16 July 2020

Nyss - DATA PROTECTION IMPACT ASSESSMENT REPORT
## Acknowledgements

**Version 1.0:**

*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.*

*The contract under which this DPIA was conducted, was part of a joined effort by the Belgium Red Cross and the Norwegian Red Cross, with financial support by the Belgium government.*
## Contents

1. Introduction .................................................................................................................. 6  
   1.1. Quick summary ........................................................................................................ 6  
   1.2. Nyss and the CBS project ...................................................................................... 8  
   1.3. Applicability of GDPR to Norway ......................................................................... 8  
2. Methodology ................................................................................................................ 9  
   2.1. Humanitarian setting .............................................................................................. 10  
3. DPIA threshold analysis ............................................................................................. 11  
   3.1. Processing on a large scale .................................................................................... 12  
   3.2. Vulnerable data subjects ...................................................................................... 12  
4. Processing of data in CBS with Nyss ........................................................................ 14  
   4.1. Data flows in a single organization project .......................................................... 14  
   4.2. Data flows in a project with multiple organizations .............................................. 15  
   4.3. Nyss: A cloud-based solution ............................................................................... 15  
      4.3.1. GDPR/Security of Microsoft Azure ................................................................. 16  
   4.4. Data flows from Nyss to external users via SMS/Email ........................................ 17  
      4.4.1. Data flow for SMS feedback messages via Email ........................................ 17  
      4.4.2. Data flow for SMS feedback messages via Azure IOT Hub ......................... 18  
      4.4.3. Data flow for sent emails .............................................................................. 19  
      4.4.4. Notifications upon escalation of alerts ......................................................... 20  
   4.5. Processing of community reports ........................................................................ 21  
      4.5.1. Reports sent by Data Collectors/Data Collection Points ............................. 21  
      4.5.2. Reporting on an affected community member (3-digit code) .................. 21  
      4.5.3. Aggregated reports on affected community members (5-digit code) .... 22  
      4.5.4. Content of data collection points (8-digit code) ............................................. 23  
      4.5.5. Visibility of data of reports to different Nyss users .................................... 24  
      4.5.6. Metadata ........................................................................................................ 25  
      4.5.7. SMS gateway: SMSEagle ............................................................................. 26  
4.6. Alerts ...................................................................................................................... 28  
4.7. Dashboards / Visualization ..................................................................................... 28  
4.8. Data Collector pages .............................................................................................. 29  
4.9. Exporting data ....................................................................................................... 31  
   4.9.1. Reports ............................................................................................................. 31  
   4.9.2. Data Collectors/collection points .................................................................... 31  
   4.9.3. Generating PDFs of the dashboard .................................................................. 32  
4.10. Users with and without access to Nyss ................................................................. 33  
   4.10.1. Risk assessment and collected personal data ................................................. 35  
   4.10.2. Data Collectors personal data ...................................................................... 37  
   4.10.3. Controller/Processor role of different users .................................................. 39  
5. The role of the Norwegian Red Cross (hosting organization) .................................. 42  
   5.1. NorCross’ obligations as a controller .................................................................. 43  
   5.2. NorCross’ obligations as a processor .................................................................. 46  
   5.3. Legal basis for processing of personal data ....................................................... 47  
6. The role of implementing organizations .................................................................... 49  
   6.1. Considering joint controllership ......................................................................... 49  
   6.2. Legal basis for the collection of personal data ................................................... 50  
   6.3. Purpose limitation ............................................................................................... 51  
7. Rights of data subjects .............................................................................................. 53
7.1. The right to information ........................................................................................................ 54
7.2. The right of access .................................................................................................................. 54
7.3. The right to rectification ........................................................................................................ 55
7.4. The right to erasure ............................................................................................................... 55

8. Recommendations ................................................................................................................... 57
8.1. Changes made during conducting the DPIA ......................................................................... 59

Appendix I — SMSEagle GDPR Compliance Report ................................................................. 61
Appendix II — Conformity with EU Radio Equipment Directive ................................................. 65
### Glossary

