Punainen Risti

POLICY

Data protection documentation
Approved by: The Board of the Finnish Red Cross on **27 April 2018**
Updated by: The Board of the Finnish Red Cross on **22 November 2024**
To be updated by: 2028

DATA PROTECTION POLICY

---

1. PURPOSE AND FUNDAMENTAL PRINCIPLES OF THE FINNISH RED CROSS

According to Section 2 of its rules, the purpose of the Finnish Red Cross is, in all conditions, to protect life and health, defend human dignity and human rights, promote co-operation and peace between nations, save human lives in and outside Finland, help those in the most disadvantaged position to prevent and alleviate human suffering, support and assist public authorities in times of both peace and war and armed conflict in order to promote people's well-being, promote solidarity and willingness to help among citizens, increase understanding towards the Red Cross' work and universal efforts, and affirm the organisation's readiness and operational capacity.

The operations of the Red Cross Movement are steered by seven fundamental principles: humanity, impartiality, neutrality, independence, voluntary service, universality and unity.

2. BASIC PRINCIPLES OF THE FINNISH RED CROSS DATA PROTECTION POLICY

The foundation of all activities of the Finnish Red Cross is that the beneficiaries, volunteers, partners and supporters have confidence in the work of the organisation. The realisation of data protection is very important to the Finnish Red Cross, and the whole organisation must be committed to it. The processing of personal data is essential to the operation of the organisation, and the appropriateness of the processing is important for maintaining trust. The Finnish Red Cross, similarly to other operators within the movement, collects, stores and processes personal data only insofar as it is necessary to implement the humanitarian mandate of the movement. Personal data will not be requested or used for purposes that would conflict with the purpose and principles of the Red Cross laid down in the Act on the Finnish Red Cross and the Presidential Decree on the Finnish Red Cross.

All those working and acting within the organisation are required to act in accordance with the legislation and the organisation's values and principles and be aware of their own responsibility in maintaining the trustworthiness of the organisation when they process personal data as a part of their duties.

Data protection refers to the protection of privacy in the processing of personal data. The protection of privacy is a fundamental right of every natural person in accordance with the Constitution of Finland and the Charter of Fundamental Rights of the European Union, and the processing of personal data must always be based on law.

Personal data is information relating to a natural person (= data subject), which can be used to identify the person either directly or indirectly by combining information. Personal data includes such information as a name, a personal identity code, a picture, location data, an online identifier or a physical, physiological, genetic, mental, economic, cultural or social characteristic specific to the individual.

Processing of personal data refers to all operations relating to personal data, such as the collection, recording, organisation, storage, alteration, retrieval, use, disclosure, dissemination, combination, restriction, erasure or destruction of such data.

A personal data register is a set of personal data that can be accessed on certain grounds. The register may consist of several databases, and some of the data may also be in paper format, for example. Data protection is regulated by the EU General Data Protection Regulation (2016/679, GDPR), the Finnish Data Protection Act (1050/2018), the Act on the Protection of Privacy in Working Life (247/2019) and special legislation depending on the activities.

The Finnish Red Cross processes personal data on a large scale in its operations. Data subjects include volunteers, members, donors, beneficiaries, clients, partners and school contact persons and employees, among others. As a rule, the Finnish Red Cross receives personal data from the persons themselves when they participate in or support the organisation's activities.

An essential requirement in data protection legislation is accountability, i.e. the Finnish Red Cross must be able to demonstrate that personal data processing is appropriate and within the legal framework. In addition, the Finnish Red Cross has a duty to inform data subjects if the confidentiality of their personal data has been compromised. This requires sufficient documentation of the personal data processing activities and internal processes.

This policy outlines the principles of data protection in the Finnish Red Cross. The data protection policy applies to all processing of personal data by and on behalf of the Finnish Red Cross, regardless of the origin, content or purpose of the data. The data protection policy is public.

The data protection policy is supplemented by detailed guidelines regarding the maintenance of personal data registers, the exercise of data subjects' rights and the management of data protection deviations. However, the detailed guidelines must not contradict the principles set out in the data protection policy.

The Blood Service and Punainen Risti Ensiapu Oy are independent data controllers whose activities differ significantly from other activities of the Finnish Red Cross. The Blood Service and Punainen Risti Ensiapu Oy have separate data protection policies that support this policy, practical guidelines, data protection officers and data protection management models. This has been deemed necessary to ensure the necessary expertise and sufficient data protection throughout the Finnish Red Cross organisation. The prerequisite for the realisation of data protection is sufficient data security, the principles of which are set out in the Finnish Red Cross data security policy.

The realisation and effectiveness of the data protection and data security policies are regularly evaluated as part of the inspection of other operations and reported in the data balance sheet.

