Data Processing Agreement from the Norwegian Red Cross

Norwegian Red Cross

RE**1** **DEFINITIONS**

Data Processing Agreement (DPA): These terms and conditions with appendices and any alterations and updates agreed upon between the Parties in writing. The DPA is in accordance with the Norwegian Personal Data Act, guides from the Norwegian Data Protection Authority and the GDPR. The DPA applies between the Customer as the Controller and the Supplier as Processor, within the meaning of the Norwegian Personal Data Act.

Principal Agreement The agreement in force between the Customer and the Supplier that establishes what the Supplier shall supply to the Customer and the commercial terms. This DPA is an appendix to the Principal Agreement and does not entail any changes to the commercial terms of the Principal Agreement.

Customer: See Appendix 1 section 1. The Customer is the legal entity that acquires goods or services from the Supplier, whereby the Supplier by some means process personal data on behalf of the Customer. The Customer is a party to the Principal Agreement with the Supplier.

Controller: Customer (the company that receives goods or services from the Supplier that includes the processing of personal data).

Processor: Supplier.

Sub-processor: Another processor engaged by the Processor.

Third country: A country outside the EEA that the European Commission has not decided to ensure an adequate level of protection.

Supplier: See Appendix 1 section 1..

Party: Customer or Supplier.

Parties: Customer and Supplier.

Personal data: Means any information relating to an identified or identifiable natural person ('data subject').

Processing: Means, with respect to the Controller's personal data, means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction ("process" and "processing" shall be construed accordingly).

2 DPA'S PURPOSE

The purpose of the DPA is to regulate the rights and obligations of the Parties in accordance with the Norwegian Personal Data Act and the GDPR. The DPA fulfils the minimum requirements of the GDPR.

The DPA shall ensure that personal data related to data subjects is not unlawfully processed or made available for unauthorized persons. The DPA regulates the Processor's processing of personal data on behalf of the Controller, including collection, recording, organization, storage and disclosure or combinations thereof.

3 DPA'S AIM

The Processor and any person acting on behalf of the Processor, who has access to personal data, shall process the relevant data only in accordance with documented instructions from the Controller, as stated in GDPR art. 28 (3). The Parties agree that what is stated in this DPA shall be considered as such instructions from the Controller.

The aim of this DPA is to specify that the Supplier as the Customer's Processor may process personal data in accordance with the terms that are agreed upon with the Customer, including processing pursuant to the Principal Agreement, to perform any processing that the Customer requests the Supplier assist the Customer with, or to fulfil the Supplier's contractual relationship with the Customer, as it stands at any time.

Categories of **data subjects**:

- Manager (National Society)
- Technical Advisor (National Society, NorCross, third-parties)
- Coordinator (NorCross, third-parties)
- Data Consumer (third parties)
- Supervisor/Head Supervisor (National Society)
- Data Collector (National Society)
- Community members in locations where NYSS is active

More information is provided on each category of data subject, including their affiliations, below.

Personal data processed pursuant to the agreement:

- Manager/Technical Advisor/Co-ordinator/Data Consumer: Name, phone number, email
- Supervisor/Head Supervisor: Name, email, Phone number, age bracket, gender
- Data collector (volunteers): Name, Gender, age bracket, phone number (personal), location (region, district, village and latitude and longitude)
- Community members in areas where NYSS is active: Physical health condition (symptoms) linked to individual's gender, age group (above or below 5 years) and reporting volunteer's location

Processing activities covered by the DPA:

Processor responsibilities

- Record and store data in accordance with legal obligations
- Pseudonymising and, where appropriate, anonymising for archiving of data upon termination of services
- Communication of changes to Head Managers
- Test technical developments and bug fixes of the Nyss platform
- Report aggregated data to donors of Nyss
- Analyse aggregated data to:
  - Understand use of services
  - Service improvements
  - Service evaluation
- Assist the controller with fulfilling the controller's duty to respond to requests given by the data subject for the purpose of exercising his/her rights as a data subject

Controller Responsibilities

- All activities that take place under Your Users' Accounts, the use of their usernames and passwords allowing access to the Services
- Registering information in the system, ensuring accuracy and currency of information and removing information from the system (including at termination of services), including personal data

- Providing user accounts to third parties
- Adding and deleting users and their data
- Providing access to data to third parties (e.g. IFRC), including for the purpose of administration and research.