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBS</td>
<td>Community Based Surveillance</td>
</tr>
<tr>
<td>DC</td>
<td>Data Collector</td>
</tr>
<tr>
<td>DCP</td>
<td>Data Collection Point</td>
</tr>
<tr>
<td>EDPB</td>
<td>European Data Protection Board</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>Hosting organization</td>
<td>The organization hosting Nyss. At the time of writing this is only NorCross.</td>
</tr>
<tr>
<td>ICRC</td>
<td>International Committee of the Red Cross</td>
</tr>
<tr>
<td>IFRC</td>
<td>International Federation of Red Cross and Red Crescent Societies</td>
</tr>
<tr>
<td>Implementing organization</td>
<td>The organization implementing CBS. An in-country organization, that is provided access to Nyss through a Head Manager or Coordinator user.</td>
</tr>
<tr>
<td>NorCross</td>
<td>Norwegian Red Cross</td>
</tr>
<tr>
<td>NS</td>
<td>National Society</td>
</tr>
<tr>
<td>VUB</td>
<td>Vrije Universiteit Brussel</td>
</tr>
<tr>
<td>WP29</td>
<td>Article 29 Working Party</td>
</tr>
</tbody>
</table>
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 a data protection impact assessment (DPIA). The Norwegian Red Cross (NorCross) commissioned a DPIA in order to gain a better understanding of the data processing operations and associated risks within Nyss - a real time community-based surveillance (CBS1) system that NorCross develops.2 The DPIA was conducted during the Nyss development and testing phase and continues to be adapted throughout the lifetime of Nyss.

We use this assessment to find if Nyss is compatible with the EU data protection framework, in particular the General Data Protection Regulation 2016/679 and if necessary, adapt Nyss.

1.1. Quick summary

We start with an analysis to find if we are legally obliged to conduct a DPIA (chapter 3). Within its function as a controller for some of the processing, the arguments made in chapter 3.1 and 3.2 can be taken as an obligation to conduct a DPIA for at least some of the processing. Conducting a DPIA for all processing operations could also be seen as being part of a best effort obligation within the humanitarian sector.

We conclude that it is necessary in some cases and useful in other to conduct a DPIA and include all processing operation within Nyss as part of a best effort obligation.

Analysing the various processing operations (chapter 4), we find that the hosting organization (e.g. NorCross) and implementing organizations (e.g. National Societies) fill different roles in terms of data protection, depending on the processing operation (chapters 5 and 6). In particular, for part of processing operations the hosting organization acts as a controller and for the other part it acts as as processor. Provided this legal set-up, it has to follow different GDPR requirements according to the role it plays in each processing activity.

We also find 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 not necessarily as a controller, but as the developer of the Nyss platform (chapter 5). It defines such default settings available for implementing organizations at the platform development stage in order to ensure early warning and response to health risks/events in local communities.

---


2 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.
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 as the hosting organization (chapter 5.3) and any implementing organizations (chapter 6.2), e.g. National Societies.

Lastly the rights of data subjects are discussed (chapter 7) and some recommendations moving forward are made (chapter 8).
1.2. Nyss and the CBS project

Within the scope of the CBS project, NorCross launched a CBS system called Nyss, that includes a cloud-based web-platform for data collection, analytics, visualisation, generation of automatic alerts and data sharing.

The main objective of CBS systems is to complement health authorities’ efforts in detecting health risks/events by filling information gaps in existing public health systems to enable early warning and response. More specifically, while information gathered by health authorities is mainly based on information collected by healthcare facilities when treating patients, CBS allows 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).

CBS systems’ capability to attain their primary objectives rely on data provided by Data Collectors – in this project, volunteers registered with implementing organizations such as National Societies – living and working directly with the affected communities, who are also consulted before launching a CBS project in their community.

The Nyss platform is the result of multiple years of collaborative efforts of the Norwegian Red Cross and other organizations involved in CBS. Over the course of this time NorCross has worked at least with the following organizations:

- Vrije Universiteit Brussel (VUB) - Research Group on Law, Science, Technology & Society (LSTS)
- Belgian Red Cross
- Somali Red Crescent society
- Senegalese Red Cross society
- IFRC
- Clave Consulting AS
- Volunteer IT experts
- DoLittle
- Itera
- Microsoft Norway
- Bekk Consulting

1.3. Applicability of GDPR to Norway

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.
2. Methodology

The process of a DPIA is a derivative of a 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 assessment made in this report builds on the systematic analysis made in guidance documents published by the Article 29 Working Party (WP29), 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).

