Research Council of Finland data protection policy

SA/2025/04797

Research Council of Finland

Contents

1. Introduction and scope

Data protection safeguards the rights and freedoms of natural persons, i.e. data subjects, in the processing of their personal data. The processing of personal data is governed by the European Union General Data Protection Regulation (EU) 2016/679, which is directly applicable legislation. In addition, data protection legislation includes the Data Protection Act (1050/2018), which specifies and supplements the General Data Protection Regulation and its national application. The protection of private life is a fundamental right under the Constitution of Finland (731/1999).

In connection with the tasks of the Research Council of Finland (hereinafter RCF), personal data is continuously processed. As a rule, the processing of personal data is based on compliance with the RCF's statutory obligations or performance of tasks in the public interest. It is vital for the RCF to maintain trust in funding applicants, personnel, stakeholder representatives and partners and to process personal data responsibly.

In addition to the data protection policy, the RCF has issued more detailed guidelines on the implementation of data protection and information security. Their aim is to ensure compliance with the obligations laid down in data protection regulations in all RCF activities. The data protection policy also applies to processors of personal data. Compliance with the data protection policy and guidelines issued by the RCF is required whenever processing personal data on behalf of the RCF or when RCF systems or other resources are used in the processing of personal data.

In its activities, the RCF undertakes to comply with the EU General Data Protection Regulation and other data protection legislation. The data protection policy and other data protection documents, such as guidelines, are also part of accountability under the General Data Protection Regulation.

2. Definitions

Personal data refers to all information related to an identified or identifiable person. A person can be identified directly or indirectly on the basis of personal data, such as by combining the data with other data that enables identification. Personal data includes, for example, a person's name, home address, email address, telephone number, location information, photograph and health information.

The *processing of personal data* refers to all activities involving personal data during their life cycle, such as:

the collection, storage, use, transfer and disclosure of personal data.

A *data subject* is a person whose personal data is being processed.

A *controller* is a person or organisation that determines the purpose and means of processing personal data.

A *processor* is a person or organisation that processes personal data on behalf of the controller.

Special personal data is data that reveal a person's ethnic origin, political opinions, religious or philosophical beliefs, union membership, health information, sexual orientation or behaviour, or genetic and biometric data for the purpose of identifying that person. As a rule, the processing of this data is prohibited. Special personal data may only be processed in situations separately provided for in legislation.

Pseudonymised personal data is personal data processed in such a way that it can no longer be attributed to a specific person without using additional information. When the data is converted back to an identifiable form, it is subject to the GDPR.

Anonymised data refers to personal data that cannot be used to identify a person. The prevention of identification must be permanent. It must also be impossible to identify the person indirectly.

3. Organisation and responsibilities

Executive management bears overall responsibility for data protection in the RCF.

Appointed by management, the *Data Protection Officer* is an attorney responsible for overseeing data protection issues. The tasks of the Data Protection Officer include: providing advice and information on obligations under the General Data Protection Regulation and other data protection provisions; providing advice related to data protection impact assessments; supervising implementation of impact assessments; and cooperating with the supervisory authority. The Data Protection Officer reports matters concerning data protection to management.

The Data Protection Officer acts as a contact point for data protection within the RCF and to outside parties (email: tietosuoja@aka.fi). The competence of the Data Protection Officer is continuously developed, and resources are guaranteed for its further development.

The RCF has an *information security and data protection group*, which includes the Data Protection Officer, the Information Security Officer and the head of the information management group. The tasks of the group include: developing and monitoring data protection and information security; participating in risk assessments; preparing and supporting the implementation of information security and data protection tasks required by the State within the RCF; and participating in the planning and implementation of training.

The *supervisor's* duties include ensuring that their subordinates comply with data protection legislation, the RCF data protection policy and internal guidelines, as well as that new employees are familiarised with these.

RCF personnel must comply with data protection legislation in their work, participate in training required by the employer and comply with RCF guidelines. The RCF requires all personnel to complete data protection training on a regular basis, and other necessary training is also provided. Compliance with guidelines also includes a direct reporting obligation on personal data breaches or suspected breaches and shortcomings related to data protection.

In addition, the duties of the *person responsible* for the register or processing function and the *contact person* are specified in more detail by the Administration Office.

4. Implementation of data protection at the Research Council of Finland

4.1. Principles relating to processing of personal data

The processing of personal data must comply with the following principles under Article 5 of the GDPR:

Lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Purpose limitation

Personal data shall 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 shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.

Data minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Storage limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject

Integrity and confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4.2. Data protection by design and by default

The RCF data protection policy is based on data protection by design and by default. These requirements are already taken into account in planning the processing of personal data and, for example, in the planning and procurement phase of a service or system.

When planning the processing of personal data, attention must be given to the principles relating to processing of personal data, the impacts and risks of the processing must be assessed from the perspective of the data subject, the risks must be minimised by appropriate safeguards, and the measures taken must be documented appropriately.

The Data Protection Officer and, if necessary, the information security and data protection group must be involved in addressing data protection issues at as early a stage as possible. The persons in charge of processing and contact persons are responsible for

carrying out the duties assigned to their respective roles. Data protection obligations cover the entire life cycle of personal data processing.

