31 March 2020

Nyss PLATFORM DATA PROTECTION IMPACT ASSESSMENT REPORT
This document was commissioned under contract for a data protection impact assessment report concerning the set-up of the Nyss platform by the Norwegian Red Cross (NorCross). The document was prepared by Lina Jasmontaite and Julia Zomignani Barboza under the supervision of Paul Quinn. The document was co-authored by Nikolai Riedel and Tine Mejdell Larsen. Information concerning the factual data processing was provided by NorCross representatives. The document can be made available for transparency and information purposes only and does not constitute legal advice.
<table>
<thead>
<tr>
<th>Version</th>
<th>Comment</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Finalized version by VUB</td>
<td>31.03.2020</td>
</tr>
<tr>
<td>1.1</td>
<td>Updated SW version of SMSEagle GDPR report to include down to v 3.1</td>
<td>16.04.2020</td>
</tr>
</tbody>
</table>
Contents

1. Introduction .............................................................................................................................................. 5
1.1. Project description: the Nyss platform ................................................................................................. 6
1.2. Project background ................................................................................................................................. 7
1.3. Methodology .......................................................................................................................................... 8

2. Impact assessment method ..................................................................................................................... 9
2.1. Who should carry out a DPIA? .............................................................................................................. 12
2.2. DPIA threshold analysis ....................................................................................................................... 13
2.3. Processing on a large scale ................................................................................................................... 14
2.4. Vulnerable data subjects ...................................................................................................................... 14

3. Description of data flows in Nyss .......................................................................................................... 15
3.1. Data flows to the Nyss platform .......................................................................................................... 15
3.2. Data flows inside the platform ............................................................................................................. 15
3.3. The dashboards ..................................................................................................................................... 16
3.4. Exporting data ...................................................................................................................................... 16
3.5. Escalated reports ................................................................................................................................... 17

4. Types of users and their personal data ................................................................................................... 18
4.1. Roles and responsibilities of users ....................................................................................................... 19

5. The role of the Norwegian Red Cross ................................................................................................... 22
5.1. NorCross’ obligations as a controller .................................................................................................. 23
5.2. NorCross’ obligations as a processor .................................................................................................. 27
5.3. Legal basis for processing personal data of National Societies’ personnel ..................................... 28

6. The role of National Societies ............................................................................................................... 28
6.1. A note on joint controllership .............................................................................................................. 29
6.2. Registering Data Collectors by Supervisors ...................................................................................... 29
6.3. Improvements based on data protection considerations ................................................................. 32
6.4. Legal basis for the collection of personal data ............................................................................... 33
6.5. Purpose limitation ............................................................................................................................... 35

7. Rights of data subjects ........................................................................................................................... 36
7.1. The right to information ..................................................................................................................... 37
7.2. The right of access .............................................................................................................................. 37
7.3. The right to rectification ...................................................................................................................... 38
7.4. The right to erasure ............................................................................................................................. 38

8. SMS gateway: SMSEagle ......................................................................................................................... 39

9. SMS reports ............................................................................................................................................ 41
9.1. Content sent by Data Collectors ......................................................................................................... 41
9.2. Reporting on an affected community member ................................................................................... 41
9.3. Aggregated reports on affected community members ....................................................................... 42
9.4. Content of data collection points ....................................................................................................... 42
9.5. Metadata .............................................................................................................................................. 43

10. Nyss: reasoning for a cloud-based solution ......................................................................................... 44

11. Recommendations ............................................................................................................................... 45

Appendix I — SMSEagle GDPR Compliance Report ............................................................................. 48
Appendix II — Conformity with EU Radio Equipment Directive .......................................................... 52
1. Introduction

The processing of personal data, especially of vulnerable populations, can bring severe negative consequences for individuals and hence such processing calls for tools to address such possible negative outcomes (frequently referred to as risks). One of the ways to address these risks is to attempt to foresee them in advance and to deal with them in a preventive manner, before they materialise. This is done by minimising or, when feasible, eliminating negative consequences and maximising, if possible, positive outcomes.

An important tool to achieve this end is the process of data protection impact assessment (DPIA). In this regard, the present document presents the DPIA report of the Nyss platform. It closes the DPIA process, presenting the process’ analyses and recommendations.

The Norwegian Red Cross (NorCross) commissioned a Data Protection Impact Assessment (DPIA) in order to gain a better understanding of the data processing operations and associated risks within the platform the organisation is developing to implement a real time community-based surveillance (CBS) system.\(^1\) The DPIA was conducted during the Nyss development and testing phase. To complete the DPIA process, in this document we assess whether and how the processing of personal data related to the reporting of health risks via Nyss is compatible with the principles stemming from the EU data protection framework, in particular the General Data Protection Regulation 2016/679. This DPIA report also includes references to the applicable data protection regime in Senegal, where the platform will first be implemented. The Senegalese regime, to a large extent, includes similar principles and requirements as foreseen in the EU data protection framework.\(^2\) The DPIA, however, has been conducted keeping in mind the possibility of launching Nyss in other countries as well, as that would involve data processing operations that are similar in nature, scope, context, purpose and risk.

Provided that the primary aim of the DPIA process is to assess potential impacts of Nyss in terms of adherence to data protection principles, the assessment includes a description of the personal data processing operations and the purposes of Nyss. While the main purposes of the platform are the protection of public health interests, prevention of serious (cross-border) threats to health, monitoring and alerting of suspected diseases, prevention or management of infectious diseases and other threats to health, the analysis in this report distinguishes the roles and responsibilities of NorCross as developer and host of the platform from those of other red cross or red crescent National Societies that will use Nyss in terms of data protection obligations, including the ones concerning implementation of data subject rights.\(^3\)

In particular, the assessment points out that for part of processing operations NorCross acts as a controller and for the other part it acts a as processor. Provided this legal set-up, it has to follow different GDPR requirements according to the role is plays in each processing activity. For consistency purposes, however, taking a comprehensive approach to compliance with the GDPR may be a more appropriate strategy.

The assessment recognises that while NorCross decides and defines personal data collection processes within Nyss (i.e. what personal data should be collected and by what means), it acts as a developer. It defines such default settings available for National Societies at the platform development stage in order to ensure early warning and response to health risks in local communities.

The report also considers the applicable legal ground for different processing operations carried out by the two main actors of the platform – i.e. NorCross and other National Societies.

The assessment, after describing data flows within the platform, identifies users, their functionalities and roles from the data protection point of view. The assessment concludes that

\(^1\) While our analysis suggests that the threshold for high-risk criteria further defined by EU regulators is not met, conducting a DPIA is still deemed to be a good practice as it allows of the foreseen processing operations and potential risks arising from such processing.

\(^2\) See the Gap Analysis of Senegalese Data Protection and the GDPR.

\(^3\) The term ‘National Society/ies’ is used to refer to any implementing partner that runs their own instance of the codebase, e.g. it could possibly also include IFRC.
Nyss includes a role-based access control system, where users are assigned roles corresponding to their functions. The predefined governance structure is considered to be an appropriate measure ensuring usability, consistency, and security of data, including personal data, in the platform.

With regard to the assessment of risks to individuals arising from the processing of users’ personal data, the analysis takes into account the principles of data minimisation, necessity and proportionality of the processing in relation to the purpose of the processing. This assessment pays a particular attention to the collection of personal data about Data Collectors, who although constitute an essential part of Nyss (as they report health risks), do not have direct access to the platform.

The assessment, when providing descriptions of different Nyss comportments, describes technical security measures taken to comply with the requirements stemming from the GDPR. While doing so, the assessment refers to publicly available technical descriptions and reports made available by technology providers (i.e. Microsoft Azure and SMSEagle).

1.1. Project description: the Nyss platform

Within the scope of this project, the Norwegian Red Cross (NorCross) aims at launching a community-based surveillance (CBS) system (so-called the Nyss platform), including a digital platform for data collection, analytics, visualisation, generation of automatic alerts and data sharing (all of these elements are further explained below). CBS is considered to be ‘the systematic detection and reporting of events of public health significance within a community by community members’.

In this regard, the main objective of CBS based systems is to complement health authorities’ efforts in detecting risks and events that are relevant for public health and fill potential gaps in existing detection systems to ensure timely information is acquired at the community level to enable quick responses to contain the spread of contagious diseases. More specifically, while information gathered by health authorities is mainly based on information collected by healthcare facilities when treating patients, CBS allows, as is further explained below, the detection of public health risks/events in populations that do not seek treatment at healthcare facilities or that experience barriers to treatment (e.g. living in a remote location). In particular, CBS can provide early detection and response to health risks and events having public health significance that may not be detected by existing systems, but that, if untreated, could result in epidemics.

CBS systems’ capabilities to attain their primary objectives as well as the underlying goal of improving the overall global health security rely on data provided by Data Collectors – in this

---

6 Ibid.
project, volunteers registered with national Red Cross and Red Crescent societies (National Societies) – living and working directly with the affected communities, who are also consulted before launching a CBS project in their community.

To ensure that National Societies can activate such system globally, the Norwegian Red Cross (NorCross) has been working in cooperation with the following actors:

- Vrije Universiteit Brussel (VUB) - Research Group on Law, Science, Technology & Society (LSTS);
- Clave Consulting AS;
- The International Federation of Red Cross and Red Crescent Societies (IFRC) health team and legal service;
- DoLittle;
- Itera;
- Volunteer IT experts (through hackathons organised in March and April, October of 2019);
- Microsoft Norway;
- Bekk Consulting;
- Belgian Red Cross;
- Somali Red Crescent society; and
- Senegalese Red Cross society.

To anticipate possible consequences to individuals whose personal data are going to be processed via Nyss as well as to ensure a wide acceptance of the system, a Data Protection Impact Assessment (DPIA) is concluded before the launch of the system. In the context of this assessment, the following sections of this impact assessment report explains the processing activities expected to be conducted by CBS systems and evaluates their compliance with principles related to the protection of personal data. In brief, the processing activities involving personal data (also referred to in this report as data points and data sets) that are intended to be undertaken throughout the different stages of Nyss are the following:

- Registration of users and Data Collectors;
- Data collection in community;
- Reporting;
- Cross-checking of reports;\(^8\)
- Data management and analysis;
- Dissemination;\(^9\)
- Response & Feedback.

### 1.2. Project background

The development of CBS is a strategic priority for Norwegian Red Cross’ international programmes and preparedness department. It seeks to support Red Cross and Red Crescent

---

\(^8\) This stage includes verification of the symptoms by the supervisor with the data-collector and automatic internal evaluation if reports of data-collectors by adjacent supervisors should be counted as a single alert.

\(^9\) This stage includes sharing data. Only pseudonymised or anonymized data is shared across the boundaries of national societies.
volunteers, staff and delegates, from local to global levels, in health related decision-making based on relevant and reliable information in real-time.\textsuperscript{10} The driving force behind a custom-built CBS application for the Red Cross and Red Crescent movement (the Nyss platform) is the fact that: \textit{since starting CBS related work in 2012, the assumption has been that technologies and tools are already out there, we just need to access and use them. But, after three implementation phases and extensive research, we came to the conclusion that we need a custom-built application that could be also adapted to local needs and context.}\textsuperscript{11} In particular, the development of Nyss builds on the lessons learned in previous CBS platform pilots, which showed that:\textsuperscript{12}

1) volunteers can be trained to detect and report disease outbreaks, such as cholera (Haiti Cholera, 2014).
2) Scale up and exhaustive coverage is possible through strong volunteer management, and utilising scalable business intelligence tools (Sierra Leone, Ebola 2015).
3) shifting focus from data management to public health response requires automation of data processing (Madagascar Plague, 2016).

