Punainen Risti

Data protection documentation
Created: 10 February 2019
Updated: 17 September 2024

**DATA PROTECTION POLICY, APPENDIX 1**

---

# PROCESSING THE ORGANISATION'S PERSONAL DATA – TRIPARTITE AGREEMENT

## 1 Parties

The Parties to this Personal Data Processing Agreement (**the Agreement**) are:
1) the Finnish Red Cross at the national level (**the Organisation**), represented by the Headquarters;
2) the Finnish Red Cross at the regional level (**Districts**); and
3) the Finnish Red Cross at the local level (**Branches**).

By decision taken at their respective meetings, the boards of each Party accede to this Agreement and, in the same decision, declare their commitment to complying with the data protection policy of the Finnish Red Cross (the Organisation, Districts and Branches, hereinafter collectively referred to as **the Parties**).

## 2 Purpose and scope of the Personal Data Processing Agreement

This Agreement defines the cooperation between the Parties and applies to all processing of Personal Data carried out on the Organisation's behalf.

This Agreement covers any Personal Data for which the Organisation acts as Controller (**the Controller**) and the District and Branch act as Processors (**Processors**).

Under this Agreement, the Processors process Personal Data for the purpose of supporting the Controller's activities. The Personal Data processed may include Personal Data of the Organisation's members, volunteers, trainees, trainers, collaborators at companies and schools, and various beneficiary groups, among others.

## 3 Definitions and roles

For the purposes of this Agreement:

1) **Data Protection Legislation** refers to the data protection legislation in force in Finland at any given time (incl. Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR) and the Finnish Data Protection Act 1050/2018) and any binding provisions issued by data protection authorities;
2) **Data Subject** refers to a person whose Personal Data is processed for the purpose of supporting the Organisation's activities;
3) **Personal Data** refers to any information concerning an identified or identifiable natural person that has been obtained in the context of the Organisation's activities before or after this Agreement entered into force;
4) **Controller** refers to the party that determines the purposes and means of the processing of Personal Data; the Headquarters acts as Controller under this Agreement;
5) **Processor** refers to the party that processes Personal Data on the Controller's behalf; the Districts and Branches act as Personal Data Processors under this Agreement; and
6) **Summary Document** refers to an account of the Personal Data processing activities carried out on the Controller's behalf.

## 4 Common obligations of the Parties

Each Party must:
1) process Personal Data in compliance with good data processing practices and in accordance with the Data Protection Legislation;
2) undertake to develop and use the Organisation's centralised systems that support the processing of Personal Data; and
3) undertake to process all Personal Data of the Organisation in a secure manner and with due care.

## 5 Obligations of the Controller

The Controller must:
1) provide the Processors with written instructions on the processing of Personal Data that comply with the Data Protection Legislation and are binding on the Processors;
2) respond to requests for exercising the Data Subjects' rights; the Controller will notify the Processors of such requests if responding to the requests also requires actions from a District or Branch;
3) support the Districts by providing appropriate material and support for the Branches' data protection training.

## 6 Obligations of the Districts

The Districts must:
1) appoint a responsible person for data protection for the District;
2) maintain a Summary Document, as per the template, regarding Personal Data processing carried out on the Organisation's behalf;

3) support the Branches in their region as Personal Data Processors for the Organisation;
4) undertake to provide data protection training for the members of their Branches;
5) ensure that the Branches are aware of their obligations and rights as Personal Data Processors for the Organisation;
6) support the Branches in cases in which the Branches do not have direct access to the Organisation's personal data systems;
7) respond, without undue delay, to questions asked by the Headquarters regarding the rights of the Data Subjects.

## 7 Obligations of the Branches

The Branches must:
1) process Personal Data based on the legal grounds for processing;
2) appoint a data protection contact person for the Branch (J2);
3) maintain a Summary Document, as per the template, regarding Personal Data processing carried out on the Organisation's behalf;
4) ensure that elected officials, volunteers in charge and other key persons are knowledgeable about data protection;
5) respond, without undue delay, to questions asked by the Headquarters regarding the rights of the Data Subjects.

## 8 General obligations of the Processors

The Processors must:
1) process Personal Data in accordance with the documented instructions provided by the Controller;
2) notify the Controller immediately if they find that the Controller's instructions infringe the Data Protection Legislation;
3) implement sufficient technical and organisational security measures to protect the Personal Data as required by Article 32 of the GDPR;
4) assist the Controller, as applicable and to the extent necessary, in ensuring compliance with the obligations pursuant to Articles 32–36 of the GDPR;
5) ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
6) delete or return all the Personal Data to the Controller after the end of processing for the specified purpose, unless otherwise required by law;
7) make available to the Controller all information necessary for compliance with the Controller's obligations;
8) notify the Controller without undue delay after becoming aware of a Personal Data breach.

## 9 Disclosure of Personal Data

The Processors are not allowed to disclose or transfer the Organisation's Personal Data to a third party for any reason other than for the purpose of processing, as specified in advance.

The Organisation's Personal Data may be disclosed within the organisation, between the Headquarters, Districts and Branches, if necessary.

## 10 Subcontractors

The Processors may use subcontractors for the processing of Personal Data.
The Processors are responsible for the actions of their subcontractors as if they were their own, and they enter into the necessary data processing agreement with their subcontractors.

## 11 Audit

The Controller is entitled to carry out audits and inspections on the Processors in order to ensure that the Processors comply with the Data Protection Legislation and the obligations provided in this Agreement with regard to the processing of Personal Data. The Districts are entitled to carry out audits and inspections on Branches on behalf of the Controller.

## 12 Limitation of liability

The liability for data protection related damage is determined in accordance with the GDPR.

## 13 Applicable law and dispute resolution

This Agreement is subject to the laws of Finland. Any disputes are primarily resolved through negotiation. In the event that a dispute cannot be resolved through negotiation, the matter may be referred to the District Court of Helsinki.