3. FINNISH RED CROSS DATA PROTECTION PRINCIPLES

- We shall only collect personal information necessary for our activities
- We shall openly disclose our processing of personal data
- We shall process personal data confidentially and diligently
- We shall not store personal data unnecessarily
- We shall process personal data from various registers in centralised systems, making personal data with different purposes of processing available to be combined with other registers of the organisation (e.g. members, volunteers, donors)
- In emergencies and exceptional situations, we shall use personal data extensively to ensure the sharing of information, to communicate the need for help and to invite people to participate in the activities
- We shall use profiling and machine learning methods for the processing of personal data in order to improve our operations

- We shall utilise anonymised and/or synthesised personal data as part of our research and/or volunteer work to develop our activities
- When necessary, we shall share information between the headquarters, district offices, branches and institutions within the organisation
- We shall not disclose personal data outside of the organisation with the exception of authorities in exceptional situations and emergencies or other situations in which data sharing is required by law, such as for the purpose of investigating and preventing misuse
- The personal data of vulnerable data subjects (e.g. older people, minors, victims of persecution) shall be processed with particular diligence in separate systems

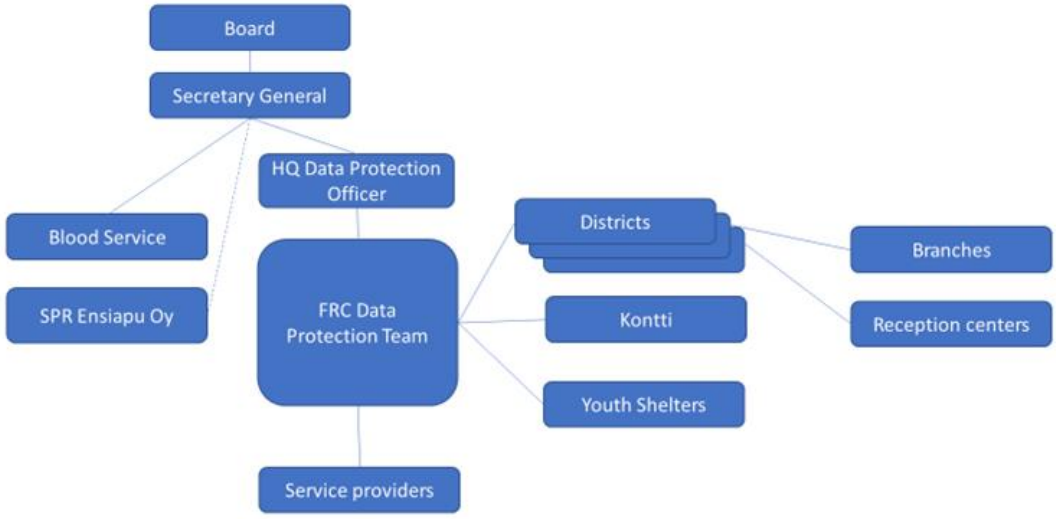
4. PERSONAL DATA REGISTERS

Personal data processed for a specific purpose constitutes a personal data register. Each personal data register must have a responsible unit/institution and a contact person. The operation of each personal data register is described in a privacy statement that must be made available to the data subject, easy to understand and up to date.

The person in charge of each register shall be responsible for the register, its adequate and up-to-date documentation and instructing the necessary persons in processing the information contained in the register. The person in charge of the register is also responsible for the destruction of useless and unnecessary data in accordance with the data retention periods specified in the privacy statement.

5. DATA PROTECTION ORGANISATION AND RESPONSIBILITIES

The Finnish Red Cross data protection organisation is structured as follows:



As a rule, the Red Cross is the data controller in all processing of personal data. This includes all personal data of members, volunteers, beneficiaries, trainees and staff. The districts of the Finnish Red Cross are the data controllers in the processing of the personal data of their own employees and other personal data processing they do for themselves. The data protection responsibilities between the headquarters, districts and branches are described in the attached tripartite agreement.

Data Protection Officer

- acts as a data protection expert
- coordinates the activities of the Data Protection Team
- acts as a contact person for the supervisory authority
- monitors and controls the processing of personal data and its compliance with requirements
- reports to the Finnish Red Cross management on the state of data protection according to predefined indicators
- reports to the Finnish Red Cross management on the need to improve data protection issues
- supports the data protection work of the entire organisation
- provides training and is responsible for training materials and instructions
- is responsible for the organisation-level data protection pages and documentation of data protection processes
- investigates issues, does not make decisions
- supports and trains register owners
- is responsible for the support of the data protection contact persons in the districts and institutions
- is responsible for the preparation of the data balance sheet
- is responsible for communicating data protection work within the organisation
- follows their time, educates themselves, networks
- keeps in touch with the international organisation of the Red Cross on data protection issues

Data protection steering group

- preparation of strategic decision-making
- no operational responsibility, guiding auxiliary
- organisation-level prioritisation
- deals with current data protection issues, such as data protection impact assessments
- develops data protection procedures and principles
- meets at least twice per year
- reviews the differences between the data balance sheet, policy and practice
- handles deviations
- development-oriented
- is responsible for updating the policy