1.3. Methodology

The assessment made in this report builds on the systematic analysis made in guidance documents published by the Article 29 Working Party (WP29)\textsuperscript{13} the European Data Protection Board (EDPB), the French Data Protection Authority (CNIL) and the Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab).

Taking into account that the General Data Protection Regulation (EU) 2016/679 (GDPR) was incorporated into the European Economic Area (EEA) agreement and became applicable in Norway on 20 July 2018 and that Norwegian entities processing personal data are bound by the GDPR in the same manner as entities in the EU Member States, this report will refer to the GDPR and not to the Norwegian Act of 15 June 2018 no. 38 relating to the processing of personal data that implements the GDPR. Consequently, the terminology that is used in this report is based on concepts and definitions provided in the GDPR.

In addition to this guidance, this report also takes into consideration specific suggestions made by the IFRC and the International Committee of the Red Cross (ICRC) data protection frameworks. The two frameworks were developed with humanitarian principles and the needs of humanitarian workers in mind and therefore should be incorporated into the DPIA process. In fact, both frameworks stipulate an obligation to conduct a DPIA in cases where the processing of personal data could result in a high risk to the rights and freedoms of a data subject – the same formula used in the GDPR. A DPIA, therefore, should assess such risks and offer ways to mitigate them.

\textsuperscript{10} Norwegian Red Cross, ‘Community Based Surveillance (CBS) Project Mandate 2018 - 2020’ (2018)
\textsuperscript{2}.

\textsuperscript{11} Based on the information shared during the call with NorCross.


\textsuperscript{13} With the entry into force of the General Data Protection Regulation WP29 was replaced by the European Data Protection Board (EDPB).
Having in mind that a DPIA is a process for building and demonstrating compliance for either a single data processing operation or multiple operations that are similar in nature, scope, context, purpose and risk, the following sections develop a DPIA that, while primarily focuses on the implementation of the Nyss platform in Senegal, can be used to assess the implementation of CBS with Nyss in different countries. The reasoning behind conducting a single DPIA to assess the implementation of the Nyss platform globally is that the platform concerns predefined personal data processing operations that present similar risks within any country using Nyss. To complete the DPIA process, in this document, we assess whether and how the processing of personal data related to the reporting of health risks/events via Nyss is compatible with the principles stemming from the EU data protection framework, in particular the GDPR, which is increasingly considered the “gold standard” in data protection. When conducting a DPIA, it is important to consider that a “risk” is understood as ‘a scenario describing an event and its consequences, estimated in terms of severity and likelihood,’ whereas “risk management” is ‘defined as the coordinated activities to direct and control an organization with regard to risk.’ Also, when discussing high risk to the rights and freedoms of individuals, concerns are not limited to the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

Finally, the DPIA process takes into consideration the specific context of humanitarian action, which is considered to be ‘one of the humanity’s great moral achievements in last sixty years.’ In this regard, concerns about physical security of affected individuals should be anticipated and addressed within the scope of a DPIA. On the other hand, it is worth noting that despite the positive impact humanitarian action brings - such as restored health, skills learned, improved gender relations; the humanitarian sector may also create risks and ethical tensions. Recognising such possibilities, the DPIA process seeks to anticipate and identify such tensions and propose ways to address them already during the technology development phase. To the extent necessary, this report refers to publicly available technical descriptions provided by technology providers (e.g. Microsoft Azure) and manufactures (e.g. SMS Eagle) as well as expert reports.

This report is prepared on the basis of exchanges and knowledge sharing between NorCross, IFRC and VUB during a series of calls hosted during the period of April 2019 – March 2020.

2. Impact assessment method

---

15 A note should be taken that a DPIA per se does not ensure compliance with the GDPR.
17 Ibid.
19 Ibid 7.
The process of DPIA is a derivative of privacy impact assessment (PIA). Both tools—PIA and DPIA—belong to a larger family of impact assessments, which could be defined as tools ‘used for the analysis of possible consequences of an initiative on a relevant societal concern or concerns, if this initiative can present dangers to these concerns, with a view to support the informed decision-making whether to deploy this initiative and under what conditions, ultimately constituting a means to protect these concerns.’

The momentum for DPIA came with the approval of the GDPR in the EU in 2016, which introduced a requirement for data controllers to conduct an assessment of the impacts of data processing operations that are ‘likely to result in a high risk to the rights and freedoms of natural persons’ with regard to the processing of their personal data (Art. 35 GDPR).

While the DPIA is a new addition to the EU data protection framework, it builds on the rich experience of conducting impact assessments in business practices in fields concerning, for example, environment and information technology.

**Impact assessments are conducted to assess the consequences (“impacts”) of activities carried out in the context of a project and their severity.**

To be effective, impact assessments are carried out at the early stage of a project (proactive initiative), at the phase of planning or designing, and are aimed to anticipate the potential beneficial and adverse (i.e. negative) impacts of such project. Impact assessments help decision-makers find the best and most beneficial solutions for the development and deployment of initiatives. To be practical, impact assessments must be scalable, flexible and applicable inter alia for large organisations, consortia or for small and medium-sized enterprises.

**Risk management is the systematic process of identifying and assessing risks, avoiding or mitigating them where possible, and then accepting and managing the remaining ones.**

---
21 The tool of DPIA has been frequently criticised for being a ‘poor cousin’ of PIA, as the former is triggered only when personal data are being processed, excluding from its scope e.g. non-personal data processing that impact negatively on one’s privacy. Hence, resorting solely to DPIA might employ a wrong tool for a job. However, DPIA, at least in the EU, is meant to, *inter alia,* protect all fundamental rights whenever personal data are being processed.


24 E.g. environmental impact assessments originated from green movements in the 1960s (read more at: International Association for Impact Assessment: Principles of Environmental Impact Assessment Best Practice <https://www.eianz.org/document/item/2744> [07/05/2016]) and social impact assessments (SIA) were developed in the 1980s. SIAs aim at ensuring that developments or planned interventions maximise the benefits and minimise the costs of those developments, including, especially, costs borne by the community (for more information read: The Interorganizational Committee on Guidelines and Principles for Social Impact Assessment: Guidelines and Principles for Social Impact Assessment <http://www.nmfs.noaa.gov/sfa/social_impact_guide.htm>).
The elements of an impact assessment may vary, depending on the specific area in which it is conducted. Building on the experience of previous DPIA processes conducted by the VUB and recommendations put forward by the EDPB, this data protection impact assessment includes the following steps:

1. Threshold analysis – determining whether personal data processing activities require an impact assessment;
2. Description of the envisioned processing – e.g. identification, characterisation and description of applications processing personal data in the Nyss;
3. Assessment of the necessity and proportionality;
4. Measures already taken;
5. Assessment of the risks to the rights and freedoms;
6. Measures envisioned to address risks;
7. Documentation;
8. Monitoring and review - according to the GDPR, there is no mandatory timeframe to follow when reviewing the DPIA process. The review of a DPIA should be carried out by the controller, where necessary, to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change in the risk represented by processing operations. In situations where there are multiple parties (e.g. a number of controllers can join the processing operations at different points in time) there is no need to conduct a new DPIA, if such scalability of the project has been considered at its inception. More guidance in this respect is provided by the European data protection regulators:

A new (i.e. revised version of) DPIA could be required if the risks resulting from the processing operations change, for example because a new technology has been introduced or because personal data is being used for a different purpose. Data processing operations

---

can evolve quickly and **new vulnerabilities** can arise. Therefore, it should be noted that the **revision of a DPIA is** not only **useful for continuous improvement**, but also critical to maintain the level of data protection in a changing environment over time. A new DPIA may also become necessary because the **organisational or societal context for the processing activity has changed**, for example because the effects of certain automated decisions have become more significant, or **new categories of data subjects become vulnerable** to discrimination.

Each of these examples could be an element that leads to a change in the risk analysis concerning the processing activity at hand. Conversely, certain changes could lower the risk as well. For example, a processing operation could evolve so that decisions are no longer automated or if a monitoring activity is no longer systematic. In that case, the review of the risk analysis made can show that the performance of a DPIA is no longer required.

The process of DPIA is described in more detail in the following sections. In addition, we suggest tailoring the DPIA to the scope and goals of the CBS project by including considerations concerning the humanitarian sector, such as humanity and impartiality, “do no harm”, participation by beneficiaries and building on local capacity, and accountability.27 Due to the specific humanitarian goal of NorCross’ effort to develop a CBS platform, we deem it important to comply with these principles as well as with the requirements stemming from the EU data protection framework.

### 2.1. Who should carry out a DPIA?

Article 35 of the GDPR requires controllers, that is, the person or entity that ‘determines the purposes and means of the processing of personal data’ (art. 4 GDPR), to conduct a DPIA in cases where the processing of personal data is ‘likely to result in a high risk to the rights and freedoms of natural persons’.28 This means that other parties concerned with the processing operations within a particular project or initiative do not have an obligation to conduct a DPIA. It should be noted, however, that processors - that is, actors who process personal data on behalf of the controller (art. 4 GDPR) - should assist controllers complying with a DPIA obligation as they often provide infrastructure for the processing and have a better overview of the entire lifecycle of the management of personal data.

Considering the attribution of responsibilities within Nyss (see sections 5 and 6), NorCross is responsible only for a limited set of processing operations concerning the creation of accounts for National Societies.29 The personal data involved in such processing is limited to professional contact details and it does not include special categories of personal data. In practice, the National Societies implementing CBS at the national level are the ones responsible for the collection and processing of personal data of their personnel, volunteers as well as of affected individuals.

As NorCross is the entity developing Nyss and a processor hosting Nyss, however, conducting a DPIA benefits the organisation and the system, as it not only brings transparency to the data flows within Nyss, but, most importantly, the DPIA report (or a summary of it) could be displayed to implementing National Societies to further the trust relationship between NorCross (the platform developer) and the platform’s users (National Societies). A DPIA summary in

---


28 The threshold analysis is included in the following sections.

29 Within the scope of this report a term ‘account’ refers to the national or regional profile to which the National Society representatives receive access upon agreeing to the terms and conditions of NYSS.
principle could include useful information without neither compromising secrets, nor leading to security risks by disclosing system vulnerabilities.

2.2. DPIA threshold analysis

The primary aim of this DPIA process is to assess potential impacts of Nyss in terms of adherence to data protection principles. In this regard, the first step in the DPA is to conduct a preliminary threshold analysis (initial assessment) to determine whether a DPIA is necessary as it is prescribed in Article 35 of the GDPR. A DPIA is necessary if the envisaged processing operations entail:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b) processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences; or
c) a systematic monitoring of a publicly accessible area on a large scale.

While at first Nyss may not seem to meet any of these three requirements, considering the possible scalability of Nyss, as defined in the platform’s functional requirements,\(^{30}\) as well in the project mandate, the second condition is likely to be met once the system is deployed in multiple countries, as Nyss may, in that case, result in large scale processing (see section 2.3). The text messages sent by Data Collectors (that often include volunteers) will essentially report risks and events concerning public health and will include personal data of local community members concerning their health in the pseudonymised form (see section 2.4).\(^{31}\) Also, it may be argued that the third condition – a systematic monitoring of a publicly accessible area on a large scale – is partially met. The qualifying criterion of “large scale”, however, can be debated. Such criterion is discussed below in section 2.3.

Despite possible different interpretations of the criteria set in the GDPR, we believe that a DPIA should be conducted for Nyss because such a system is likely to entail the processing of personal data of vulnerable individuals. Furthermore, the processing may be of a large scale as the system is easily scalable and could be launched in different countries and regions across the globe simultaneously. Furthermore, conducting a DPIA and adopting a risk-based approach can be considered to be the best practice in humanitarian action embraced by numerous humanitarian organisations and data protection experts.\(^{32}\) Finally, conducting a DPIA could also be seen as a pre-condition for the application of the principle of “do no harm” in a digital environment, due diligence, and part of a “best efforts obligation” stemming from humanitarian principles.\(^{33}\)

---

\(^{30}\) Norwegian Red Cross, ‘Functional Requirements: Community Based Surveillance’; Norwegian Red Cross.