Building on the experience of previous DPIA processes conducted by the VUB and recommendations put forward by the EDPB, this DPIA includes the following steps:

- Threshold analysis – determining whether personal data processing activities require an impact assessment;
- Description of the envisioned processing – e.g. identification, characterisation and description of applications processing personal data in the Nyss;
- Assessment of the necessity and proportionality;
- Measures already taken;
- Assessment of the risks to the rights and freedoms;
- Measures envisioned to address risks;
- Documentation; and

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 DPIA 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:

---

1. 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.
3. With the entry into force of the General Data Protection Regulation WP29 was replaced by the European Data Protection Board (EDPB).
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 organizational 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.

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.\textsuperscript{8}

\textbf{2.1. Humanitarian setting}

This report also takes into consideration specific suggestions made by the IFRC and the ICRC data protection frameworks. The two frameworks were developed with humanitarian principles and the needs of humanitarian workers in mind. 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\textsuperscript{9} and offer ways to mitigate them.

Within this DPIA we take into consideration the specific context of humanitarian action. In this regard, concerns about physical security of affected individuals should be anticipated and be addressed. It is also worth noting, that despite the positive impact humanitarian action brings - such as restored health, skills learned and improved gender relations - the humanitarian sector may also create risks and ethical tensions.


\textsuperscript{9} 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.
3. DPIA threshold analysis

Article 35 of the GDPR requires controllers\textsuperscript{10} 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'.\textsuperscript{11} Other parties than controllers concerned with the processing operations within a particular project or initiative do not have an obvious 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 (chapters 5 and 6), NorCross is responsible only for a limited set of processing operations concerning the creation of accounts implementing organizations. 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 implementing organizations 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 organization 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 organizations to further the trust relationship between NorCross (the platform developer/hoster) and the platform’s users (e.g. National Societies).

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 DPIA 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:

\begin{itemize}
  \item [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;
  \item [b)] processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences; or
  \item [c)] a systematic monitoring of a publicly accessible area on a large scale.
\end{itemize}

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,\textsuperscript{12} as well as 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.

The text messages sent by Data Collectors (that often include volunteers) will essentially report health risks/events concerning public health and will include personal data of local community

\textsuperscript{10} The person or entity that ’determines the purposes and means of the processing of personal data’ (art. 4 GDPR)
\textsuperscript{11} The threshold analysis is included in the following sections.
\textsuperscript{12} Norwegian Red Cross, ‘Functional Requirements: Community Based Surveillance’; Norwegian Red Cross.
members concerning their health in a pseudonymised form (chapter 4.5).\textsuperscript{13} 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 (chapter 3.1).

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. Conducting a DPIA and adopting a risk-based approach can also be considered to be best practice in humanitarian action embraced by numerous humanitarian organizations and data protection experts.\textsuperscript{14} 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.\textsuperscript{15}

### 3.1. Processing on a large scale

The GDPR does not define what constitutes processing on a large scale. According to recital 91,\textsuperscript{16} 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:\textsuperscript{17}

- 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 implementing organizations such as National Societies. There is neither a limitation 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.\textsuperscript{18}

### 3.2. Vulnerable data subjects

\textsuperscript{13} 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.

\textsuperscript{14} Christopher Kuner and Massimo Marelli, ‘Handbook on Data Protection in Humanitarian Action’ 164.


\textsuperscript{16} Please note, recitals are not legally binding, yet are used to interpret the binding provisions.


\textsuperscript{18} 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.
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 implementing organizations 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 implementing organization) can cause vulnerability for data protection purposes, if such individuals would be disadvantaged in case the processing of personal data is not performed.\(^{19}\)

---

4. Processing of data in CBS with Nyss

4.1. Data flows in a single organization project

Figure 1 shows roughly the flow of data from communities through Nyss to health actors and back to the communities. Data Collectors send in reports on health risks/events using SMS (1) via an SMS gateway (2) to a cloud-based web application (3). The web application (the Nyss platform) stores, analyses and visualizes the collected data. Users registered by the implementing organization (e.g. National Society) can access the web application (4).

