

Nyss platform agreement

V.1.5 4.02.2021

This Agreement concerns access to the Nyss platform and the free of charge use of its functionalities (the “Services”). The Norwegian Red Cross (“Norcross”) developed the Nyss platform in order to enable Red Cross and Red Crescent National Societies as well as other organisations (the “contracting party”) to implement a real time community-based surveillance system. The Nyss platform aims at filling an information gap between communities and public health surveillance that relies on information collected by healthcare facilities.

By accepting this Agreement and ticking the box below, the “Head Manager”, as a representative of the contracting party, confirms having full legal authority to enter to this Agreement and activate a country or regional profile (the “Account”) in the Nyss platform.¹ To conclude the Agreement, the Head Manager further confirms:

- having read and understood the implications of the Agreement and its clauses listed below;
- the processing of personal data, including its collection and transfer, within the Nyss platform will be performed in accordance with the laws applicable to the contracting party. Furthermore, as much as this is compatible with national law, the processing of personal data should also follow requirements and principles of personal data protection described in Annex 1 and in the IFRC’s Policy on the Protection of Personal Data;²
- having understood the roles and responsibilities of the different types of Users of the Nyss platform described in Annex 3;
- the Agreement is in force until the actual termination of Services following the Head Manager’s request to Norcross.

1. Agreement definitions

- a) “Services” within the scope of this agreement refer to the combination of hardware and software components provided to the contracting party by Norcross. Services include a dedicated part of the Nyss platform to the contracting party (i.e. the national or regional profile, hereafter the “Account”); an SMS gateway facilitating the reporting of health risks; technical assistance upon request (provided remotely).
- b) “Account” refers to the Services environment, where the contracting party representatives registered as Users can access features facilitating the reporting of health risks and management of resources.
- c) “You” and “Your” refers to the individual having legal authority to enter to this Agreement (the Head Manager) or to the contracting party that is subject to this Agreement.
- d) “Users” are individuals within and outside Your organisation (e.g. employees, contractors, volunteers and third-party representatives), whom You authorize to access the Account or part of it. Users may also include third parties to whom you can provide

¹ In situations where the Head Manager who has legal authority to enter in this Agreement is not available, s/he can be replaced by a representative of an active aid provider on the ground (i.e. the Technical Advisor).

² See: <https://fednet.ifrc.org/en/ourifrc/about-the-federation/ppp/?b=s&d=Legal%20Department&l=&n=&t=>

access to parts of the Account in order to facilitate necessary interaction with You. The different roles that Users can assume are described in Annex 3. Within Your Account, the following types of Users may be created:

- Head Manager;
 - Manager;
 - Technical Advisor;
 - Supervisor
 - Data Collectors; and
 - Data Consumers.
- e) “Personal data” means any information relating to an identified or identifiable natural person.
- f) “Data subject” is an individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- g) “Processing” 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.
- h) “Data controller” refers to the person(s), organisation or institution that determines the means and purposing of the processing.
- i) “Data processor” is the person(s), organisation or institution that processes data on behalf and under the instruction of the controller.
- j) “Your data” means all text, information, data, including personal data and other content provided by You or Your Users that are processed, reside in, or run on or through the Services.
- k) “Material impact and significant changes” or “material changes” refer to changes to the Nyss platform that would require a substantive revision of provisions of this Agreement.
- l) “Third-party” means a natural or legal person, public authority, agency or body other than the data subject, the contracting party, Norcross and persons who, under the direct authority of the contracting party, are authorised to process personal data.

2. Rights granted

For the duration of the Services, You will have access to the Account and the Services that are subject to this Agreement, including features and functionalities available within them solely for Your needs and activities concerning health risk reporting and management.

3. Nature of the processing

Data in Nyss is collected through Data Collectors sending reports via SMS to Nyss and by users registering other users in the Nyss web platform.

Data Collectors send reports as SMS to a SMS gateway. The SMS gateway forwards the SMS to the cloud resources backing the Nyss platform. Nyss matches the reports to the personal data of the sending Data Collector and stores the reports within the Nyss databases.

SMS messages to Data Collectors or other users are sent back through the SMS gateway, using either an intermediate Email provider (SendGrid) or a direct connection to the SMS gateway.