\(^{31}\) In this regard, ‘data concerning health’ is understood as personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

\(^{32}\) Christopher Kuner and Massimo Marelli, ‘Handbook on Data Protection in Humanitarian Action’ 164.

2.3. Processing on a large scale

The GDPR does not define what constitutes processing on a large scale. According to recital 91, large scale processing operations ‘aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity.’ Additional guidance in this respect is provided by the WP29, which recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

- the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
- the volume of data and/or the range of different data items being processed;
- the duration, or permanence, of the data processing activity;
- the geographical extent of the processing activity.

At the moment, Nyss is developed in a way that allows it to be easily scalable as it can be launched in different countries, provided it has the assistance of local authorities and national Red Cross or Red Crescent Societies. There is neither a limitation set on the number of health reports that can be sent, nor on the number of Data Collectors. Considering these settings, we conclude that the processing of personal data within Nyss may be carried out on a large scale.

2.4. Vulnerable data subjects

According to Recital 75, a DPIA should be conducted if the processing concerns data of vulnerable data subjects. The WP29 argues that the processing of this type of data is a criterion for conducting a DPIA because of the increased power imbalance between the data subjects and data controllers. According to the European regulators, vulnerable data subjects may also include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), employees (in relation to their employers due to the power relationship that exists between them), and other vulnerable segments of the population requiring special protection (e.g. mentally ill persons, asylum seekers, the elderly, medical patients, etc.)

In the particular context of Nyss, community members presenting health risks (to whom pseudonymised health reports relate) may be considered vulnerable and unable to consent to, or oppose, the processing of their data, or exercise their rights. Furthermore, in some circumstances, Data Collectors and personnel of National Societies may also include vulnerable data subjects. As explained by some regulators, even if these individuals are not part of a group that might automatically be considered vulnerable, an imbalance of power in their relationship with the controller (in particular with the National Society) can cause vulnerability for data protection purposes, if such individuals would be disadvantaged in case the processing of personal data is not performed.

---

34 Please note, recitals are not legally binding, yet are used to interpret the binding provisions.
36 This is especially true since scalability is one of the guiding principles of this project, i.e. NYSS lightweight approach in terms of local infrastructure and resources facilitates scaling NYSS to cover as many community members as possible.
3. Description of data flows in Nyss

3.1. Data flows to the Nyss platform

High level data flow and functional areas

![Data flow diagram]

Figure 1: Data flow of reports about community members.

The above graph depicts the initial vision of data flows within different components of a previous CBS platform, created in 2018 (the principle data flows stay the same to this day). Following this structure, the “data collector” – a volunteer from an implementing National Society – sends a health report via a text message to the SMS gateway. For the purposes of this document we will consider SMSEagle as the SMS gateway as well as a cloud based alternative solution. SMSEagle has a so called “Callback URL plugin”, that allows forwarding incoming SMS messages to a defined URL address. In principle, it functions as an API endpoint likely based on the URL created for Nyss. This allows the two parts of Nyss (the SMS report sent to SMSEagle and the website interface - URL) to communicate with each other. When the plugin is enabled, for each incoming SMS message, the SMSEagle triggers a HTTP(S) request to a defined URL. The SMSEagle identifies itself via a so-called API Key that it adds to the query string of each request to the URL, i.e. each SMS it forwards to Nyss. While the API Keys can be freely defined in the configuration of the SMSEagle, we use Universally Unique Identifiers (UUIDs), with an extremely low collision probability. The same API Key as in the SMSEagle, is configured in a National Society in the CBS platform. Nyss matches incoming reports to National Societies via this API Key / UUID.

This API Key would be linked to the country where the system is being used and would be created by NorCross upon concluding the agreement with the country’s National Society to join Nyss.

3.2. Data flows inside the platform

---

38 API stands for application program interface.
With the development of the project, however, the initial data flow graph was revised, and the following graph presents a view of data flows, including personal data, within the platform. This graph also introduces the roles of different users in the platform.

![Data Flows Diagram](image)

**Figure 2: Data flows inside NYSS**

Following this graph, text messages with reports (SMS reports) sent by Data Collectors would be uploaded into a sub-section of the Nyss web portal (each country deploying the system would have its own sub-section – a dedicated service environment – or a national “profile”) that would be accessible only to the concerned National Society (the one located in the country deploying the system). The SMS report itself is seen as a line/report list in Nyss and it would not be visible to NorCross or to other Nyss actors outside the country in which the National Society is operating. These sub-sections of the platform could also be made available to the technical advisor if assistance is required by the responsible manager in the National Society. Users can manually export this list to csv (i.e. a comma-separated values) files.

### 3.3. The dashboards

Nyss provides the possibility to see a summary of the SMS reports in the form of graphs and charts on the project and National Society dashboards. The dashboards can be accessed by different users who need to have e.g. an overview of the number of reports or active Data Collectors. While the project dashboard aggregates data across one project, the National Society dashboard aggregates data across one National Society. The shown aggregated information includes: reported health risk/event by location, reported health risk/event by village, number of reports by health risk/event, reported health risk/event by sex and age in a map, bar charts and a table. It includes pseudonymised data, which means that the linkability of the dataset with the data subject is reduced. The dashboards also give users the possibility to filter data for a reporting period, location, and type of a risk reported.

---

39 The provision of technical assistance, upon a request of the national society, would be an exception to this default setting.

40 The location, the respective Data Collector was initially registered to.
While Global Coordinators only have access to the National Society dashboard, users that are part of a National Society have access to the project dashboard. Data Consumers have access to project dashboards, if National Societies decide to give them access. The dashboards also include the number of reports that contained an error. This information may be useful in order to evaluate whether additional training and follow-up with Data Collectors, who are (in many cases) volunteers and not necessarily medically trained professionals, is necessary.

### 3.4. Exporting data

An implementing National Society may decide to share raw reports received from Data Collectors with local authorities, such as ministry of health representatives or responsible healthcare workers. Raw data reports include data about Data Collectors. Sharing raw reports is possible through exporting the aggregated data from the platform and then handing/sending it manually to external parties. The platform does not implicitly allow the sharing functionality of a single data report. Raw data reports include pseudonymised data of affected individuals, which means that the linkability of the dataset with the data subject is minimised.

### 3.5. Escalated reports

If a defined number of reports in the same region matches a threshold definition (the number is defined in an alert rule editable by the National Society), the platform triggers an alert. If the reports in the alert are cross-checked by any of the connected Supervisors to match the definition, the Supervisor can escalate the report. This automatically triggers an Email or SMS notification to all Email addresses and phone numbers that the National Society has put as a recipient to Supervisors that are connected to that alert. The alert recipients are solely set by the National Society. The following information is included in the Email/SMS:

1. The health risk by which the alert was triggered.
2. The name of the project in which the alert was triggered.
3. The last village from which a relevant report came from.

Justification for shared information:

1. Recipients need to know what kind of Health Risk/Event they need to investigate and if it is relevant for them.
2. Health facilities need to know in which locations the Health Risk/Event occurred.

The recipients of an alert notification will most often be representatives of the national health authorities, but they can also be representatives of the International Red Cross and Red Crescent Movement or partners. While it is possible to anticipate categories of recipients (e.g. health

---

41 So far, functionality for Global Coordinators to have access to the data dashboard has not been developed.
42 National Societies can share certain information with so called Data Consumers. However, this raw data shows no metadata of the report (i.e. data of the Data Collector such as a display name), except for the predefined location the Data Collector was registered to, which is necessary to see where events are taking place.
authorities/professionals), in principle the recipients could be anyone with an Email address/phone number. The content of the notification is kept to an absolute minimum as defined above. Any other forwarding of information is done manually and external to the platform and therefore keeping track of such processing is not possible. Other information generated through the reports may be forwarded to the relevant national authorities, who can act to prevent, stop or declare a suspected outbreak and, when necessary and following international commitments, can report it to the World Health Organisation. While NorCross can anticipate that an alert may be shared widely, it is the National Society that remains ultimately responsible for its sharing with Data Consumers and other third parties. Finally, it should be noted that only the National Society that entered into an agreement to deploy CBS using Nyss is responsible for assigning third parties that could receive such alerts.

4. Types of users and their personal data

The analysis below considers the roles of users and types of personal data collected about them within Nyss. The analysis also considers the risk level (i.e. low, moderate, high) associated with the processing of users’ personal data. The risk level in this case is presented in terms of effects on the individual if a personal data breach occurs (i.e. if personal data is disclosed accidentally or if it is accessed by an unauthorised party).43

<table>
<thead>
<tr>
<th>Global (NorCross) level</th>
<th>National Society level</th>
<th>Domestic level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global coordinator: name, surname, organisation, contact details. The processing of this data would be done within the scope of duties assigned by the employer (e.g. in the engagement contract). Such personal data does not include special categories of personal data (e.g. health related data) and therefore its processing entails a low risk if disclosed accidentally or if accessed by an unauthorised party.</td>
<td>Head Manager: name, surname, organisation, contact details. The processing of this data would be done within the scope of the duties carried out at the National Society. The processing of such personal data under normal circumstances should present low risk if disclosed accidentally or if accessed by an unauthorised party</td>
<td>Community members: for Data Collectors to prepare reports and to be able to follow up on reported cases and events with Supervisors, they need to collect personal data about affected community members. Such data about affected community members is gathered after introducing Nyss to the community in the logbook. While the logbook is not part of Nyss, information in the logbook may include special categories of personal data about affected community members, in particular, data concerning health. The processing of such data entails a high risk if disclosed accidentally or if accessed by an unauthorised party. Therefore, National</td>
</tr>
</tbody>
</table>

---

43 There are different methods to assess risk and high risk within the EU data protection framework. For the purpose of this report, we follow suggestions made by Article 29 Working Party in Guidelines on Personal data breach notification under Regulation 2016/679.
<table>
<thead>
<tr>
<th><strong>System administrator:</strong> generic login that resides with NorCross.</th>
<th><strong>Manager/Technical Advisor:</strong> name, surname, organisation, contact details. The processing of this data would be done within the scope of duties carried out at the National Society.</th>
<th>Society representatives should take appropriate measures in order to ensure and encourage that such logbooks are treated confidentially.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supervisor:</strong> name, surname, gender, age group, organisation, contact details. The processing of this data would be done within the scope of the National Societies’ arrangement for their work with local volunteers. The processing of such personal data entails a moderate risk if disclosed accidentally or if accessed by an unauthorised party.</td>
<td><strong>Data Collector:</strong> name, surname, gender, age group, location. The processing of this data would be done within the scope of the National Societies’ arrangement for their work with Data Collector that will be signed at the time of the training.</td>
<td></td>
</tr>
<tr>
<td><strong>Data Consumers:</strong> name, surname, organisation, contact details. Such personal data does not include special categories of personal data (e.g. health related data) and therefore its processing entails a low risk if disclosed accidentally or if accessed by an unauthorised party.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 4.1. Roles and responsibilities of users

A number of different users can be created within Nyss. The role of Head Manager and Manager are created by a Global Coordinator. The Head Manager and Manager can then create users with different access rights to the account of the National Society (e.g. Supervisors and Data Consumers); such users, however, cannot manage the scope of their access rights as they
are set by default – that is, each category of user created within Nyss has access rights predefined within the platform that cannot be altered.

