

EUROPEAN FOREST INSTITUTE
DATA PROTECTION RULES

Adopted by the Board

22 April 2020, to come into force 1 July 2020

Table of Contents

Article 1	Scope of application	1
Article 2	Definitions.....	2
Article 3	Principles for the processing of personal data	3
Article 4	Grounds for processing of personal data	4
Article 5	Rights of the data subject	6
Article 6	Transfer of personal data	8
Article 7	Compliance	9
Article 8	Administrative and judicial redress	10
Article 9	Final provisions.....	11

Article 1 Scope of application

These rules apply to:

1. Processing at European Forest Institute (EFI) of personal data wholly or partially by automated means.
2. Processing at European Forest Institute of personal data, other than by automated means, which form part of a filing system or are intended to form part of a filing system.

Article 2 Definitions

Personal data means any information relating to a data subject.

Data subject means a natural living person that is identified or who is reasonably likely to be identified by EFI. Time and resources required, as well as technology available, have to be considered when establishing whether a person is reasonably likely to be identified.

Processing means any operation or set of operations which is performed upon personal data or sets of personal data, e.g. collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction.

Filing system means any structured set of personal data which are searchable or accessed according to specific criteria.

Article 3 Principles for the processing of personal data

Personal data must be:

- (a) accurate, adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed
- (b) processed in accordance with these rules, in a transparent manner in relation to the data subject
- (c) only collected and processed for specified and legitimate purposes, and not further processed in a manner not compatible with those purposes
- (d) processed in a manner that ensures security of the personal data, and only made accessible to persons with a legitimate need for access
- (e) kept in a form which permits identification of a data subject for no longer than is necessary for the purposes for which the personal data are processed

Article 4 Grounds for processing of personal data

1. Processing of personal data can only take place to the extent that at least one of the following applies:

(a) consent to the processing has been given by the data subject.

The data subject can withdraw his or her consent at any time, but the withdrawal of consent will not affect the lawfulness of processing based on the consent before its withdrawal.

Consent by a data subject under the age of 16 requires confirmation by the data subject's legal guardian.

(b) processing is required for EFI to fulfil obligations or pursue rights as employer, or processing for the purpose of recruitment, secondments, hosting and traineeships

(c) processing is required for compliance with a legal obligation to which EFI is subject, other than as follows from (b)

(d) processing is necessary for EFI to fulfil contractual obligations, or is required in order to establish a contractual relationship

(e) processing is necessary for the performance of a task carried out in the public interest

(f) processing is necessary in order to protect the interests of the data subject, another natural person, or a legal person

(g) processing is necessary for the purposes of the legitimate interests pursued by EFI or by a third party, especially the proper functioning of the organs and bodies of EFI, subject to the processing being proportional in relation to the legitimate interests of the data subject

2. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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, the following will apply is *sensitive personal data*.

Processing of *sensitive personal data* can only take place to the extent that at least one of the following applies:

(a) consent to the processing has been given by the data subject.

The data subject can withdraw his or her consent at any time, but the withdrawal of consent will not affect the lawfulness of processing based on the consent before its withdrawal.

Consent by a data subject under the age of 16 requires confirmation by the data subject's legal guardian.

- (b) processing is required for EFi to fulfil obligations or pursue rights as employer, or processing for the purpose of recruitment, secondments, hosting and traineeships
- (c) processing is necessary for the performance of a task carried out in the public interest
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person where the data subject is prevented from giving consent

Article 5 Rights of the data subject

Basic rights

1) Right to information

EFI shall at the request from the data subject provide him/her with information on his/her personal data processed, as well as the purpose and the grounds for the processing.

Where EFI is processing personal data based on consent, in accordance with article 4.1(a) or 4.2(a), and the processing is done by automated means, EFI will at the request of the data subject make the personal data, which he or she has provided to EFI, available in a machine-readable format.

2) Right to rectification

The data subject may request rectification of personal data which are inaccurate or completion of incomplete personal data.

The personal data shall, if found inaccurate or incomplete, be rectified or completed. This will however not apply if required to safeguard EFI's legitimate interests.

If a request for rectification is not accepted by EFI, the data subject may where technically possible append a statement relating to the matters which are deemed inaccurate or incomplete.

3) Right to erasure

The data subject shall have a right to have personal data erased if EFI no longer has any grounds for the processing.

If a request for erasure is not accepted by EFI, the data subject may where technically possible append a statement relating to the matters which are deemed inaccurate or incomplete.

Process for exercising the basic rights

Requests for access, rectification or erasure according to the preceding shall be in writing and shall be sent to dataprotection@efi.int or by ordinary mail to *Data protection, European Forest Institute, Yliopistokatu 6 B, 80100 Joensuu, Finland.*

EFI shall respond to the initial request in writing within 30 calendar days and shall provide the information, or information on the measures taken, within an additional 60 calendar days. In extraordinary circumstances the Director can decide to extend the deadlines.