District/institution data protection contact person

- is responsible for the data protection practices and training of staff in their district/institution
- is the primary contact person for the reception centres and branches and is responsible for implementing the data protection guidelines in the practices of the branches
- maintains the district's/institution's data protection documentation, including the documentation for the registers where the district/institution is the data controller or where processing is different from the headquarters
- understands the responsibilities of the data controller versus the processor and understands when the district is the controller and when the processor
- is responsible for the district's/institution's contribution to the data balance sheet
- understands the role of data protection in a branch's operations inspection

Branch data protection contact person

- is the point of contact to the district and central administration in data protection issues concerning the branch
- is responsible for data protection practices in the branch's activities
- maintains the branch's data protection documentation
- is responsible for the branch's internal data protection guidelines and training

- understands the responsibilities of the data controller versus the processor and understands when the branch is the controller and when the processor
- maintains the branch's data protection documentation
- is responsible for data protection training and instructions for the branch's volunteers

Headquarters Data Protection Ambassador

- a unit's data protection support person who reminds people of data protection practices or observing them
- more dedicated, interested
- participates in data protection group meetings and is active
- brings their unit's questions/challenges to the working group
- assists in the preparation of the data balance sheet

Supervisors are responsible for compliance with the data protection policy in their area of responsibility and ensuring that the instructions are sufficient and up to date.

Every employee adheres to the data protection principles and reports any observed deviations related to data protection to the Data Protection Officer at tietosuoja@redcross.fi.

6. DATA SUBJECTS' RIGHTS

Data subjects have the right to be informed about the processing and use of their personal data. Every data subject has the right to:

- access their own data
- request rectification of data
- request erasure of data
- request restriction of processing
- request transmission of data from one system to another

The Finnish Red Cross always assesses the content of the request received from the data subject and its execution on a case-by-case basis. The Finnish Red Cross may not always be able to comply with the data subject's request. The rights of data subjects for each personal data register are recorded in the privacy statement.

All requests regarding the exercise of data subjects' rights shall be directed to the Data Protection Officer tietosuoja@redcross.fi.

7. TRANSFERS AND DISCLOSURES OF PERSONAL DATA TO THIRD COUNTRIES OUTSIDE THE EU AND EEA

Transfers and disclosures of personal data to third countries must be made exercising particular diligence. In the case of systematic transfers, it must be ensured as a precondition of the system functionality that the required safeguards are implemented on behalf of the recipient.

In the case of individual transfers, the main priority is to ensure that the data subject understands and accepts the principles of the transfer and the recipient. A transfer may also be made if it is necessary in order to carry out a contract or protect the person.

8. BUILT-IN DATA PROTECTION AND IMPACT ASSESSMENT

Data protection requirements must be taken into account as early as possible when planning changes to activities, procedures or systems. Any plans for changes to the processing of personal data and new processing operations must always be accompanied by an assessment of the risks the activities pose to the rights and freedoms of individuals. If processing may pose risks, an impact assessment must be carried out to assess the risks posed by the processing in relation to the benefits of the processing.

9. DELETION, ANONYMISATION AND PSEUDONYMISATION OF PERSONAL DATA

Personal data shall not be stored unnecessarily or as a precaution. Each privacy statement specifies the need to retain personal data and acts accordingly. Personal data registers contain plenty of information that is used for creating statistics on the activities and monitoring them in the long-term. For this reason, after the end of the actual purpose of use, personal data may be anonymised or pseudonymised on a case-by-case basis, which means that the actual personal data will be destroyed, but unique identifiers, such as customer, member or reference numbers, may be retained for monitoring and statistical purposes. Pseudonymised personal data is processed in accordance with the General Data Protection Regulation and other applicable legislation.

10. INCLUDING DATA PROTECTION IN CONTRACTS

External operators, such as subcontractors, must also act in accordance with the data protection principles of the Red Cross. When drawing up and updating contracts, it must be ensured that they adequately and unambiguously take data protection aspects into account. Particular attention must be paid to the fact that data protection practices and related legislation vary considerably outside the European Union. A data processing agreement must be drawn up with each processor of personal data as required by the General Data Protection Regulation.

11. BREACHES OF PERSONAL DATA

A breach of personal data is a breach that results in personal data transferred, stored or otherwise processed to be accidentally or illicitly destroyed, lost, altered, disclosed or accessed.

Any suspected or detected data security breaches shall immediately be reported to the person responsible for the register in question, the person in charge of the activities and the data protection officer, and the necessary corrective action shall be taken.

More detailed instructions on the handling of data security breaches and the necessary notifications to data subjects and supervisory authorities will be provided separately.

Appendices: Processing the organisation’s personal data – tripartite agreement