When considering the set-up of Nyss, it is important to point out that users may play multiple roles within the meaning of the EU data protection framework. The table below demonstrates that the foreseen users can be assigned to different legal notions found in the GDPR depending on the processing operation. For example, users can act as “controllers”, “joint-controllers”, “processors”, “third-party”, or “data subjects” within the scope of the different processing operations within Nyss. A representative example in this regard is the Global Coordinator, who acts as a representative of the controller for the processing operations concerning the Head Manager’s personal data and as a data subject when the processing concerns her/his personal data. Understanding these concepts is important when determining each user’s responsibility for compliance with the GDPR.

In this regard, numerous technological and practical challenges and developments (e.g., the unlimited number of parties who could join Nyss as Data Consumers) can potentially render the attribution of these core data protection concepts unclear to the users. In the following sections, therefore, this report considers the factual circumstances of Nyss, to clearly determine the responsibilities (roles played) of each actor (e.g. NorCross and implementing National Societies) within the system.

<table>
<thead>
<tr>
<th>Username</th>
<th>Controller</th>
<th>Processor</th>
<th>Data subject</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Coordinator</td>
<td>No</td>
<td>Yes (a representative of the processor)</td>
<td>Yes</td>
<td>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 the Account to the Head Manager.</td>
</tr>
<tr>
<td>System Administrator</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>If the System Administrator is part of the same organisation as the Global Coordinator, then this user would function within the scope of responsibilities taken on by the controller. However, this user also could be outsourced. Since this is a generic login that can be used by the NorCross staff entitled to access the Nyss platform, the System Administrator is not considered to be a data subject.</td>
</tr>
<tr>
<td>Head Manager</td>
<td>Yes (a representative of the controller)</td>
<td>No</td>
<td>Yes</td>
<td>The Head Manager (on behalf of the National Society) enters into an agreement with the NorCross. At the same time, the Head Manager is a data subject, whose data will be processed by the Nyss platform.</td>
</tr>
<tr>
<td>Manager</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>The Manager is a representative of the National Society, whose data will be processed by the Global Coordinator and or Head Manager.</td>
</tr>
<tr>
<td>Technical Advisor</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>The Technical Advisor can be a representative of NorCross or the International Red Cross and Red Crescent Movement, but not within the concerned National Society. This user can be created by the Global Coordinator and it may have access to several National Societies.</td>
</tr>
</tbody>
</table>
The table above shows that Nyss includes a role-based access control system, where users are assigned roles corresponding to their functions. The predefined governance structure aims at ensuring usability, consistency, and security of data, including personal data, in the platform. In practice, this means that it is possible to manage and control users’ access rights across the platform in a systematic way.

<table>
<thead>
<tr>
<th>User</th>
<th>Functionalities</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Administrator</td>
<td>Creates Global Coordinators’ “profiles”. Can see all users within all National Societies registered in the platform, including Data Collectors.</td>
</tr>
<tr>
<td>Global Coordinator</td>
<td>Creates Head Managers’ “profile” as the first user within a new National Society’s account. Can see the list of all National Societies using the platform. Can see most user lists within National Societies, with the exception of Supervisors and Data Collectors. Can see the settings of National Society (only overview). Cannot act as System Administrator.</td>
</tr>
<tr>
<td>Head Manager</td>
<td>Signs the Nyss platform agreement to create a National Society account. Creates and edits user roles on the account of the National Society s/he represents. Can assign a new Head Manager. Has access to the accounts data.</td>
</tr>
</tbody>
</table>

The table above shows that Nyss includes a role-based access control system, where users are assigned roles corresponding to their functions. The predefined governance structure aims at ensuring usability, consistency, and security of data, including personal data, in the platform. In practice, this means that it is possible to manage and control users’ access rights across the platform in a systematic way.
5. The role of the Norwegian Red Cross

Within the scope of Nyss, the Norwegian Red Cross (NorCross) can have different users. In particular, it can act as Global Coordinator and as System Administrator. These two user roles result in separate processing activities. When it acts as Global Coordinator, NorCross is considered to be a controller in relation to the processing of personal data of Head Managers. Whereas for the processing activities concerning the role of System Administrator it acts as a processor in relation to all processing activities conducted in the platform. These classifications relate to the meaning of controller and processor within the General Data Protection Regulation (GDPR). Considering its territorial scope, the GDPR applies to both controllers and processors, either established in the EU, processing data in the EU or processing personal data of data subjects located in the EU.  

It is worth pointing out that NorCross, besides acting as a processor (when providing technical assistance) and as a controller (when processing personal data of members of National

---

45 More specifically, according to Article 3 of the GDPR, it applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. Also, it applies to the processing of personal data of data subjects who are in the Union when a controller or processor not established in the Union.

46 This statement also takes into consideration opinion of the Norwegian Data Protection Authority, which explains that the GDPR was incorporated into the EEA agreement and became applicable in Norway and therefore Norwegian entities are thus bound by the GDPR in the same manner as EU Member States.
Societies), is also the “developer” of the system itself. As developer, it defines the functional requirements of the system. Developers, however, are not subject to the obligations stemming from the GDPR as the processing of personal data is required to trigger the applicability of the Regulation. Recital 78 of the GDPR, however, encourages ‘the producers of products, services and applications’ (i.e. system) ‘to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.’ This encouragement is not legally binding for processors and developers. At the same time, it can be regarded as a good practice to follow. Furthermore, Recital 78 could be used when interpreting obligations stemming from Article 25 of the GDPR concerning data protection by design and by default requirements. While Article 25 is addressed to controllers (similarly to Article 35 on DPIAs), it is deemed by regulators that processors should assist controllers when implementing this provision and developing data processing operations with the principle of data protection by design and by default in mind.\footnote{L Jasmonita and others, ‘Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR’ (2018) 4 European Data Protection Law Review 168 <http://edpl.lexxion.eu/article/EDPL/2018/2/7>.
} Considering that NorCross plays different roles within Nyss (i.e. controller or processor), it has different obligations depending on the processing operation in question. An analysis of the requirements that controllers and processors should adhere to is provided below. However, for consistency purposes taking a comprehensive approach to compliance with the GDPR may be a more appropriate strategy.

Following the comprehensive compliance approach, NorCross would take into account the GDPR requirements applicable to both controllers and processors. This approach would also be in line with a best-efforts obligation stemming from the moral framework applicable to humanitarian actors.

Furthermore, the GDPR principles are widely reflected across domestic data protection laws outside the EU due to the convergence of law caused by so-called “Brussels effect”.\footnote{Anu Bradford, ‘The Brussels Effect’ (2012) 107 Northwestern University Law Review.
} For example, the study of the applicable data protection regime in Senegal demonstrated that it entails remarkably similar principles and requirements as foreseen in the EU data protection framework.\footnote{See the Gap Analysis of Senegalese Data Protection and the GDPR.
}

5.1. NorCross’ obligations as a controller

It is established by the case law of the Court of Justice of the EU (CJEU) and WP29 guidance that the determination of whether an entity is a controller or a processor for the purposes of the EU data protection law is a key element in the assessment of the application of the GDPR to the processing of personal data in question. Under the EU data protection framework, controllers bear an ultimate responsibility for the processing of personal data and for complying with the key data protection principles, which include: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality (security), and accountability.\footnote{European Union Regulation (EU), 2016/679 GDPR, Article 5.1.
}
Following the current set up of Nyss, NorCross acts as a controller for the part concerning the collection and processing of Head Managers’, including their contact details. The GDPR provides the following definition:

|‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (Article 4 (7)). |

It is important to recognise that while NorCross decides and defines personal data collection processes within Nyss (i.e. what personal data should be collected and by what means), it does so as the developer of the platform. In this role, it defines default settings available for National Societies in order to ensure early warning and early response to health risks/events in local communities.

**Implementation of data subjects’ rights:** this would include the provision of information notices and the facilitation of access, rectification and erasure requests for the staff of NorCross and the National Society members, whose personal data are going to be processed in the context of their duties. In particular, this should allow staff (data subjects) to get access to data that are being processed about them within the system, to rectify data concerning them and to request to have their data deleted. Requests concerning the implementation of such rights should be dealt within the timeframe of 1 month, unless such data must be kept in order to comply with a legal obligation. For more detailed description of each data subjects’ right, see section 7 on the rights of data subjects. Personal data of members of National Societies acting as Supervisors and Data Collectors would be outside the scope of this obligation, as only users within the National Society have access to such data and not NorCross.

**Responsibility for the processing** (accountability): according to Article 24 of the GDPR, the controller is responsible for implementing appropriate technical and organisational measures to ensure and to demonstrate that its processing activities are compliant with the requirements of the GDPR. When taking such measures, the controller has to take into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. Privacy policies, an inventory of the processing activities and contracts are examples of documents that facilitate demonstration compliance with this obligation. For more detailed description of an inventory see the section below on documentation.

**Implementation of data protection by design and by default principles:** according to Article 25, these two principles require ensuring that when designing a tool (e.g. platform, system, programme) that processes personal data, the key data protection principles are implemented from its inception, and that the most protective data protection settings are applied. As it has been shown by the enforcement actions undertaken by national data protection authorities (DPAs) in Greece, Germany and Romania, non-compliance with this provision may result in
It should be noted, however, that the two principles, reinforce the core data protection principles and data subjects’ rights.\textsuperscript{52}

**Documentation**: according to Article 30, data controllers are required to keep records of their processing activities. When discussing the documentation obligation alternative terms are being used, including but not limited to, an inventory, a register, and a data management plan. Upon request, these records must be disclosed to the national DPA. Keeping accurate documentation of processing activities can be useful for an entity if its compliance practices are subject to a DPA investigation.

European data protection regulators explain that documentation of processing activities must be kept in writing.\textsuperscript{53} The controller (and the processor) can choose whether to keep such records in paper or in an electronic form. It is assumed that organisations will, however, benefit more from maintaining their documentation electronically as such documentation can then be easily edited, removed, and amended as necessary. Paper documentation is regarded appropriate for SMEs and micro enterprises. It should be added SMEs (entities having less than 250 employees) are exempt from this obligation if:

- processing that is likely to result in a risk to the rights and freedoms of data subjects;
- processing that is not occasional (meaning that it is regular); or
- processing that includes special categories of data or personal data relating to criminal convictions and offences.

This exemption does not apply to NorCross when processing personal data in the Nyss context as it is going to involve continuous processing of personal data. Finally, it should be noted that multiple templates and specialist software packages facilitating documentation are available on the market. Examples of free templates are provided by data protection regulators; they are included in the folder shared with NorCross via OneDrive.

<table>
<thead>
<tr>
<th>The documentation should include information about the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• the name and contact details of the controller/representative/ DPO;</td>
</tr>
<tr>
<td>• the purpose/s of the processing;</td>
</tr>
<tr>
<td>• the categories of data subjects and personal data processed;</td>
</tr>
<tr>
<td>• the categories of recipients with whom the data may be shared;</td>
</tr>
<tr>
<td>• information regarding international data transfers;</td>
</tr>
<tr>
<td>• where possible, the applicable data retention periods; and</td>
</tr>
<tr>
<td>• where possible, a description of the security measures implemented in respect of the processed data.</td>
</tr>
</tbody>
</table>

Provided the documentation obligation described above, NorCross needs to keep a record of its processing operations concerning Nyss. Such a record should clarify that NorCross will be:

---
\textsuperscript{51} The German data protection authority has imposed the highest GDPR fine to date on real estate company Deutsche Wohnen (German Living): € 14.5 million. The enterprise is being accused of storing sensitive data on tenants and failing to reconfirm whether the data still need to be kept or not; whereas the Greek data protection authority has fined the country’s largest telecommunications company €400,000 for multiple GDPR failings, including a violation of the privacy by design principle.
\textsuperscript{52} EDPB, Data Protection by Design and by Default, version for public consultation, adopted 12-13 November 2019.
\textsuperscript{53} Based on the opinions and guidance provided by the UK DPA (ICO), the French DPA (CNIL) and the Irish DPA.
• processing personal data of specified National Society users (i.e. Head Managers) and their contact details concerning their official capacity for the purposes of setting up an account for National Societies in the platform and maintaining contact with individuals handling this account in Nyss;
• performing an international data transfer by default as the platform will be facilitated via the cloud application hosted on servers in the EU; and
• taking specific technical and organisational (e.g. access control, encryption) measures to protect the information hosted on the system.