The Supervisor would then cross-check the reports by calling the Data Collector. This is done outside the scope of Nyss. While in some cases a Manager user of the implementing organization escalates the alert, usually it is the Supervisor. This triggers a notification to alert escalation notification recipients (5) in the form of an Email or SMS (data flows are described in chapters 4.4.1, 4.4.2, 4.4.3). More details on the users in chapter 4.10.

The escalation notification is the end of the data flow in Nyss. Usually the recipients would contact the implementing organization and assemble some kind of help towards the community.

---

20 A good overview of the Nyss platform with its data flows is also presented in the following short video: https://www.youtube.com/watch?v=784izOlkzJE

21 Access to the data is protected by different user roles that the implementing organizations can use. These are tailored see only the minimum amount of data they need to fulfil their function within Nyss (chapter 4.10).
Nyss allows multiple implementing organizations to share data in a pseudonymized form in a Nyss project. In these projects we make sure, that only pseudonymized data is shared between organizations (chapter 4.2).

4.2. Data flows in a project with multiple organizations

Figure 2: Data flow of reports about community members for a multiple organizations project. All parts except for the Nyss servers would usually reside within the country. All user facing parts separate the data by organization. Thus, no personal data is visible across organizations.

Figure 2 shows the data flow in a Nyss project with multiple organizations. The flow of data is quite similar to the one described for a single organization project (chapter 4.1).

In the way it is shown in Figure 2, the raw report, timestamp of report and phone number would all pass the same SMS gateway which could present a risk. On the other hand, there is no name or other personal data on the SMS gateway connected to this data. In addition, its possible to have several SMS gateways per implementing organization within Nyss. Thus, if a higher level of data protection is necessary, the implementing organizations could each use their own gateway, while still share pseudonymized data within Nyss.

Users in the web interface of Nyss are registered with their respective organization. They only see the personal data of Data Collectors of their own organization and thus can only cross-check reports of Data Collectors who are part of their organization.

In addition, recipients are separated by organization.

4.3. Nyss: A cloud-based solution

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 is also easily scalable and provides reliable access to the service developed by NorCross across the globe.
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 in Nyss, e.g. through the account of an implementing organizations and actions of its users, are processed and stored on Azure cloud servers.

This has the advantage that implementing organizations such as National Societies, don’t have to setup hardware infrastructure to start using Nyss. Local technical resources can be a major hurdle in CBS implementations and solutions must be available quickly especially in an emergency.

On the other hand, we also realize that many implementing organizations need to have more control over the data or are even bound to have the data hosted within their country. Since the complete codebase is open source, implementing organizations can choose to host Nyss on their own servers, thereby becoming the hosting organization themselves. In these cases, NorCross is only the developer of the codebase and thus not responsible for any collected or stored data.

4.3.1. GDPR/Security of Microsoft Azure

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 European data centres. Furthermore, Azure as well as all tools that are provided are acclaimed 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.

---

22 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/
4.4. **Data flows from Nyss to external users via SMS/Email**

Feedback messages (SMSe back to e.g. Data Collectors) are mostly used to give direct feedback to Data Collectors, if the report they sent in was interpreted correctly and give guidance on how to proceed. For the Data Collectors it is convenient if the feedback message comes from the same number as the one, they sent their report to, since that way it is easier to match which feedback message belongs to which sent report. In addition, in this way it is easy to manage the costs through the implementing organization, who just has to make sure that the SIM card they use in the SMSEagle has enough credit.

On the other hand, that means the SMSEagle somehow has to be reached from the Nyss platform, to tell it to send out an SMS message. This is difficult because reaching the SMSEagle from the outside could result in security risks. In addition, we don’t know beforehand if the network the SMSEagle is connected to, is protected by a firewall.

We currently support two different methods of reaching the SMSEagle and sending out SMSe.

