staff or other potential data subjects during or after a DPIA in order to better understand and assess the concerns of the data subjects.

14. STORAGE

14.1. Rules on electronic storage

The ESS Rules for Handling Confidential Information [5] designates personal data as "confidential" information. Specifically, these Rules for Handling Confidential Information require:

a) Personal data to be stored in a password protected internal ESS IT system;

b) Personal data to be designated "confidential" in such IT systems, where applicable;

c) Devices containing personal data to be secured when left unattended; and

d) The sender of personal data to ensure the security of transfer to the recipient.

14.2. Rules on paper storage

The ESS Rules for Handling Confidential Information [5] designates personal data as "confidential" information. Specifically, these Rules for Handling Confidential Information require:

a) Circulation to be restricted to persons approved by the line or project manager;

b) Documents and copies to be stored in a locked container or in limited-access archive rooms;

c) Disposal by security bin or physical destruction of the document(s).

15. SECURITY MEASURES

15.1. Access to IT systems

Only individuals registered as an authorised user in the access control system may gain access to the IT systems at ESS. Each user shall have a unique user ID and a password known only to him or her.

15.2. Service coordinator

The service coordinator, as defined in the IT Security Plan [6], shall decide what information on what system should be subject to encryption or deletion routines, and how many generations of backups are required.

Further information regarding the technical security measures of ESS systems may be found in the IT Security Plan [6].

16. TRAINING SESSIONS

16.1. The data controller will hold training sessions on updates in personal data law or updates in ESS procedures and rules.

16.2. The data processor shall attend the above training sessions or its equivalent or risk disciplinary action, including the removal of his or her data processor mandate.

17. CONTACT

17.1. The data processor shall follow the rules of the data controller when commencing any data processing activity.

17.2. The data processor shall defer to the data controller’s authority on any decisions to be made regarding personal data.