Cooperation with DPAs: according to Article 31, controllers (and their representatives, if any) are required to cooperate, on request, with DPAs in the performance of their tasks.

Implementation of appropriate technical and organisational security measures to protect personal data.

According to Article 32, such measures may include but are not limited to

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

This article also stipulates that the role of each user and permission levels (access control) appropriate to the role including the system administrator accounts, will be defined by the controller.

This obligation also requires the controller to take due diligence and assess whether the guarantees offered by the processor, in this case the cloud service provider, are sufficient. During this process, the controller may take into account whether the processor provides adequate documentation proving compliance with data protection principles that could be found in privacy policies, records management policies, information security policies, external audit reports, certifications and similar documentation. The controller in particular should take into account the processor’s expert knowledge (e.g. technical expertise when dealing with data breaches and security measures), reliability and its resources. After carrying out a due diligence process, the controller should be able to take a decision with sufficient evidence demonstrating that the processor is suitable, it can then enter into an arrangement. It should be added that this due diligence process is not a one-time effort and it needs to be regularly repeated in order to check whether the processor is compliant. When outsourcing the processing of personal data (e.g. for the provision of technical assistance or cloud services), the controller should conclude a contract, another legal act or binding arrangement with the other entity already setting out clear and precise data protection obligations.

Data breach notification to DPAs and individuals: the controller is required to report personal data breaches that entails risks to data subjects to the DPA without undue delay (within 72 hours) of becoming aware of it. It is recommended that the controller sets an internal process to be able to detect and address breaches. The controller should also have in place arrangements with any processors the controller engages, which themselves have an obligation to notify the
controller in the event of a breach. The notification to individuals is necessary only if the breach is likely to result in a high risk to affected data subjects. Examples of high risk provided by the European data protection regulators include the following personal data breaches scenarios: exfiltration of data entered to the website (i.e. a data breach situation in case of British Airways breach in September 2018), ransomware attack encrypting data, an unauthorised access to customer data breach, cyberattack against a hospital medical records database, sending an email with personal data to the wrong list of recipients, sending a direct marketing email revealing other recipients.54

5.2. NorCross’ obligations as a processor

When discussing the role of NorCross within Nyss, it is important to consider that in order to facilitate processing within some parts of Nyss, it will act as a processor. In this regard, it must be considered that it will act as a provider of technical assistance and it will also provide cloud storage space for personal data collected and processed by National Societies.

‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Article 4 (8)).

Typically, controllers appoint processors to process the personal data on their behalf through contractual means and, therefore, processors are regarded as the secondary actors.55 This restrictive dichotomy imposed by law as noted by different scholars and practitioners is difficult to apply in practice.56 In the case of Nyss, NorCross will act as a processor for certain personal data operations. Its role as a processor will be clarified within the scope of the contractual agreement with a National Society. This being said, it should be added that, in comparison with controllers, processors have fewer obligations, which include:

Documentation: according to Article 30, processors are required to keep records of the controller’s processing activities. Upon request, these records must be disclosed to the national data protection authority.57

The documentation should include information about the following:
- the name and contact details of the controller/representative/ DPO;
- the categories of personal data processed on behalf of the controller;
- information regarding international data transfers;
- where possible, a description of the security measures implemented in respect of the processed data.

Cooperation with DPAs: according to Article 31, processors (and their representatives, if any) are required to cooperate, on request, with DPAs in the performance of their tasks.

56 Ibid.
57 For more detailed description of the documentation obligation, see the section on controller’s obligations.
Data breach notification: processors are required to notify personal data breaches to the controller. In this case, this means that following the GDPR, should NorCross encounter a ‘personal data breach’ concerning National Societies, which may include a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, it must inform them without delay. The time period for this communication could be included in the contractual obligations. However, it must be considered that National Societies act in accordance to domestic data protection laws (if in place), which may or may not include an obligation to notify data breaches. Notification of personal data breaches could be considered to be a good practice that can lead to better protection of personal data (e.g. such a notification may trigger users to change their passwords).

Implementation of appropriate technical and organizational security measures to protect personal data (Article 32).

5.3. Legal basis for processing personal data of National Societies’ personnel

The controller has to ensure that personal data is being processed in a legal and lawful way. For this purpose, the controller has to ensure that he selects one (or several) of the appropriate grounds (also referred as lawful bases for processing) that are set out in Article 6 of the GDPR. In particular, the processing of personal data is lawful in situations where:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

It should be added that point (f) does not apply to processing carried out by public authorities in the performance of their tasks.

In the case of NorCross, it can be argued that (b) performance of a contract seems to be the most appropriate ground for processing personal data of representatives of National Societies, given that by providing access to Nyss, National Societies can report and get an overview of particular health risks/events and NorCross can implement the mandate assigned to it.

6. The role of National Societies

After a careful mapping of data flows within Nyss, it can be said that National Societies act as controllers with respect to the personal data that is being collected at the national/regional level.
This consequently means that upon the creation of an account, a National Society becomes the controller for part of Nyss, over which it has de facto direct influence. The responsible personnel of each National Society can choose the types and number of users to include in the account (e.g., how many Supervisors and Data Consumers to appoint), the purpose of the processing (e.g., what kind of health risks/events can be communicated), data sharing practices (e.g., when alert notifications such as SMS to Supervisors and when alert escalation notifications - SMS, Email - can be triggered), what legal basis to invoke for the processing, the retention period (e.g., for how long the data will be processed) and with whom aggregated data based on text messages can be shared. The personal data processed by the National Society in this case would include information about personnel working for (i.e., Managers) or associated with the National Society (i.e., Supervisors and Data Collectors) as well as personal data of representatives of Data Consumers. Provided this factual influence, it is deemed that National Societies would act as controllers within Nyss. Their obligations as controllers are also explained in the Nyss platform agreement, which is signed at the time of opening an account.

6.1. A note on joint controllership

A note should be taken that when considering roles and responsibilities for different parties within Nyss, NorCross considered a possibility of having a joint controllership over personal data processing operations with National Societies. The GDPR provides the following explanation of the joint controllership:

Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects. (Article 26.1)

Following from this definition, parties qualify as joint controllers when they determine together the purposes and means to some extent and for some part of the data processing. The analysis above provides a detailed description of responsibilities that NorCross and National Societies have over personal data processing operations within Nyss. This legal analysis demonstrates that even though parties are engaged in the processing operations on the same platform, due to role based access control, they do not have access to all personal data collected through the platform, the ‘factual influence’ of the processing operations remains separate on the domestic/regional and global level.

6.2. Registering Data Collectors by Supervisors

The data concerning health risks/events in Nyss will be provided by individuals, who are assigned the role of Data Collectors. In some cases, these individuals will be volunteers and in some cases these individuals will be persons associated with National Societies. Data Collectors can be registered in the system by representatives of the National Society or in case of deployment as an Emergency Response Unit by representatives of the deploying National
Society (or IFRC). The registration phase and data collected during this process is essential as it allows to verify that the sender of a given message is a registered Data Collector. In addition, the platform needs to be able to allocate incoming messages to route incoming reports to the Supervisors, that are responsible for that particular Data Collector. This is done by linking the telephone number of the incoming report to a list assigned to a Supervisor. Additionally, if a number of incoming reports meets the alert rule of the corresponding health risk/event set by the National Society, then an alert is triggered. The Supervisor then cross-checks the reports with the Data Collectors that sent in the reports, to make sure that no erroneous alerts are escalated to any external parties (recipients of alert notifications). To attain this purpose, the Supervisor can call each data collector and follow up on the report in case of doubt or if that is deemed to be necessary. For this contact to be possible, it is essential that the Supervisor has access to the phone number and the name of the Data Collector.

The table below explains what types of data are collected from Data Collectors and why.

<table>
<thead>
<tr>
<th>Details about the data processed</th>
<th>Data categories</th>
<th>Justification of the need and relevance of the data</th>
<th>Minimization controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full name</td>
<td>General; identifier</td>
<td>To ensure the verifiable identity of an individual.</td>
<td>N/A</td>
</tr>
<tr>
<td>Display name</td>
<td>General; identifier</td>
<td>To be able to separate individuals with similar names. To use instead of full name in an alert list which is visible for other Supervisors.</td>
<td>A volunteer can select any name; it can be a pseudonym.</td>
</tr>
<tr>
<td>Age group (10 years per group)</td>
<td>General; identifier</td>
<td>To have an overview of the success of the programme in terms of participating age groups.</td>
<td>By only saving the age group in 10-year intervals, it is still possible to get an overview of the participating age groups, while minimising the chance to identify Data Collectors by their date of birth.</td>
</tr>
<tr>
<td>Sex (female, male, other)</td>
<td>General; identifier</td>
<td>To have an overview of the success of the programme in terms of sex balance.</td>
<td>By allowing “other” as a choice, we provide Data Collectors with an option to refrain from revealing their sex.</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>General; identifier</td>
<td>To automatically locate reports on a map, we need to have a longitude/latitude combination. Alert rules try to find reports from separate Data Collectors, that are possibly connected due to geographical closeness. For this function the longitude/latitude combination is needed.</td>
<td>The location is a longitude/latitude combination, which is taken from a point on a map that is chosen upon registration. It can only manually be updated and in particular it is not any kind of real time tracking of the location of a Data Collector.</td>
</tr>
<tr>
<td><strong>Phone number</strong></td>
<td>General; identifier</td>
<td>To verify that a message comes from a registered volunteer. In case follow-up communication is necessary, it allows the National Society representative (in most cases a Supervisor) to contact the Data Collector and inquire further details about reported cases. It would also be used to evaluate volunteer performance based on the number of messages sent to the SMS gateway.</td>
<td>In many cases the phones used by the Data Collectors are bought by the National Society or Emergency Response Unit running the CBS implementation. That means the phones are actually registered to that entity and not to the Data Collector.</td>
</tr>
<tr>
<td><strong>Region</strong></td>
<td>General; identifier</td>
<td>Necessary to identify places that are covered by volunteers. Necessary to see where reports are coming from.</td>
<td>Currently not connected to any geospatial data such as GPS coordinates.</td>
</tr>
<tr>
<td><strong>District</strong></td>
<td>General; identifier</td>
<td>Necessary to identify places that are covered by</td>
<td>Currently not connected to any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>geospatial data such as GPS coordinates.</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------</td>
<td>------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Village</td>
<td>General; identifier</td>
<td>Necessary to see where reports are coming from.</td>
<td>Currently not connected to any geospatial data such as GPS coordinates.</td>
</tr>
<tr>
<td>Zone (optional)</td>
<td>General; identifier</td>
<td>Necessary to identify places that are covered by volunteers.</td>
<td>Currently not connected to any geospatial data such as GPS coordinates.</td>
</tr>
<tr>
<td>Additional phone numbers (optional)</td>
<td>General; identifier</td>
<td>In some cases, Data Collectors use more than one phone, or they switch phones.</td>
<td></td>
</tr>
</tbody>
</table>

6.3. Improvements based on data protection considerations

During the DPIA process, significant efforts have been made to ensure the collection of personal data from Data Collectors meets the principles of data minimisation and purpose limitation. For example, it became evident that having an overview of the initial data categories foreseen to be collected allowed the identification of numerous additional purposes for the collection of data from Data Collectors (in some cases volunteers) apart from the main purpose of Nyss – namely, protecting the interests of public health, preventing serious cross-border threats to health, monitoring and alerting of suspected diseases, preventing or controlling communicable diseases and other threats to health.