The **framework** for the Processor's processing of personal data: The Supplier may process personal data in accordance with the framework provided by the Customer in the Principal Agreement and in the subsequent contractual relationship between the Parties at any time and to fulfil the Contractor's responsibility as processor under the applicable laws.

4 THE PROCESSOR'S OBLIGATIONS

The Processor shall comply with the procedures and instructions for the processing that the Controller has decided is applicable at any given time.

The Processor is obliged to provide the Controller with access to its security documentation, and assist so the Controller can comply with its own responsibilities under the relevant privacy laws.

Unless otherwise agreed upon or provided by law, the Controller has the right to access and inspect the personal data processed and the systems used for this purpose. The Processor is obliged to provide necessary assistance to this.

The Processor has a duty of confidentiality regarding documentation and personal data that they obtain access to pursuant to this DPA. This provision also applies after the DPA's termination. The Processor shall ensure that persons authorized to process the personal data are committed to processing the information confidentially by a confidentiality statement in an employment contract or in other agreement with the Processor, if such person is not subject to an appropriate statutory duty of confidentiality

The Processor shall comply with the security requirements imposed by the applicable personal data protection legislation. The Processor shall implement the principles of privacy by design and default. The Processor shall document routines and other measures to fulfil these requirements. The Processor shall implement appropriate technical and organizational measures to achieve a level of security appropriate to the risks associated with processing personal data and to ensure that processing meets the requirements of applicable data protection legislation, including the requirements of the GDPR, and the protection of the rights of the data subject.

The Processor shall assist the Controller with fulfilling the Controller's duty to respond to requests given by the data subject for the purpose of exercising his/her rights as a data subject.

The Processor shall assist the Controller in ensuring compliance with the Controller's obligations pursuant to GDPR articles 32 - 36.

The Processor shall implement appropriate technical and organizational measures to achieve a level of security appropriate to the risks associated with processing personal data and to ensure that processing meets the requirements of applicable data protection legislation, including the requirements of the GDPR, and the protection of the rights of the data subject.

The Processor shall immediately inform the Controller if, in its opinion, an instruction from the Controller infringes the GDPR or other statutory provisions on the protection of personal data.

The Processor shall not disclose or make available personal data to third parties without the prior written consent of the Controller, except for any approved Sub-processors to the extent that they need the information in order to carry out their tasks.

5 USE OF SUB-PROCESSORS

The Processor shall not engage another processor without prior specific or general written authorization from the Controller. In the event the Processor's use a sub-processor or a person that normally is not employed by the Processor, this shall be agreed upon in writing with the Controller before the processing of personal data commences. Anyone that performs assignments on behalf of the Processor, where processing of the relevant personal data is included, shall be familiar with the Processor's contractual and legal obligations and comply with the conditions for these. The Processor must ensure that any subcontractors used by the Processor, and which process personal data, assume the same obligations as those set out in this DPA.

An overview of approved sub-processors can be outlined in Appendix 1 to this DPA or by e-mail to the Controller's contact person. Appendix 1 shall be updated if changes are made to the use of sub-processors. The Processor is fully responsible for the Sub-processor's performance of its obligations.

6 INTERNATIONAL DATA TRANSFER

The Supplier only processes personal data within Norway/EU/EEA and may only transfer personal data to countries within the EU/EEA. If the Processor intends to transfer or process personal data outside the EU/EEA, the Processor shall notify the Customer before such processing is initiated and document that the Processor has entered into a data processor agreement or other necessary contracts with the relevant sub-processor which fulfils the requirements for such transfers/processing as well as that the security for such processing fulfils the requirements in the GDPR article 32 and the requirements following the Schrems II judgment.