Nyss automatically recognises configurable patterns in the incoming reports (alert rules) that are used to alert users to potential outbreaks.

The reports are also used to indicate how frequently Data Collectors send SMS and how many errors they make.

More information on the nature of the processing can be found in the data protection impact assessment accessible at cbsrc.org/resources (available only in English).

4. Purpose of the processing

Any data processed within Nyss serves to facilitate the implementation of a community based surveillance system.

Reports on health risks/events are processed to allow CBS implementers to detect potential outbreaks in real-time and warn health authorities early, which allows them to respond early.

Personal data of users of Nyss is collected to allow them to login, ease communication between them, notify them upon events that should trigger an action (e.g. a potential outbreak has been found) and to indicate the performance of the CBS implementation in terms of report correctness, completeness of reporting, gender & age uniformity and others.

Data processed within Nyss can also be used in pseudonymized form to improve CBS implementation methodology and statistical purposes.

More information on the purpose of the processing can be found in the data protection impact assessment accessible at cbsrc.org/resources (available only in English).

5. Accountability

You are responsible for information you register in the system and personal data is processed in accordance with current regulations.

6. Account management

- a) The Head Manager, upon accepting this Agreement, is granted access to the Account for the contracting party covering an area in a country or the entirety of the country. The Head Manager, by receiving access to the Account, recognises that the contracting party becomes the data controller with respect to the processing of personal data in the context of the Services covered by this Agreement. For the purpose of opening the Account, the Head Manager shares the contracting party's ID and contact details, such as an email address and a phone number with the Global Coordinator. In situations, where the contracting party acts outside the International Red Cross and Red Crescent Movement, it should provide the Global Coordinator with relevant information, including contact details.
- b) Access to the Account is secured by a password set by the Head Manager, who shall take all reasonable efforts to protect this password. The password must be reset at any point if its confidentiality has been breached.
- c) The Head Manager has a duty of care when creating and authenticating other Users, in particular Managers within the Account (the role of Managers is defined in Annex 3). The Head Manager oversees the access control policy and takes reasonable steps to ensure that individuals responsible for creating Users are acquainted with the access control policy, according to which 1) each User shall be granted access using a unique

- username and password; 2) unauthorised sharing of Account information, such as log in details is prohibited; 3) User rights are to be granted using the principle of least privilege and need to know basis; and 4) Users entitled to process personal data are acquainted with requirements concerning personal data protection listed in Annex 1.
- d) The Head Manager takes the necessary organisational measures to ensure the confidentiality of usernames, passwords and Account information as well as of the personal data that is being processed by Users. Such measures focus mainly on training Users.
 - e) The Head Manager is responsible for all activities that take place under Your Users' Accounts, the use of their usernames and passwords allowing access to the Services.
 - f) The Head Manager notifies Norcross immediately of any unauthorised use of Accounts or log in details.
 - g) The Head Manager ensures that when providing User accounts to third parties, an assessment of potential privacy, data protection and security risks is conducted.
 - h) Upon the request to terminate Services, the Head Manager takes necessary measures to ensure that the projects are closed and that the Global Coordinator can archive the Account. Such necessary measures may include a regular revision of the Account and communication with the Global Coordinator.

7. Data security

- a) Norcross will implement and maintain technical and organizational measures to protect Your data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, and to provide a level of security that is appropriate to the risk presented by the processing and the nature of the data to be protected. Within the scope of these activities, Norcross is bound by the General Data Protection Regulation 2016/679 made applicable in Norway by the Norwegian Act of 15 June 2018 no. 38 relating to the processing of personal data.
- b) The security measures include efforts: to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of the Nyss platform and the Services; to help restore timely access to Your Account, and personal data within it following an incident; and for regular testing of effectiveness.
- c) Norcross will update the security measures considering the changing state of the art of security measures. Such updates will not have material impact on the Nyss platform.
- d) When selecting a storage provider for Your data, Norcross will ensure that such provider adheres to appropriate industry standards safeguarding the security, availability and confidentiality of Your data.
- e) Encryption protocol on the Nyss platform allows Your data to be accessed only to Users that were granted access to the Nyss platform for the purpose of executing their responsibilities and duties within the Account of the contracting party concerning health risk management and reporting.
- f) Norcross will not access Your Account, unless You agree to grant such access, for example, to provide technical assistance.
- g) Data "in transit" between endpoints is secured and protected from interception. This is achieved by using an encrypted protocol that meets recognised industry standards.
- h) Data "at rest" is also secured by appropriate use of encryption.
- i) Norcross implements a robust key management policy to maintain a high level of protection.