For example, the collection of data concerning gender serves the purpose of measuring whether Data Collectors/volunteers constitute a gender representative sample related to the implementation of the two core humanitarian principles – humanity and impartiality – which embody the idea that humanitarian action should aim to prevent and alleviate human suffering and enable local communities without discrimination based on gender (as well as nationality, race, religious beliefs, class or political opinion). A similar observation was made when considering the need to include the birth date of Data Collectors/volunteers. Consequently, the two categories do not seem to be objectively necessary to attain the main purpose of the processing. Collecting data about volunteers’ gender and age seems to entail an excessive data collection as perhaps just knowing if a person is above a certain age limit would be suffice (e.g. a volunteer is 16 or older), even though National Societies are used to keeping a record of such data and often share it with other parties (e.g. IFRC member directory). Considering these remarks, NorCross made adjustments in the system, so the data collection on the application
includes age groups instead of birth dates and allows an option of not indicating gender. Additionally, the purpose of collecting data in order to identify region, district and village of a Data Collector concerns the need to map out the territory which is covered by volunteers in a particular country/region and not the exact location of his/her whereabouts.

Additionally, after considering the principles of data minimisation and purpose limitation, other improvements in Nyss were considered:

- Instead of including the preferred language in the data sets about Data Collectors, the preferred language is now set on a National Society basis. The preferred language set in the National Society is the default language for all users in the concerned National Society. Currently, Nyss settings support English and French.
- Collecting pseudonymous data about Data Collectors should suffice to confirm that a message comes from a registered a data collector. “Pseudonymisation” requires that the processing of personal data is done in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information (that would be stored locally by the National Society), provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. According to Recital 28, the application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data protection obligations. The use of “pseudonymisation”, however, does not preclude any other measures of data protection.
  - Justification: After considering this recommendation, it was decided to keep collecting names of Data Collectors/volunteers. This decision was based on two reasons. First, NorCross received feedback from National Societies where the first Nyss (and a previous CBS platform) pilot implementations took place. According to the feedback, it was suggested that having the name of volunteers is necessary for effective follow-up with Data Collectors from the Supervisor’s side. Supervisors have to call to cross-check Data Collector reports, and in some cases, they also need to do monitoring visits. Completing these tasks would be challenging without knowing who they are calling and visiting. It could also create challenges with retaining trust and motivation from the Data Collectors’ perspective. Furthermore, having names on the system reduces complexity of having to constantly refer to local databases of the National Society, which would include the name of the concerned person.
- National Societies are responsible for informing Data Collectors about the processing of their personal data. During their registration with the National Society, Data Collectors should be informed about their data subject rights – namely, the right to access, rectification and erasure of their data. Nyss includes by default settings on National Societies’ accounts that facilitate implementation of such rights. However, Head Managers have to ensure that the responsible personnel of the National Society they represent receive appropriate training.

6.4. Legal basis for the collection of personal data

As noted above, the controller has to ensure that personal data is being processed in a lawful way. For this purpose, the controller has to ensure that he selects one (or several) of the
appropriate grounds (also referred to as lawful bases for processing) that are set out in Article 6 of the GDPR. In principle, this means National Societies are free to determine the most appropriate legal ground for the processing of personal data.

For example, in case of Supervisors and Data Collectors the collection of personal data could be facilitated by the means of a contract. Consent could be also considered as a legal ground. However, it must be considered that in some cases Supervisors and Data Collectors may receive reimbursement for their efforts or may be employed by the National Society. Considering the possibility of the unequal balance of power between the controller (i.e. the National Society) and the data subject, it is not recommended to choose consent as a legal basis legitimising the processing of personal data. Consent of the data subject should be ‘freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’. 58

However, it must be noted that National Societies that are based outside the EU have to consider the legal framework applicable to them. In particular, they have to consider if there are national data protection laws that apply to them, and, if yes, what are the grounds under national law for processing personal data. The terms and conditions of the Nyss platform agreement clarify that in cases where there are no domestic data protection laws that apply, the National Society, when processing personal data in Nyss, should follow the requirements and principles of personal data protection described in Annex 1 of the agreement and in the IFRC’s Policy on the Protection of Personal Data. Additionally, it is important that National Societies’ representatives understand that having a legal ground for the processing of personal data is an essential aspect of the transparency principle. The controller has to communicate the legal ground of the processing (among other information) to data subjects before the processing starts.

National Societies should also consider a legal basis for processing personal data related to health of affected individuals in a highly pseudonymised format. In this particular case, they need to consider if national applicable laws provide for the possibility to process data that can include special categories of personal data.

In this respect, the Senegal Data Protection Act presents an insightful example. In Article 33 it stipulates that apart from consent the processing of personal data can be conducted if it is necessary for:

- the performance of a public interest or the exercise of official authority vested in the controller or the third party to whom the data are communicated; and
- safeguarding the interest or fundamental rights and freedoms of the data subject.

The GDPR provides similar legal bases for situations in which the processing of special categories of data could be envisioned:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition to process special categories of personal data may not be lifted by the data subject;

58 European Union Regulation (EU), 2016/679 GDPR, Article 4.11.
• processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
• processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
• processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
• processing relates to personal data which are manifestly made public by the data subject;
• processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
• processing is necessary for reasons of substantial public interest
• processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems
• processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices,
• processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

6.5. Purpose limitation

Besides defining the legal basis for processing personal data, it is also essential to define a specific purpose for the processing, which should also be notified to data subjects. Having a clearly defined purpose for the processing of personal data prevents further unintended processing of that data. To further process personal data (that is, process it for reasons that go beyond the original purpose for which data was collected), a controller would have to conduct a compatibility test (explained below). A simple change of privacy policy would not be sufficient to legitimise a new, incompatible data-processing purpose. In order to assess whether further processing is compatible with the initial purpose or not, entities should conduct a “compatibility test” that takes into account the following criteria:
a) the relationship between the purposes of the processing at the time of data collection and the purposes of further processing;
b) the context of the data processing (e.g., registration to Nyss) and the reasonable expectations of the individuals regarding further use of data (e.g., verification of text messages);
c) the sensitivity of the data and the impact on individuals’ privacy; and
d) the use of mitigating measures, such as adequate security and confidentiality measures ensuring fair processing and limiting the impact on individuals’ privacy. However, it should be noted that a new purpose is not necessarily incompatible with the original purpose. For example, further use of data for historical, statistical, or scientific purposes is generally compatible and would not raise major issues, provided that adequate security is in place (e.g., data minimisation, anonymisation, privacy-enhancing techniques).

7. Rights of data subjects

An identifiable natural person, who can be identified, directly or indirectly, 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 is a data subject within the meaning of the EU data protection framework. Every data subject is entitled to certain rights, which allow him or her to exercise control over his or her personal data. Data controllers are required to facilitate the implementation of these rights as this contributes to the attainment of the key objectives of data protection law and provides the effective and complete protection of the fundamental rights and freedoms of natural persons with respect to the processing of personal data. Data subjects’ rights, however, are not absolute and, therefore, can be restricted and the controller is allowed to take into account available technology and the cost of implementation when faced with a data subject’s request to exercise rights. This being said, it should be added that such restrictions are acceptable only in exceptional cases.

Within Nyss the envisioned data subjects include: Global Coordinator, Technical Advisors, (Head)-Managers, Supervisors, Data Collectors and potentially Data Consumers. When considering different rights of personnel and Data Collectors with respect to their data, it is important to consider the principle of transparency. Transparency is a well-established principle of the EU law and it is an overarching obligation under the GDPR applying to three central areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights. All rights of personnel and Data Collectors and other data subjects should be considered through the transparency prism.

It should be noted that considering the set-up of Nyss, NorCross and National Societies will be responsible for the implementation of rights of different data subjects.

<table>
<thead>
<tr>
<th>NorCross will facilitate data subject rights of the following users:</th>
<th>National Society will facilitate data subject rights of the following users:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Coordinator</td>
<td>Manager</td>
</tr>
<tr>
<td>System Administrator</td>
<td>Supervisor</td>
</tr>
<tr>
<td>Technical Advisor</td>
<td>Data Collector</td>
</tr>
<tr>
<td>Head Manager</td>
<td>Data Consumer</td>
</tr>
<tr>
<td></td>
<td>Affected community members</td>
</tr>
</tbody>
</table>

Regarding the implementation of data subjects rights of affected community members, it should be noted that while they should be provided with an information notice concerning the processing of their personal data by a Data Collector, in practice, implementing other data subject rights (e.g. rights to access, rectification and erasure) within the scope of Nyss will be nearly impossible as text reports include pseudonymised data that will be added to the platform’s aggregated health risk reports. Further information allowing to directly or indirectly identify affected community members will remain in logbooks of Data Collectors and such logbooks are not in possession of National Societies or NorCross.

---

7.1. The right to information

Controllers, at the time of collection of personal data, should provide individuals with a privacy notice (also referred as an information notice or a privacy policy). 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 the following information:60

- the name and contact details of the entity acting as controller;
- 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 lawful 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 a legal basis for the processing);
- the right to lodge a complaint with a supervisory authority;
- 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 if the personal data is collected from the individual it relates to); and
- the details of the existence of automated decision-making, including profiling (if applicable).

A privacy notice should be provided to Head Managers when obtaining their personal details by NorCross. National Societies should also provide privacy notices to data subjects, including data controllers. A privacy notice can be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. National Societies in most cases will be subject to less stringent requirements than foreseen the GDPR. National Societies are likely to be required to provide information points similar to the ones foreseen in Directive 95/46/EC, namely:

- 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.

7.2. The right of access

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;

---

the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

the right to lodge a complaint with a supervisory authority;

where the personal data are not collected from the data subject, any available information as to their source;

the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

This obligation requires that controllers accommodate access requests not only by reciting generic information already available in the privacy policy/notice/statement but also a tailored response to the data subject concerned, who wishes to know what exact information was collected for what purposes and under what lawful ground, for his/her particular situation. It is recommended that means of responding to access requests are envisioned at that time of setting up the processing operation. Provided that the response time should be limited to 30 days, it is recommended that such response to such requests is at least partially automated. Individuals after receiving a response to their request as well as a copy of their personal data collected by the controller, however, need to further interpret the information and consider if any further action is needed. In this way the right to access is an enabling right ‘on which other rights control rest.’

7.3. The right to rectification

The right to rectification: this right can be exercised without a prior request to access under Article 15 of the GDPR. Individuals whose data are subject to processing can at any point of that processing request the controller to rectify and correct incomplete or inaccurate information about them.

7.4. The right to erasure

Individuals whose data are being processed have a right to request the controller for the immediate erasure of their personal data. This request is subject to certain constrains and has to meet one of the conditions foreseen in Article 17.1. As pointed out earlier, data subjects’ rights are not absolute and there are circumstances under which requests for erasure could be limited. The following situations could trigger for the right to erasure:

• the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

• the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

• the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);


• the personal data have been unlawfully processed;
• the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
• the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

For the right to erasure to be fully executed properly (e.g., after the data subject withdraws consent or after the processing is no longer necessary), data controllers should in principle irretrievably remove all personal data from their system rather than merely anonymising it. Anonymisation is often considered a valid way to escape the applicability of the GDPR. For data controllers to reduce confusion over the terms of anonymisation and erasure the following must be considered. Recital 26 of the GDPR states that data protection rules should not apply to ‘anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.’ In its 2014 Opinion on anonymisation techniques, the A29WP also stressed that ‘anonymisation results from processing personal data in order to irreversibly prevent identification.’ This view has been integrated in the GDPR, which means that anonymisation of personal data entails making it irreversibly impossible to identify the data subject, having regard to all the means likely reasonably to be used. This test does not only depend on the relevant context and circumstances of each individual case and its outcome can also change over time. For a dataset to be truly anonymous, the data controller should have no means of distinguishing between anonymous and personal data in a mixed dataset, otherwise it must treat the entire set as personal data.