Standard Contractual Clauses (SCC) from 4. June 2021 shall be used for transfer to a country outside EU/EEA that is not approved by the EU Commission, unless a valid Binding Corporate Rules (BCR) apply for such transfer.

7 THE RIGHTS AND OBLIGATIONS OF THE CONTROLLER

The Controller has the rights and duties at any time given by law applicable to the Controller for the processing of personal data.

In the event of violations of this DPA, the Norwegian Personal Data Act og GDPR, the Controller may require of the Processor to stop further processing of the data with immediate effect.

8 SECURITY

Both the Controller and the Processor shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the Controller shall provide the Processor with all information necessary to identify and evaluate such risks.

Appendix 1 to this DPA gives an overview of the Processor's technical and organizational security measures. The Processor may send an overview of the Processor's technical and organizational measures by email to the Controller's contact person. The technical and organizational security measures may be improved and further developed in accordance with the technological development. In such cases, the Processor may implement updated technical and organization security measures, provided that the security level for the relevant security measures stays unchanged or is increased to a better level of security. If in the assessment of the Controller, mitigation of the identified risks require further measures to be implemented by the Processor, than those already implemented by the Processor pursuant to Article 32 GDPR, the Controller shall specify these additional measures to be implemented in writing to the Controller, either in Appendix 1 or by e-mail.

9 SECURITY BREACH

The Processor shall inform the Controller of any breach of this DPA or breach of security of processing. Such security breach notice shall be given without undue delay after the Processor became aware of the breach, and no later than 48 hours after becoming aware of the breach

10 SECURITY AUDITS

The Controller shall decide with the Processor that security audits are carried out regularly for the systems and similar entities covered by this DPA. The Processor shall, upon request, enable and contribute to audits, including inspections, carried out by the Controller or another inspector, authorized by the Controller.

The Processor shall, upon request, make available to the Controller all information necessary to demonstrate that the requirements set out in this DPA are met.

11 DURATION OF THE AGREEMENT

The DPA applies as long as the Processor is processing personal data on behalf of the Controller, and the DPA follows the same rules for termination as the Principal Agreement.

Termination of this Data Processing Agreement will result in a corresponding termination of the Principal Agreement - and a termination of the Principal Agreement will result in termination of the DPA - so that both agreements terminate simultaneously.

12 UPON TERMINATION

Pursuant to the Controller's decision, the Processor shall delete or return all personal data received on behalf of the Controller to the Controller after the services associated with the processing are provided (upon termination of this DPA). The Controller can demand a return in a structured and commonly used machine-readable format.

Upon termination of the DPA it could be agreed upon that the Processor will delete or securely dispose of all documents, data, etc., which contain data covered by the DPA. This also applies to any backups. The Processor shall delete existing copies of such personal data, documents and data, unless applicable laws require that the Contractor continue to store personal data or such documents / information. Processor shall delete existing copies of such personal data, documents and data, unless law requires storage of such data.

The Processor shall document in writing that the deletion and / or destruction has been carried out according to the DPA within reasonable time after the termination of the DPA.

13 NOTICES

Notices under this DPA shall be sent in writing between the parties' stated contacts as specified in the Principal Agreement.

14 LIABILITY

The limitation of liability in the Main Agreement applies to this DPA. No limitation of liability applies to a natural person's claim for compensation arising from Article 82 of the GDPR. The parties' liability for damages to natural persons caused by a breach of the GDPR, the Norwegian Personal Data Act with regulations or other regulations implementing the GDPR, follows from the provisions of Article 82 of the GDPR. The parties are individually liable for fees imposed under the GDPR art. 83.

15 DISPUTE RESOLUTION

The DPA shall be interpreted and regulated in accordance with Norwegian law. Any disputes between the Customer and the Supplier relating to the DPA shall be settled by ordinary Norwegian courts. Lawsuits in such disputes shall be brought before the Oslo District Court (Oslo tingrett), which the parties agree upon as the legal venue. This also applies after termination of the DPA.