8. Norcross obligations as data processor

While providing technical assistance, Norcross acts as a data processor, and, thus, is bound by the following obligations:

- a) Comply with the procedures and instructions for the processing that the controller has decided is applicable at any given time.
- b) Not engage another processor without prior specific or general written authorization from the Controller.
- c) Maintain a duty of confidentiality regarding documentation and personal data that they obtain access to pursuant to this agreement.
- d) 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.
- e) The agreement shall ensure that personal data related to data subjects is not unlawfully processed or made available for unauthorised persons.
- f) Assist the controller in ensuring compliance with the applicable controller obligations (e.g. in Europe, obligations pursuant to articles 32 – 36 of the General Data Protection Regulation - GDPR).
- g) 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 agreement).
- h) Make available to the controller all information necessary to demonstrate compliance with the obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

9. Modifications

- a) Norcross may review and make changes to this Agreement. In case of materially significant changes to any of the provisions of this Agreement an email will be sent to Head Managers.
- b) By default, all patches, bug fixes, updates, and maintenance necessary for the proper function and security of the Services, without having a material impact and significant changes on the Nyss platform will be automatically implemented.

10. Termination of Services

- a) Services provided under this Agreement shall be provided for the period necessary to report and manage health risks within the country or a specific region(s) of the country where the contracting party is located. To terminate the Services, You need to provide Norcross with a written request to terminate Services.
- b) Upon such request, Your Account, including Your data concerning health risk reporting, will be pseudonymized and, where appropriate, anonymized within the period of six months, unless there is a request to retain the raw data.

11. Technical assistance

Norcross may use different tools, scripts, software, and utilities to monitor and provide technical assistance related to the Services and to help resolve Your requests.

12. Service analyses

- a) Norcross collects statistical and other information related to the performance, operation and use of the Services.
- b) Norcross uses data from the Services environment in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes concerning the improvement of the Nyss platform.

- c) No personal data is included in the analyses.

13. Dispute resolution

The parties to this Agreement (i.e. You and Norcross) shall attempt to resolve any dispute concerning any alleged breach of this Agreement in good faith. In the event that such dispute cannot be resolved informally such dispute shall be settled under the rules of arbitration of the United Nations Commission on International Trade Law (UNCITRAL) by one or more arbitrators appointed in accordance with the said rules, such as the International Chamber of Commerce. Such arbitration shall be final and binding and no punitive damages may be awarded.

14. Disclaimers

- a) Norcross does not guarantee that Services will be performed error-free or uninterruptedly.
- b) Norcross is not in control of Your data transfer over communication facilities, including the Internet.
- c) Norcross is not responsible for any harm caused by the processing of personal data by Your Users within the Service environment.

Annex 1

Data protection principles

The Head Manager will take appropriate steps to ensure that any User acting under the authority of the contracting party shall process the personal data necessary to report health risks in a manner compatible with *inter alia* the following principles:

- a) Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes related to health risk reporting.
- b) Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed.
- c) Transparency: Data subjects (in particular, the Data Collectors) whose data are being processed through the Nyss platform must be provided with the information necessary to ensure fair processing (such as information about the purposes of processing and about possible transfers of data; see Annex 2 for a more detailed explanation).
- d) Security and confidentiality: Technical and organisational security measures must be taken by the contracting party that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the contracting party, including authorised third parties must not process the data except under instructions from the contracting party.

The Head Manager will take appropriate steps to ensure that data subjects can exercise their rights to access, rectification, deletion and objection. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against the principles listed in above. If there are compelling grounds to doubt the legitimacy of the request, the contracting party may require further justifications before proceeding with the rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort.