**4.4.1. Data flow for SMS feedback messages via Email**

![Diagram](Figure 3: SMS feedback messages are retrieved from an Email inbox by the SMSEagle.)

In this variant, the SMSEagle polls an Email inbox every five second. If there are unread Emails with a specific format (phone number in subject and raw message in body), the SMSEagle sends out a SMS with the subject of the email as the receiving number and the body of the Email as the SMS.

This solution uses out of the box technology of the SMSEagle. In addition, it is independent of Azure specific cloud resources and thus more portable for usage in other environments. The disadvantage is, that the feedback messages travers the servers of SendGrid and the mailbox.

An Email sent in this way would include a phone number and a customizable feedback message. The message usually represents some sort of advice on the health risk/event that Data Collectors previously reported on.

Since it is hard to deduct more personal data from nothing but a phone number and oftentimes the phone numbers are registered to an implementing organization (e.g. a National Society) instead of the actual name of the Data Collector, this can be considered pseudonymized data.

---

4.4.2. **Data flow for SMS feedback messages via Azure IOT Hub**

In this variant the SMSEagle opens a direct connection to an Azure cloud resource called Azure IOT Hub, using the MQTT protocol. All device connection is secured using TLS/SSL\(^26\). A port that is usually open even in firewalled networks is used.

SMS feedback messages don’t traverse any third-party services between the Nyss cloud resources and the SMSEagle.

From a data protection point of view this is preferable.

On the other hand, this does not come out of the box with the SMSEagles, but instead needs additional configuration and a running service\(^27\). This increases the complexity which can also increase security risks. Besides that, this depends on Azure specific cloud resources and is thereby less portable.

Data sent from Nyss to the SMSEagle includes a phone number and a feedback message, that is customizable but represents some sort of advice on the health risk that Data Collectors previously reported on.

Since it is hard to deduct more personal data from nothing but a phone number and oftentimes the phone numbers are registered to an implementing organization (National Society) instead of the actual name of the Data Collector, this can be considered pseudonymized data.

---


4.4.3. Data flow for sent emails

In addition to sending out messages via SMS, Nyss also sends out messages via Email. This includes notifications upon alert escalations, registration emails, reset password emails and notifications to head managers if an alert has no cross-checked reports 24 hours after it has been triggered.

Emails are sent out via an API call to the SendGrid servers, who offer SMTP servers as a service. SendGrids policy on GDPR is described here: https://sendgrid.com/resource/general-data-protection-regulation-2/.

Recipients of registration emails, reset password emails and notifications to head managers are all users within Nyss. The type of processed data is described in the following table. The notification sent out upon an escalation of an alert is described in more detail in chapter 4.4.4.

<table>
<thead>
<tr>
<th>Email type</th>
<th>Justification</th>
<th>Recipients</th>
<th>Data in Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration emails</td>
<td>To greet new users and send them a link with which they can verify their user and set their password.</td>
<td>New users in Nyss</td>
<td>Chosen name of user, user role in Nyss, Email address of user, verification token to be able to set password</td>
</tr>
<tr>
<td>Reset password emails</td>
<td>To make it possible for users to reset their password</td>
<td>Existing users in Nyss</td>
<td>Chosen name of user, Email address, verification token to be able to set new password</td>
</tr>
<tr>
<td>Notifications to head managers</td>
<td>It sometimes happens that alerts are open in Nyss, but they are not being taken care of. This mechanism ensures that someone is</td>
<td>Head Managers in Nyss.</td>
<td>Health risk/event of the alert, village of the report that triggered the alert, time since it was triggered (currently 24 hours), name of supervisors/organizations28 with reports in the alert.</td>
</tr>
<tr>
<td>when an alert has not been handled</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

28 In a project with multiple organizations, Supervisors of different organizations might have reports within one alert. 24 hours after the report was initially triggered the Head Managers of all organizations are notified. Since the names of the Supervisors should not be shared to other organizations, the name of the Supervisor is replaced by the name of the organization in the notification Email.
4.4.4. Notifications upon escalation of alerts

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 implementing organization), Nyss triggers an alert. If the reports in the alert are cross-checked by any of the connected Supervisors to match the community case definition of the report, the Supervisor can escalate the report. This automatically triggers an Email or SMS notification to all Email addresses and phone numbers that the implementing organization has put as a recipient to Supervisors that are connected to that alert.