***

This DPA has been executed in two – 2 copies, each Party has received one original copy

Place and date: .....

Controller	Processor
.....	.....
Name:	Name:

APPENDIX 1: SPECIFICATION OF THE SUPPLIER'S SERVICES AND PROCESSING OF PERSONAL DATA COVERED BY THIS DPA

1. Parties

Supplier (Processor): Norges Røde Kors with registered organization number 864 139 442 and registered business address Hausmanns gate 7, 0133 Oslo, Norway.

Customer (Controller): [insert company name] with registered organization number [insert organisation number], with registered business address [insert].

2. Contact Persons for Notices

Contact person from Supplier:	[name]	[e-mail]
Contact person from Customer:	[name]	[e-mail]

3. The Supplier's services and processing of personal data covered by the DPA

In accordance with the Master Agreement, the Processor shall deliver:

The Master Agreement (the "Nyss platform agreement") is the contract between the Customer and the Supplier (signed electronically).

Personal data processed pursuant to the agreement:

Name, mobile phone number, address, place of work, e-mail address and similar which the Customer or the Customer's end user supplies. Education, experience, certifications, working hours/vacation and time clock

As part of the Processors fulfilment of their obligations pursuant to the Master Agreement, the Processor will have access to personal data in the Parties' systems. These may include user information such as username and password. The Processor's solution can also include additional personal data, such as position data, if the Controller wishes.

Categories of data subjects:

The Customer's own employees, Customer's contract personnel, Customer's owners and management, contact persons associated with the Customer's suppliers or customers. The Customer's other contractual parties that make use of the solution from the Supplier pursuant to the Master Agreement, and any other end user the Customer connects with the Supplier's offered product or service. The categories of data subjects may be further described in an additional appendix to this DPA or an e-mail between the Parties given contact persons.

Processing pursuant to the agreement:

The Supplier's processing which is necessary to fulfil the Supplier's duties pursuant to the Master Agreement. In addition, the processing that is necessary for the Processor to fulfil its duties and rights pursuant to this DPA or applicable laws or to suggest improvements to the information security of the personal data being processed.

In addition, processing for statistical purposes, any duties, including advising the Controller about the type of solution and other advise to improve the deliverables pursuant to the Master Agreement, including advise on improvements to security for the processing of personal data.

The framework for the processing:

The Supplier only processes personal data within Norway/EU/EEA and may only transfer personal data to countries within the EU/EEA. If the Supplier intends to transfer or process personal data outside the EU/EEA, the Supplier shall notify the Customer before such processing is initiated and document that the Supplier has entered into a data processor agreement or other necessary contracts with the relevant sub-processor which fulfils the requirements for such transfers/processing as well as that the security for such processing fulfils the requirements in the GDPR article 32. The Supplier must be able to document compliance according to the Schrems II judgement of any transfer to a third party in a country outside EU/EEA that is not approved by the EU Commission, in example document which additional measures that apply in addition to a valid Standard Contractual Clauses.

Instructions from the Controller:

The Processor and any other person who processes personal data for the Processor who has access to personal data, shall process such personal data only in accordance with documented instructions from the Controller.

This DPA is considered to be such documented instructions. E-mails from the Controller are also considered to be such documented instructions. In addition, the following is considered documented instructions: [insert]

Privacy by design and privacy by default:

Privacy by design and by default shall be a fundamental part of the Processor's activities any service delivered to the Controller. The Processor shall ensure and be able to document that that the key principles of privacy by design and by default are adhered to by the Processor and its subcontractors as well as any system the Processor is making available to the Controller through the term of the Agreement that may process any personal data that the Controller is a supervisor for.