Annex 2

Information notices to data subjects

Representatives of the contracting party, at the time of collection of personal data from individuals, should provide them with a privacy notice. This notice should be provided in a way that is concise, transparent, intelligible, easily accessible; and uses clear and plain language. The notice should include at minimum the following information:

- **the identity of the controller and of his representative;**
- **the purposes of the processing;**
- **the categories of data concerned, the recipients or categories of recipients, and**
- **the existence of the right of access to and the rights to rectify and erasure of the processed personal data.**

Upon the initiative of the contracting party, a more detailed notice following the requirements of the General Data Protection Regulation could be developed. It could then include the following:³

- the name and contact details of the entity acting as a controller (in the Nyss case, the contracting party);
- the name and contact details of the controller's representative (if there is one);
- the contact details of the controller's data protection officer (if applicable);
- the purpose/s of the processing;
- the legal basis/ground for the processing;
- the legitimate interests for the processing (if applicable);
- the categories of personal data obtained (if the personal data is not obtained from the individual it relates to);
- the recipients or categories of recipients of the personal data;
- the details of transfers of the personal data to any third countries or international organisations (if applicable);
- the retention periods for the personal data;
- the rights of individuals in respect to the processing;
- the right to withdraw consent (if that is the legal basis for the processing);
- the right to lodge a complaint with a supervisory authority (if applicable);
- the source of the personal data (if the personal data is not obtained from the individual it relates to);
- the details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable); and
- the details of the existence of automated decision-making, including profiling (if applicable).

³ European Union Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ EC (GDPR) Article 13.

Annex 3

Users within the Nyss platform

Global Coordinator	The Global Coordinator is a representative of Norcross managing the Nyss platform. The Global Coordinator creates the Account for National Societies and grants access to it to the Head Manager.	The Global Coordinator acts as a processor. Regarding his/her personal data, the individual acting as Global Coordinator is also a data subject.
Head Manager	The Head Manager enters into the agreement with the Global Coordinator on behalf of a contracting party.	The Head Manager acts as a controller. At the same time, the Head Manager is a data subject, whose data will be processed by the Global Coordinator.
Manager	The Manager is a representative of the contracting party.	The Manager acts as a controller. At the same time, the Manager is a data subject, whose data will be processed by the Global Coordinator and the Head Manager.
Technical Advisor	The Technical Advisor could be a representative of Norcross or the International Red Cross and Red Crescent Movement. This User can be created by the Global Coordinator and it may have access to several Accounts upon requests for support from the contracting party. The Head Manager will have an option to add the Technical Advisor as an “existing user”. Such a request can also be processed directly by Manager.	The Technical Advisor acts as a processor. Regarding his/her personal data, the individual acting as Technical Advisor is also a data subject.
Supervisor	A representative of the contracting party.	The Supervisor acts as a representative of the controller. At the same time, the Supervisor is a data subject, whose data will be processed by the Manager.
Data Collectors	Individuals, who in some cases receive compensation and reimbursements, and who receive training to identify public health risks.	In the sense that their own personal data will be processed within the system, they are data subjects.

Data Consumers	The Data Consumer acts as a “third party” who, under the direct authority of the contracting party, are authorised to access to the Nyss platform.	Regarding their personal data, the individuals acting as Data Consumers are also data subjects.
Affected community members	Affected community members are the ones presenting symptoms considered as a health risk/event and whose personal data are going to be processed in the pseudonymised and sometimes aggregated form.	Within the Nyss platform, affected community members are only data subjects.

Annex 4

Types of personal data processed in the Nyss platform

Global Coordinator	Email, Name, Phone number, Additional phone number (optional), Organization (optional).
Head Manager	Email, Role in Nyss, Name, Phone number, Additional phone number (optional), Organization (optional).
Manager	Email, Role in Nyss, Name, Phone number, Additional phone number (optional), Organization (optional).
Technical Advisor	Email, Role in Nyss, Name, Phone number, Additional phone number (optional), Organization (optional).
Supervisor	Email, Role in Nyss, Name, Phone number, Additional phone number (optional), Organization (optional), Birth group (10 year groups), Sex (Male, Female, Other).
Data Collectors	Name, Display name, Sex (Male, Female, Other), Birthyear group (10 year groups), Phone number, Additional phone number (optional), Central location of responsible area, Name of Region/District/Village and Zone (optional) of responsible area, Name of responsible Supervisor in Nyss.
Data Consumers	Email, Role in Nyss, Name, Phone number, Additional phone number (optional), Organization.
Affected community members	Age group (below 5 or above 4 years), gender (Male, Female), health risk, residence area (village, district, region and optional zone), central GPS coordinates of the residence area.