The alert recipients are solely set by the implementing organization. The following information is included in the Email/SMS:

1. The health risk/event on which the alert was triggered.
2. The name of the Nyss project in which the alert was triggered.
3. The region, district and village from which the last report came.

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 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 Organization.

While NorCross can anticipate that an alert may be shared widely, it is the implementing organization that remains ultimately responsible for its sharing with Data Consumers and other third parties.
4.5. Processing of community reports

Community reports are SMS sent in by Data Collectors to the Nyss platform. They contain the information about other community members. These reports are the basis of the data in Nyss that potentially leads to an early warning and response.

4.5.1. Reports sent by Data Collectors/Data Collection Points

The SMS report consists of a 3, 5 or 8-digit code, which Nyss interprets in the following way:

- 3-digit code: a health risk/event, sex, age group (below 5 or above 4 years)
- 5-digit code: a health risk/event, number of male cases below 5 years, number of male cases above 4 years, number of female cases below 5 years, number of female cases above 4 years
- 8-digit code: the first 5 digits are the same as the 5-digit code, number of referred people to the hospital, number of people coming from other villages, number of people that have died

The report is matched to a Data Collector (DC)/Data Collection Point (DCP) registered in Nyss, using the sender number of the report. The geographical location of the report in Nyss, is the location the matched DC/DCP was initially registered to.

The timestamp on the message is created on the SMSEagle. The last time the message was updated in the SMSEagles database is taken, which is usually when the message was received.

If more than one case of a health risk/event is expected per day (outbreak mode), multiple cases of the same health risk/event can be reported in an aggregated report (5- and 8-digit codes). The timestamp is generated when the aggregated report is sent in and oftentimes 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.

4.5.2. Reporting on an affected community member (3-digit code)

These reports are collected by Data Collectors within their communities. Data Collector check out different community members or are alerted by other community members. Most of the respective personal data stays within the community, except for the data described in the following table. The metadata on the SMS is analysed in chapter 4.5.6.

---

29 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 organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

30 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 its 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.
## Details about the data processed

<table>
<thead>
<tr>
<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>To meet the purpose of the system.</td>
<td>Pseudonymised. This number is only matched to a specific Health Risk/Event in Nyss.</td>
</tr>
<tr>
<td>Sex</td>
<td>Indicator to see that no sex is excluded from the system.</td>
<td>Pseudonymised</td>
</tr>
<tr>
<td>Age group (below 5 or above 4 years)</td>
<td>Indicator of risk for several health risks, indicator to see that no age groups are excluded from the system.</td>
<td>Pseudonymised. There are only two age groups in this case: below 5 and above 4 years.</td>
</tr>
</tbody>
</table>

### 4.5.3. Aggregated reports on affected community members (5-digit code)

Aggregated reports are used in case there is an ongoing outbreak, and data collectors have a lot to report. The data is then even more pseudonymized, since the timestamp usually does not correspond to the time of collection. The metadata on the SMS is analysed in chapter 4.5.6.

<table>
<thead>
<tr>
<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>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 male suspected cases below 5</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>To meet the purpose of the system.</td>
<td>Pseudonymised.</td>
</tr>
</tbody>
</table>
### 4.5.4. Content of data collection points (8-digit code)

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 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>
<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>
4.5.5. **Visibility of data of reports to different Nyss users**

After the reports are sent to Nyss, they are analysed (for the alerts) and visualized (for the dashboards) in different ways. To increase the data protection measures for the community members and Data Collectors, only a limited number of users can actually see the personal data of the Data Collectors in combination with the reports, which is the only link to the community members.