4. List of sub-processors the Processor has an equivalent data processor agreement with:

Name Sub-processor	Website	Country	Data Processing Agreement
Microsoft Azure	https://azure.microsoft.com/en-us/support/legal/	Ireland	MicrosoftProductandServicesDPA(WW)(English)(Jan2023)(CR).docx (live.com)
SMS Eagle	Privacy Policy | SMSEagle	Poland	

5. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

The Processor guarantees that appropriate technical and organizational security measures are implemented at any given time to ensure satisfactory information security so that personal data is protected against unauthorized or accidental destruction, loss, damage, alteration or unauthorized disclosure of said personal data. This applies particularly to personal data that is transferred over a network and for all other illegal forms of transfer of data.

This entails that the Processor shall implement appropriate measures to secure the confidentiality of the Controller's data as well as measures to ensure that the data is not unlawfully disclosed or lost. Furthermore, the Processor shall implement appropriate measures to avoid the unauthorized alteration or destruction of data as well as measures to prevent viruses and other damaging software. The Processor is obligated to keep the Controller's data separate from any third parties' data to reduce the risk of damage and/or access to the data. Separate is understood as all technical measures necessary to ensure that the data is protected from unauthorized damage and access, are implemented maintained. Access to the data by the Processor's employees or others, which do not need to access the data to perform work for the Controller, is also considered unauthorized damage and access. The Processor shall ensure that suppliers of third party services implement sufficient and necessary measures to secure the Controller's data

Such technical and organizational security measures include, but are not limited to: Control of physical access at data centres, digital access control and password protection, transfer control, limited accessibility. See also the Supplier's privacy policy on https://www.rodekors.no/om/personvern/.

The Processor shall, at the Controller's request, make available all information that is necessary to demonstrate that the obligations stipulated in this DPA are met.

For more detailed and updated information concerning the technical and organizational security measures, please see https://azure.microsoft.com/en-us/support/legal/.

Detailed personal data and data subjects

Role	Affiliation	Description	Personal Data Collected
Manager	National Society	Managers are often employees within the National Society and have a manager role in their existing National Society structure. Managers are responsible for the overall setup, implementation, monitoring, and closing of CBS and Nyss. Managers are responsible for adding new users. Sometimes, managers are in charge of certain supervisors each.	Name, Phone Number, email
Technical Advisor	National Society NorCross Third parties as agreed by the controller (e.g. IFRC)	Technical advisors are often delegates or staff from a Partner National Society, IFRC, or ICRC. They have expertise in public health and CBS and give technical support to the National Society implementing Nyss.	Name, Phone Number, email
Co-ordinator	NorCross Third parties as agreed by the controller (e.g. IFRC)	To ensure that no personal data is shared across organizations, the setup of a joint project with another organization requires a new user role: the coordinator. The coordinator is most often an employee from the main organization involved in the joint project.	Name, Phone Number, email
Data Consumer	Third parties as agreed by the controller (e.g. IFRC)	Data consumers are external parties who have been granted access to the information, for instance the Ministry of Health, local/regional health authorities, other governmental authorities, or other partners/organizations you collaborate with, but that are not directly involved in the data collection.	Name, Phone Number, email
Head Supervisor/Supervisor	National Society	Supervisors are most often local employees or long-standing volunteers within the National Society. Supervisors are assigned to one specific project within a National Society. Supervisors are responsible for a group of data collectors within a geographical area. They are responsible for training, supervision, and support of the data collectors, monitoring and cross-checking reports sent by the data collectors, and monitoring	Name, email, Phone number, age bracket, gender

		and cross-checking alerts triggered by these reports.	
Data collectors	National Society	Data collectors are not users of Nyss themselves but are registered in the platform so that Nyss can interpret where a report is coming from, and so that a supervisor easily can follow up the data collectors they are responsible for	Name, Gender, age bracket, phone number (personal), location (region, district, village and latitude and longitude)
Community members in areas where NYSS is active	None	Data collectors report information about health risks that they detect in their local community. These health risks can be related to a person.	Physical health condition (symptoms) linked to individual's gender, age group (above or below 5 years) and reporting volunteer's location