8. SMS gateway: SMSEagle63

There are numerous SMS gateway solutions that allow handling high-volume communication in various environments. The main advantages of SMS gateway solutions include 1) a very high network coverage and availability for which no smartphone, app or landline internet connection is required; 2) text messaging is considered to be secure and widely trusted and has high open rates in comparison with other messaging services, particularly for business communications; 3) allows simple integration into existing software. The use of SMS gateway solutions in humanitarian contexts is widely accepted as it allows to maintain communication with people in rural regions and less developed countries where comprehensive mobile internet coverage is not provided. Additionally, it allows for real-time information compared to paper-based systems.

The SMSEagle is a professional hardware SMS gateway for sending and receiving SMS messages. According to its developers, the device is designed with focus on reliability and stability. It has a Linux on-board, modern responsive web-interface, database backend, and built-in GSM/3G modem. SMS messages are sent/received directly to/from GSM network without using any external third-party solutions. The SMS Eagle has a built-in SQL database for secure storage of messages.64 The device has a range of built-in plugins that enable additional functionalities and easy integration with external applications.

---

63 SMSEagle is claimed to be GDPR compliant by the developers. See Appendixes I and II for additional information concerning compliance with the GDPR and the EU Radio Equipment Directive.
64 SQL stands for Structured Query Language. SQL is used to communicate with a database. According to ANSI (American National Standards Institute), it is the standard language for relational database management systems. SQL statements are used to perform tasks such as update data on a database, or retrieve data from a database. Some common relational database management systems that use SQL are: Oracle, Sybase, Microsoft SQL Server, Access, Ingres, etc.
In Nyss, text messages are sent by Data Collectors to the SMSEagle, where they are stored as raw data. National Society representatives (typically Head Managers) with physical access (or via a network) and with log in information, such as a username and a password, could read the raw data on the SMSEagle. The only visible personal identifier would be the phone number, from which the Data Collectors are reporting, and which in many cases is registered under the National Society’s name.

The reports in raw form are available on Nyss for certain users. The database in which the reports are stored are encrypted by Microsoft Azure’s Transparent Data Encryption scheme. In addition they are separated from the user data of the data collectors in the platform and only connected by a non-personal id. Upon deletion of the personal data, the reports would stay without a connection to an actual data-collector.

To activate the SMSEagle, several steps need to be taken, but essentially, the device has to be connected to the internet network using physical cables. By opening an internet browser on a computer connected to the same local network, one can configure the gateway by going to the IP address assigned to the gateway. It also needs to have a SIM card, which is usually registered to the manager, or some other responsible person from the National Society or an Emergency Response Unit running the project.

<table>
<thead>
<tr>
<th>Details about the data processed</th>
<th>Data categories</th>
<th>Justification of the need and relevance of the data</th>
<th>Minimisation controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone number</td>
<td>General; identifier</td>
<td>Needed to match a Data Collectors report to a Supervisor and its user data in the platform.</td>
<td>In many cases these phone numbers are not registered to the Data Collectors but to the National Society (or another entity) running the project.</td>
</tr>
<tr>
<td>Time</td>
<td>Indirect identifier</td>
<td>Allows to generate reports. Needed to follow temporal evolution of health risks/events.</td>
<td>N/A</td>
</tr>
<tr>
<td>Date</td>
<td>Indirect identifier</td>
<td>Allows to generate reports. Needed to follow temporal evolution of health risks/events.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

NorCross has no direct access to the SMSEagle, as this hardware is located in the country of the concerned National Society. The process of setting up the SMS Eagle can be facilitated by a web application requiring secure access. This web application is usually only reachable within the local network of the National Society. SMS Eagle runs rsyslog for log managing.

---

65 Based on the information shared during the call with NorCross.
Provided the burden of setting up the hardware by a National Society and requirements for physical security, NorCross is considering alternative options to facilitate the functionality of a SMS gateway or preconfiguring the SMSEagle before sending it to the concerned National Society.

9. SMS reports

9.1. Content sent by Data Collectors

The SMS report entails a 3, 5 or 8-digit code, which includes information of which health risk/event the report is about, gender, and age group (i.e. 0-4 years old or 5 years old and above). The location of the report is given by the (predefined) location the Data Collector is registered to. The location data about each Data Collector is entered by Supervisors and includes a zone, village, district and region. In addition, the GPS coordinates of a central point in the designated area that the Data Collector is responsible for, is registered. Thus, the location is not real time location of where the report is sent from. The timestamp attached to the message is generated by the mobile network provider. If more than one case of a health risk is expected per day, multiple cases of the same health risk/event can be reported in an aggregated report. The timestamp is then generated when the aggregated report is sent in and does not correspond to the actual time of collection of the data anymore.

While the messages are coded (pseudonymised), they essentially include data concerning health. This data does not concern the Data Collector, yet the affected individuals on whose behalf the processing is taking place. With available technical capabilities, the possibility of linking different data sets may allow to directly or indirectly to identify these individuals. In response to a correctly interpreted report, a feedback message is sent to the Data Collector. The content of this feedback message can vary from a recognition of receipt of the report to a provision of information to treat the reported health risk. The text of feedback messages is defined by National Society users. Once the report is uploaded to the platform, the feedback message is automatically generated. It is sent through the email application that is connected to SMSEagle in order to send a text message to the concerned Data Collector. As an alternative, NorCross started implementing a solution allowing a direct connection to the SMSEagle that does not require a separate Email inbox to send feedback messages or notifications of alert escalations.

9.2. Reporting on an affected community member

<table>
<thead>
<tr>
<th>Details about the data processed</th>
<th>Data categories</th>
<th>Justification of the need and relevance of the data</th>
<th>Minimisation controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health risk/Event</td>
<td>General; identifier</td>
<td>To meet the purpose of the system.</td>
<td>Pseudonymised. This number is only</td>
</tr>
</tbody>
</table>

67 Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

68 Technical capabilities would need to include physical access to the hardware of the mobile network provider. Incoming messages are stripped of any metadata, which could be used to trace a SMS report back to a location. While it is technically possible to exploit weaknesses in the infrastructure of mobile network providers to triangulate an approximate location of the data collector, it is only possible with considerable effort.
9.3. Aggregated reports on affected community members

<table>
<thead>
<tr>
<th>Details about the data processed</th>
<th>Data categories</th>
<th>Justification of the need and relevance of the data</th>
<th>Minimisation controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health risk/Event</td>
<td>General; identifier</td>
<td>To meet the purpose of the system.</td>
<td>Pseudonymised. This number, that is only matched to a specific Health Risk/Event in Nyss.</td>
</tr>
<tr>
<td>Number of male suspected cases below 5</td>
<td>General; identifier</td>
<td>To meet the purpose of the system.</td>
<td>Pseudonymised.</td>
</tr>
<tr>
<td>Number of male suspected cases above 4</td>
<td>General; identifier</td>
<td>To meet the purpose of the system.</td>
<td>Pseudonymised.</td>
</tr>
<tr>
<td>Number of female suspected cases below 5</td>
<td>General; identifier</td>
<td>To meet the purpose of the system.</td>
<td>Pseudonymised.</td>
</tr>
<tr>
<td>Number of female suspected cases above 4</td>
<td>General; identifier</td>
<td>To meet the purpose of the system.</td>
<td>Pseudonymised.</td>
</tr>
</tbody>
</table>

NorCross has explored measures to minimise the types and amount of data collected via text messages in order to prevent any potential de-anonymisation.

9.4. Content of data collection points

Data collection points are physical structures established in communities for data collection and community response. Such data collection points would be most often used during outbreaks.
to assist community response activities to the outbreak in addition to data collection. A common example is an oral rehydration point, where volunteers give oral rehydration solution to people suffering from diarrhoea. At the same, data on health risks is collected from individuals. Volunteers at these points can provide first response, which is sometimes enough for the affected individuals. In case individuals need further medical assistance, they are referred to a health facility. For Data Collection Points the report can also include information about the number of people “Referred to hospital”, “From other villages” or “Died” (but no other information about these people).

Data collection points registered in Nyss are registered with the name and the location of the point, without any personal information of the individuals volunteering within such a point.

<table>
<thead>
<tr>
<th>Details about the data processed</th>
<th>Data categories</th>
<th>Justification of the need and relevance of the data</th>
<th>Minimization controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health risk/Event</td>
<td>General; identifier</td>
<td>To meet the purpose of the system.</td>
<td>Pseudonymised. This a number, that is only matched to a specific Health Risk/Event in Nyss.</td>
</tr>
<tr>
<td>Number of <strong>male</strong> suspected cases <strong>below 5</strong></td>
<td>General; identifier</td>
<td>To meet the purpose of the system.</td>
<td>Pseudonymised.</td>
</tr>
<tr>
<td>Number of <strong>male</strong> suspected cases <strong>above 4</strong></td>
<td>General; identifier</td>
<td>To meet the purpose of the system.</td>
<td>Pseudonymised.</td>
</tr>
<tr>
<td>Number of <strong>female</strong> suspected cases <strong>below 5</strong></td>
<td>General; identifier</td>
<td>To meet the purpose of the system.</td>
<td>Pseudonymised.</td>
</tr>
<tr>
<td>Number of <strong>female</strong> suspected cases <strong>above 4</strong></td>
<td>General; identifier</td>
<td>To meet the purpose of the system.</td>
<td>Pseudonymised.</td>
</tr>
<tr>
<td>Number of cases referred to a health facility</td>
<td>General; identifier</td>
<td>Gives an overview of severity of outbreak. Severe cases need to be referred to health facility.</td>
<td>Pseudonymised.</td>
</tr>
<tr>
<td>Number of cases who died</td>
<td>General; identifier</td>
<td>Gives an overview of severity of outbreak.</td>
<td>Pseudonymised.</td>
</tr>
<tr>
<td>Number of cases that came from other villages</td>
<td>General; identifier</td>
<td>This gives guidance to if the data collection point is in the right place.</td>
<td>Pseudonymised.</td>
</tr>
</tbody>
</table>

**9.5. Metadata**

The CJEU observed in its judgements that metadata collected by communication providers allows ‘(1) to know the identity of the person with whom a subscriber or registered user has
communicated and by what means, (2) to identify the time of the communication as well as the place from which that communication took place and (3) to know the frequency of the communications of the subscriber or registered user with certain persons during a given period. Those data, taken as a whole, may provide very precise information on the private lives of the persons whose data are retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, activities carried out, social relationships and the social environments frequented.’ 69

Examples of metadata that could be obtained from a message include:

- IMEI/IMSI (device and SIM identifiers);
- sender phone number;
- recipient phone number;
- message size;
- location data;
- time data;
- IP addresses;
- hardware model;
- web browser information.

In a similar vein to the case law, the sensitivity of metadata has been demonstrated and discussed in academic circles. Joint research by MIT and the Université Catholique de Louvain even found that it only takes four (random) data points to de-anonymise 95% of users: ‘[T]o extract the complete location information for a single person from an “anonymised” dataset of more than a million people, all you would need to do is place him or her within a couple of hundred yards of a cell-phone transmitter, sometime over the course of an hour, four times in one year.’ 70

The importance of contextualising risks is well demonstrated by the case of a CBS implementation in Senegal. When considering the launch of the platform, the concerned National Society (in this case the Senegalese Red Cross Society), acting as the controller, recognised that there were concerns over whether the rights of mobile telephony subscribers in relation to their personal data were adequately guaranteed, in accordance with the Senegal Data Protection Law. 71 In particular, it has been reported that ‘illegal telephone monitoring is routinely undertaken by the security services.’ 72

It should also be noted that even though this metadata (except sender phone number, message size and time data) is at no point available in the platform, some security measures could be taken by the controller. For example, for generating reports on Nyss, sim cards could be mostly purchased by the National Society and registered under its name, thus not linking the phone number to the individual Data Collector in any mobile phone contract.