<table>
<thead>
<tr>
<th></th>
<th>Sender number</th>
<th>Exact Timestamp</th>
<th>Date</th>
<th>Data Collector name/phone number</th>
<th>Location (Region, District, Village, Zone)</th>
<th>Village coordinates</th>
<th>Health risk/event</th>
<th>Age group of report</th>
<th>Sex of report</th>
<th>Is training report?</th>
<th>Status in alert</th>
<th>Error report?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Coordinator</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Coordinator</td>
<td>x</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Head Manager</td>
<td>✓*</td>
<td>✓**</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
</tr>
<tr>
<td>Manager</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
</tr>
<tr>
<td>Technical Advisor</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
<td>✓*</td>
</tr>
<tr>
<td>Data Consumer</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Supervisor</td>
<td>✓</td>
<td>✓</td>
<td>✓**</td>
<td>✓**</td>
<td>✓**</td>
<td>✓**</td>
<td>✓**</td>
<td>✓**</td>
<td>✓**</td>
<td>✓**</td>
<td>✓**</td>
<td>✓**</td>
</tr>
<tr>
<td>SMSEagle</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

* Of their own organization.
** Only of the Data Collectors assigned to the Supervisor.

The table above shows the visibility of individual data on reports sent about community members to different users within the platform and also the data that is visible on the SMSEagle.

Only users of the implementing organization can see all the accessible data of a report. In particular only those users (Head Manager, Manager, Technical Advisor, Supervisor) can make the connection between a report and the Data Collector who sent it in (marked in light blue in the table).

Users outside of the implementing organization can see the dashboards (chapter 4.7). The dashboard does not actually show particular reports but aggregates them into charts and maps.

Even for users of the implementing organization, its only possible to identify a community member indirectly from this data. In particular they would need to gather additional information outside of the scope of Nyss.
For users of Nyss outside of the implementing organization, it’s even more difficult, since they do not see the personal information of Data Collectors, who are the only ones that are actually in direct contact with the community members.

In case of multiple organizations wanting to share data within a Nyss project, every Data Collector is connected to an organization. While there can be Data Collectors of Organization A and Organization B within one project, no user of Organization B could see any personal information of Data Collectors of Organization A in Nyss.

### 4.5.6. 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.’  

However, it must be mentioned that the CJEU is talking about electronic communication, e.g. messaging someone else on a phone, while the communication between Data Collectors and affected community members happens external to any technological means, i.e. the Data Collector visits (or is visited by) community members physically. The full text can be found e.g. at paragraph 26 in the respective text.

A study by the ICRC and Privacy international found the following on metadata that communication providers might have:

- 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.

“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,

---

31 See CJEU, C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others.
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.\textsuperscript{33,34}

However, it must be mentioned that the source quoted in footnote 33 test something quite specific: How well can an \textit{existing} set of locations be matched with another \textit{existing} set of location data that could be extracted from a mobile provider (Figure 2\textsuperscript{35}).

Under those conditions one would have to have access to the data of the network providers to be able to actually locate the Data Collectors. What is stated is that basically if you have locations of many users from somewhere, one can match them to the data of network providers with few datapoints (4 with 95% accuracy).

In the CBS scenario, someone would have to gain access to the complete mobile network dataset (minus the personal data of each datapoint) and have a huge set of location data for users from somewhere else. On the other hand, if one does have access to the datasets of the mobile network provider, they would likely also have access to any personal data the provider stores. Then of course the location profile match is trivial, since it’s the same dataset.

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 adequality guaranteed, in accordance with the Senegal Data Protection Law.\textsuperscript{36} In particular, it has been reported that ‘illegal telephone monitoring is routinely undertaken by the security services.’\textsuperscript{37}

4.5.7. \textbf{SMS gateway: SMSEagle}\textsuperscript{38}

The SMS gateway provides a way to get the content of an SMS from a mobile network provider to the cloud services upon which Nyss is hosted (Figure 1). The SMSEagle offers basic functionality and is readily available. In addition, it has been tested in multiple implementations.

Reports sent to the SMSEagle are stored as raw data. Staff of the implementing organizations 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 name of the implementing organization.