4.3. Accountability

The RCF demonstrates compliance with the requirements of the General Data Protection Regulation and other data protection legislation by documenting its measures and practices and using data protection documents. The practices employed to ensure accountability are also continuously developed.

4.4. Informing data subjects

The RCF observes the principle of openness in its activities. Data subjects are informed at a time and to the extent necessary for each instance of personal data processing. As a rule, information on the processing of personal data concerning RCF clients and stakeholders (privacy notices) is located on the external RCF site. Information on processing the personal data of RCF personnel is available to the personnel.

4.5. Data subject rights

The rights of data subjects under the General Data Protection Regulation include the right to be informed of the processing of their personal data, the right of access to personal data, the right to rectify personal data, the right to erase personal data and be forgotten, the right to restrict the processing of personal data, the right to transfer data from one system to another (data portability), the right to object to the processing of personal data, and the right not to be subject to a decision based solely on automated processing. The RCF shall take appropriate measures to ensure that the rights of data subjects are applicable to each situation and facilitate the exercise of the rights of data subjects.

4.6. Outsourcing the processing of personal data

The RCF ensures the lawfulness of the processing of personal data in situations where an external contracting partner processes personal data, whose controller is the RCF. The risks related to personal data are assessed at the procurement planning stage, and data protection requirements are addressed during calls for tenders. Only operators with appropriate and sufficient technical and organisational capacity to process personal data in accordance with data protection legislation may be selected as processors of personal data.

An appropriate written agreement on the processing of personal data

and a description of the processing activities is drawn up between the RCF and the processor.

The person responsible for the processing is responsible for managing the agreement.

The Data Protection Officer and attorneys assist in the contractual phase. For example, the Annexes of the Terms and Conditions for the Processing of Personal Data (JYSE/JIT – Personal data) can be used as document templates. The implementation and risks of data protection are also monitored and assessed during data processing.

4.7. Transfer of personal data

When transferring personal data outside the European Economic Area (EEA), it must be ensured that the processing of personal data is permitted in the situation in question and that there is an appropriate basis for the transfer in accordance with the General Data Protection Regulation. Supplementary safeguards must also be assessed and implemented on a case-by-case basis. Furthermore, if the processor or its sub-processor transfers personal data outside the EEA, the data transfer must also ensure a level of data protection that meets EU requirements as required by the General Data Protection Regulation.

4.8. Disclosure of personal data

Provisions on the publicity of official documents and information are laid down in the Act on the Openness of Government Activities (621/1999, hereinafter the Publicity Act). In addition to the protection of privacy, the right to information on a public document is a fundamental right guaranteed by the Constitution of Finland. The RCF balances the reconciliation of these rights.

In order to comply with the principle of openness, the Research Council of Finland maintains a description of the data repositories and case register managed by it (description of document publicity). Public documents are disclosed upon request as laid down in section 13 and section 16 of the Publicity Act. A public document may also contain information whose disclosure is restricted (usually personal data). Confidential information may be provided at sight and disclosed to a party or by virtue of a right based in law only with the consent of the person concerned.

If the data that is subject to a request for information includes personal data, the person submitting the request for information is asked to provide information on the intended use of the personal data. This can be done using a separate form. The RCF uses the form to also ensure that the person requesting information understands the responsibilities related to the personal data they receive on the basis of the request.

5. Information security

Information security facilitates implementation of the principles of data protection. On its own and with the help of its partners, the RCF takes adequate technical and

organisational measures to ensure the security of personal data. Regular verification, evaluation and development form the basic framework of activities. Reports on information security are also regularly submitted to management.

6. Accountability for data protection breaches

RCF personnel are obligated to report any deviations that endanger the protection of personal data immediately in accordance with RCF guidelines. The RCF conducts a risk assessment in accordance with its practices from the perspective of the rights of the data subject, documents the breaches and, if necessary, notifies the data protection authority, the data subject, Finnish Transport and Communications Agency Traficom and the police in accordance with the General Data Protection Regulation and other applicable regulations and guidelines.

7. Notification of data protection policy violations

The RCF Data Protection Officer should be contacted if there is any failure to comply with this data protection policy in the processing of personal data. Persons in an official or employment relationship with the RCF may also report violations concerning the processing of personal data to the internal reporting channel of the RCF. Members of elected bodies may submit a similar notification to the centralised external reporting channel of the Chancellor of Justice.

A person may also refer the lawfulness of RCF activities to the Office of the Data Protection Ombudsman for evaluation.

8. Entry into force

This data protection policy shall enter into force on 11 May 2026, thus replacing the RCF data protection policy which entered into force on 5 December 2018 (AKA/7/07.01.10/2018).

9. Legal basis

Section 20 of the Rules of Procedure for the Research Council of Finland Administration Office

The data protection policy was discussed at the meeting of the Research Council of Finland cooperation group on 1 April 2026.

President
Paula Eerola

Executive Director, Operations Management Unit
Emilia Katajajuuri