10. Nyss: reasoning for a cloud-based solution

At the time of writing, the web application part of Nyss is completely cloud based and hosted on Azure - a cloud computing service created by Microsoft. This platform provides flexibility for building and testing applications. It can also be easily scalable and provides reliable access to the service developed by NorCross across the globe.

69 See CJEU, C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others.
72 Ibid.
To be granted right to access and use the Azure platform and its services, an agreement was signed between NorCross and Microsoft. Upon signing this agreement – a subscription to the infrastructure – NorCross obtained a possibility to use the public cloud for Nyss.

This consequently means any data produced, collected and processed on Nyss, e.g. through the account of a National Society and actions of its users, are processed and stored in the Azure cloud.

Azure as a cloud computing service was chosen due to its ability to provide assurances that data, including personal data, in Nyss will be processed solely within the European data centres. Furthermore, Azure as well as all tools that are provided by this platform are claimed to be built with the highest standards of data protection, in particular the GDPR, in mind throughout its policies. Relying on such policy statements is reasonable as their accuracy following the accountability and documentation requirements (see above) can be contested by a data protection authority. By taking extensive security measures, Azure ensures compliance with GDPR and it regards itself as a data processor. For example, Azure ensures information security through the following built-in measures:

- Backup-as-a-service is offered; it is particularly useful in case of a data breach;
- Azure SQL is always updated with the very latest security features;
- Data ‘in transit’ and ‘at rest’ is encrypted by default; and
- Passwords are stored in a hashed form.

11. Recommendations

Following Article 35 of the GDPR, this DPIA report included:

(a) A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(c) an assessment of the risks to the rights and freedoms of data subjects; and
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

However, as indicated at the beginning of the assessment, the DPIA is an ongoing process, which needs to be updated either on a predefined regular basis, or in situations where the risks resulting from the processing operations change, or where the organisational or societal context for the processing activity has changed. A particular attention should be paid to an assessment of the likelihood and severity of risks to individuals whose personal data is being processed within Nyss.

It must be recognised, however, that NorCross has a limited capacity to address risks to the right and freedoms of users within Nyss, as National Societies are the controllers for most operations processing users’ personal data. However, some recommendations can be suggested for NorCross, both when the organisation is acting as a controller and a processor.

---

73 For example, Microsoft privacy policies concerning collection of user data were challenged EU regulators, see https://www.zdnet.com/article/microsoft-we-promise-youll-get-better-controls-over-how-we-use-your-data/
Recommendation 1

As a controller, it should ensure that throughout the lifecycle of Nyss, the processing of personal data processing is carried out in a lawful (i.e. have a legal basis for each phase of the processing of personal data), fair and transparent way in relation to data subjects. It should implement obligations foreseen in section 5.1.

Recommendation 2

As a controller, it should adhere to data quality principles, namely: the principles of purpose limitation, data minimisation, accuracy (i.e. data is 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 (i.e. data retention periods), integrity and confidentiality (security); and accountability (policies and documentation).

Recommendation 3

As a controller, it should ensure that when engaging in data sharing, disclosure, publication and or transfer practices, it provides sufficient safeguards to the concerned personal data.

Recommendation 4

Irrespective of its role, NorCross should be following the comprehensive compliance approach, which would take into account the GDPR requirements applicable to both controllers and processors. This approach would also be in line with a best-efforts obligation stemming from the moral framework applicable to humanitarian actors. While implementing this recommendation, NorCross team members should collaborate with the DPO when considering launching personal data processing operations.

Recommendation 5

NorCross should keep documentation of personal data processing operations related to Nyss. Such documentation could be maintained in the form of an inventory which would include information about the following:

- the name and contact details of the controller/representative/ DPO;
- the purpose/s of the processing;
- the categories of data subjects and personal data processed;
- the categories of recipients with whom the data may be shared;
- information regarding international data transfers;
- where possible, the applicable data retention periods; and
- where possible, a description of the security measures implemented in respect of the processed data.

It must be recognised that keeping track of retention periods in the current set-up of Nyss is particularly challenging because the storage duration (retention period) is coupled with the lifecycle of projects managed within the account of National Societies in the platform. The duration of a project is, therefore, decided by the National Societies. When the National Society running the project decides that the project is finished, it is advised to close the project. This deletes the personal data stored in the project’s page (i.e. anonymises any connections of reports.
etc. to user data and deletes the user-data). This is of course exempt of a data subject requesting to have their data deleted earlier.

Recommendation 6

As provider of an account for National Societies, NorCross should foresee a clear and transparent allocation of responsibilities in the Nyss platform agreement provided to the representatives of National Societies at the time of creating the account.

Recommendation 7

As provider of an account for National Societies, NorCross should ensure that contracting National Societies share a clear understanding of their respective tasks and rights set in the Nyss platform agreement.

Recommendation 8

As a provider of an account for National Societies, NorCross should develop training materials that would facilitate implementation of user functions foreseen in Nyss. The training materials should also address best practices concerning personal data processing (e.g. the need to protect password of user accounts; the importance of ensuring confidentiality of data in logbooks; and possible risks involved in data sharing with third parties).

Recommendation 9

As provider of an account for National Societies, NorCross should ensure the possibility to follow up and obtain feedback from contracting National Societies concerning the user interface (i.e. the website) and arrangements concerning the processing of personal data.

Recommendation 10

As provider of an account for National Societies, NorCross should encourage and offer support for National Societies that want to provide access to Nyss to third parties to carry out an assessment of potential privacy, data protection and security risks.
Appendix I — SMSEagle GDPR Compliance Report

This report was obtained through an email request to SMSEagle.
Introduction
This document addresses compliance of software that runs on SMSEagle devices with General Data Protection Regulation (GDPR) [1]. The General Data Protection Regulation (GDPR) is the new European regulation on personal data protection that goes into effect on 25 May 2018. The new regulation harmonizes privacy laws in the European Union and aims to protect EU residents’ personal information. The regulation reshapes the way organizations approach data privacy and guides them to build GDPR-compliant software. GDPR expands on previous European Union data laws.

Basic Definitions [1]
Controller - means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Personal Data - means any information relating to an identified or identifiable natural person (‘Data Subject’); an identifiable natural person is one 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.

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;

Personal Data Scope in SMSEagle Device
Personal data processed in the SMSEagle device by the Controller are in the following scope:
- Name (and Surname if Controller decides to process it)
- Telephone Number
- Session Cookie (IP address)

GPDR requirements and their application in SMSEagle device
Below summary presents substantial requirements of GDPR and their application in SMSEagle device.
<table>
<thead>
<tr>
<th>GDPR requirement</th>
<th>Requirement Explanation</th>
<th>How the requirement is fulfilled in SMSEagle device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 25</td>
<td>“Privacy by default” and “Privacy by design” means that privacy is taken care of at every stage of the product’s lifecycle and personal data stored in application is limited to minimum.</td>
<td>SMSEagle software is developed with best engineering knowledge and modern software development standards. Data privacy is taken into account during development process.</td>
</tr>
<tr>
<td>Article 32</td>
<td>Implementation of reasonable data protection measures to protect personal data and privacy against loss or exposure</td>
<td>SMSEagle devices use pseudonymization in database structures, access to application is password protected, strong encryption algorithms are used to store passwords. Software is regularly tested and under process of continual improvement.</td>
</tr>
<tr>
<td>Article 13</td>
<td>Controller is responsible for receiving a data subject a consent to the processing of his or her personal data before entering the data in SMSEagle application.</td>
<td>-</td>
</tr>
<tr>
<td>Article 21</td>
<td>Controller is responsible for stopping any data processing as soon as a data subject requests this.</td>
<td>-</td>
</tr>
<tr>
<td>Article 15</td>
<td>Controller must provide data subject with a copy of their personal information free of charge upon request.</td>
<td>Copy of personal information (stored SMS messages) can be obtained via webGUI &gt; Reporting module &gt; Export to PDF or CSV format</td>
</tr>
</tbody>
</table>
| Article 17        | If a data subject choose to withdraw their consent to use their personal information, a Controller must delete their data. | Personal data can be erased via:  
  a) User information webGU > Users (search a user) > Delete  
  b) Phonebook contacts webGU > Phonebook > (search contact) > Delete  
  c) SMS messages webGU > Search > Advanced Search > (mark displayed messages) > Delete |
### Article 20
The right to data portability.

Data subject may require to transfer their data. This must happen in machine-readable format.

Copy of personal information (stored SMS messages) can be obtained via webGUI > Reporting module. Data can be exported to PDF or CSV file format.

### Article 19
The right to restrict Processing

Data subject have the right to ask you not to process their data. In this case, their records can remain in place, but Controller can’t use them.

To restrict processing of stored data we suggest either to mark data with [RESTRICTED] note in data content. This can be achieved:
- a) User information
  - webGUI > Users (search a user) > Edit
- b) Phonebook contacts
  - webGUI > Phonebook > (search contact) > Edit

### Article 16
The right to correct information

If personal data is out of date, incomplete, or incorrect, data subject can request that Controller must update it.

Personal data can be corrected via:
- a) User information
  - webGUI > Users (search a user) > Edit
- b) Phonebook contacts
  - webGUI > Phonebook > (search contact) > Edit

---

References:

Appendix II — Conformity with EU Radio Equipment Directive

EC DECLARATION OF CONFORMITY

We, PROXIMUS Radosław Janowski, ul. Piątkowska 163, 60-650 Poznań, Poland (manufacturer) declare under our sole responsibility that the following product:

<table>
<thead>
<tr>
<th>Product</th>
<th>Hardware SMS Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brand</td>
<td>SMSEagle</td>
</tr>
<tr>
<td>Model/Type</td>
<td>NXS-9700-3G Rev.3</td>
</tr>
</tbody>
</table>

is in conformity with the relevant Community harmonisation:

European Directive 2014/53/UE (RED)

The following harmonised standards and/or other normative documents has been applied:

<table>
<thead>
<tr>
<th>Radio Spectrum</th>
<th>ETSI EN 301 511 V12.5.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ETSI EN 301 908-1 V11.1.1</td>
</tr>
<tr>
<td></td>
<td>ETSI EN 301 908-2 V11.1.1</td>
</tr>
<tr>
<td>EMC</td>
<td>ETSI EN 301 489-1 V2.1.1</td>
</tr>
<tr>
<td></td>
<td>ETSI EN 301 489-7 V1.3.1</td>
</tr>
<tr>
<td></td>
<td>ETSI EN 301 489-52 V1.1.0</td>
</tr>
<tr>
<td>RF Safety</td>
<td>EN 62311:2008</td>
</tr>
</tbody>
</table>

The conformity assessment on the radio equipment listed above has been carried out in accordance with Annex III (module B) of RADIO Equipment Directive 2014/53/EU with the involvement of the following Notified Body:

Czech Metrology Institute, TESTCOM - Certifying Body for Certification of Products No. 3136 Hvodzanská 3, 148 00 Praha 4, Czech Republic, accredited by CAI according to EN ISO/IEC 17065:2013.

EU-Type Examination Certificate No. 0120-CC-V0021-18

Poznań, 19.11.2018

[Signature]

Radosław Janowski, CEO & Owner