The identity of the data subject must be established before EFI can proceed with a request.

Information to be provided at EFI's initiative

The following information shall be made available to data subjects with respect to personal data being processed by EFI:

- which type of personal data is being processed
- the grounds and purpose of processing of the personal data
- contact information for matters relating to data protection at EFI

The obligation to make the information available shall not apply to the extent that the data subject already has the relevant information, or if it would require a disproportionate effort in relation to the purpose of providing the information.

The information shall be provided without unreasonable delay, having regard to the processing taking place.

Article 6 Transfer of personal data

Transfer of personal data to a third party is permitted under the following conditions, and subject to the applicability of one or more of the grounds in article 4:

1. To third parties that are subject to rules affording a level of protection equivalent to these rules.

The following states and international organisations have rules affording a level of protection equivalent to these rules:

- European Union member states and the European Free Trade Association member states, including ministries and governmental agencies, also on regional and sub-regional level
- EFI Members that are not European Union member states or European Free Trade Association member states, including ministries and governmental agencies, also on regional and sub-regional level
- The institutions and bodies of the European Union
- The United Nations and its specialised agencies

The Director can decide to acknowledge other states and international organisations having rules affording a level of protection equivalent to these rules.

2. To third parties that are contractually or otherwise committed, in a legally binding and enforceable way, to appropriate safeguards in relation to the personal data.
3. To third parties, and when not based on paragraph 1 or 2, for a limited set of personal data, if one or more of the following applies:
 - consent to the transfer has been given by the data subject;
 - the transfer is in the data subject's interest, and is necessary in order to perform a contract or needed to enter into a contract;
 - the transfer is necessary for important reasons of public interest;
 - the transfer is necessary in order to be able to protect the data subject's or other person's fundamental interests, or when the data subject is prevented from providing consent;
 - the transfer is necessary for the purposes of the legitimate interests pursued by EFI or the third party, subject to the transfer being a proportional measure in relation to the interests pursued.

Article 7 Compliance

Supervision

Supervision of data protection at EFI shall be done by a Data Protection Committee, set up as a subsidiary body of the Board.

The Data Protection Committee may order any actions required in relation to data protection at EFI.

General technical and organisational measures

In order to ensure compliance with these rules, technical and organisational measures shall be implemented at EFI. These measures shall especially focus on:

- prevention of unauthorised persons from gaining access to automated systems or filing systems
- only allowing authorised users of an automated system or filing system to access the personal data to which their access right refers
- recording which personal data has been communicated, when and to whom
- preventing that, during communication of personal data and transport of storage media, the data can be read, copied or erased without authorisation

Measures in case of breach

Staff members shall without delay inform the Director in case they note or suspect a data protection breach at EFI.

The Director shall take measures to establish if a breach has occurred and necessary actions to be taken. The Director shall as soon as possible inform the Data Protection Committee on the situation and actions taken. The Data Protection Committee may decide on further actions to be taken.

Compliance assessment

To enhance compliance with these Rules, a compliance assessment shall annually be carried out by the Secretariat. The compliance assessment shall focus on the following items:

- an overview of the processing of personal data at EFI
- risks inherent in the processing
- measures taken to enhance compliance and to address and mitigate risks associated with the processing

The result of the compliance assessment shall be presented to the Data Protection Committee.

Article 8 Administrative and judicial redress

A data subject shall have the right to lodge a complaint with EFI concerning the processing of his or her personal data.

A complaint shall be addressed to the Director.

Following a complaint, the matter shall be investigated, and one or more persons shall be appointed by the Director for this purpose. The persons appointed by the Director for conducting the investigation shall for this purpose have access all relevant personal data and other information needed for the investigation. Any external person appointed to conduct or participate in the investigation shall be subject to a non-disclosure agreement.

The investigation shall be concluded within three months of the lodging of the complaint, unless extended due to extraordinary circumstances, by decision of the Director. The complainant shall be informed of any extension of the investigations.

Following conclusion of the investigation a decision shall be made by the Director. The decision shall be made in writing, and shall be sent to the complainant.

Should the Director not decide in line with the complaint, the complainant can choose to initiate proceedings under the EFI Dispute settlement rules. Such proceedings can only be initiated within three months from the complainant receiving the decision.

The arbitral tribunal can order actions to be taken by EFI. In addition, a complainant who has suffered damages as a result of EFI processing his or her personal data contrary to the provisions in these data protection rules shall have the right to receive reasonable compensation from EFI for the damage suffered. What is to be considered reasonable shall be assessed in light of the type of personal data wrongfully processed, the extent of processing, the length of period during which the processing has occurred, and the damage actually suffered by the data subject as a consequence of the wrongful processing. The maximum liability for EFI for compensation for damages granted under these rules shall be EUR 50,000 (fifty thousand euro).

Article 9 Final provisions

Changes to these rules are decided by the Board.