The SMSEagle automatically forwards the messages to the Nyss platform, however, they are stripped of almost all metadata mentioned in chapter 4.5.6. The only information on the SMS

---

\textsuperscript{33} https://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data
\textsuperscript{34} Privacy International, “Doing no Harm” in the Digital Era, p. 60, cross-ref. 63.
\textsuperscript{35} https://www.nature.com/articles/srep01376
\textsuperscript{37} Ibid.
\textsuperscript{38} 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. See www.smseagle.eu for more information on the device.
that is sent to Nyss is the content of the message, the sender number and the timestamp when
the message reached the SMSEagle. Only within Nyss are these reports matched to the
personal data of a Data Collector (name, village for which the data collector is responsible).
The following related technical data is stored in Nyss well: incoming/outgoing message id,
modemNumber (in case there are two modems in the SMSEagle), apikey (to authenticate the
SMSEagle), source (does the message come from the SMSEagle or was it added through Nyss).

The cloud database in which the reports are stored in Nyss are encrypted by Microsoft Azure’s
Transparent Data Encryption scheme.\(^{39}\) 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.

<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/sender number</td>
<td>General; identifier</td>
<td>Needed to match a Data Collectors report to a Data Collector 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 implementing organization 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 implementing organization. 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 implementing organization.

In addition, cloud-based alternatives were considered, which would alleviate the burden of
having to set up local hardware and contracts with mobile network providers. However, to keep
costs low, local phone numbers are needed in the contexts in which CBS is implemented. Local
phone numbers for cloud-based messaging services are usually not available in such contexts.
Using such services, would also pose other data protection questions, since the data would
then traverse other third-party servers.

---

4.5.7.1. Why SMS?

We use SMS technology, because it has shown to be the most easily accessible and reliable in very rural regions. Feature phones last for many days on one battery charge, which is particularly useful in areas where no electricity is available and network coverage is best for 2G. Exposure of rural communities to smartphone technology is usually low and thus feature phones can provide better access.

While being somewhat less secure than more up to date technologies, we currently see the risk of not being able to reach the communities that we actually want to reach - thereby defeating the purpose of CBS with Nyss - as too high, if we switch to other technologies.

In comparison to paper-based implementations, using SMS to cloud technology provides much faster access to the collected data and thereby a much faster response.

4.5.7.2. SMSEagle with multiple organizations

While within Nyss the reports are matched with a Data Collector through the phone number, who is matched to a Supervisor and the report thereby to an organization, on an SMSEagle that is used by multiple organizations, the data is not strictly separated.

On the other hand, the SMSEagle does not hold the name of data collectors or the location and thereby they mixed data on the device cannot easily be matched to personal data. Thus, it’s not possible without additional information, to match the data on the SMSEagle with a person. We regard the data therefore as pseudonymized.

The ownership of the data on the SMSEagle would be with the implementing organization or the one holding the Coordinator role.

Nyss allows for the possibility to use several SMSEagles for one country. In this way organizations can in principle choose to use separate SMSEagles to have an increased separation of their data.

4.6. Alerts

The alert functionality automatically analyses the incoming reports about community members, and triggers an additional notification, if an alert rule (number of reports of a health risk/event within a given timeframe within a given area) is met.

The algorithm that decides to trigger an alert or not acts purely on the number of reports, within a given timeframe and area. It does not differentiate between the sex or age within one report. A triggered alert automatically notifies Supervisors who are responsible for data collectors that have sent in reports. The Supervisors cross-check with their respective data collectors by calling them (outside of Nyss).

If the alert turns out to be valid, Supervisors can manually notify (=escalate to) external recipients who get a message that holds no personal data of involved community members or data collectors.

4.7. Dashboards / Visualization

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 (= implementing organization) 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/country\(^{41}\). The shown aggregated information includes the following visualisations:

- bar chart showing the number of reported health risks/events by location\(^{42}\)
- bar chart showing the number of reported health risks/events by village
- bar chart showing the number of reports by health risk/event
- a table showing the number of reported health risks/event by sex and age
- a map that shows the number of reported health risks/events by registered location of the Data Collector on a map
- bar chart showing the number of reports of “referred to hospital”, “from other villages”, “died” by date of all locations selected within the filters

The shown data is pseudonymized, 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 time interval, location, health risk/event, data collection type\(^{43}\) and organization (only Coordinators can filter for all organization, other users can only filter for their own or all).

While Global Coordinators only have access to the National Society dashboard, users that are part of an implementing organization have access to the project dashboard. Data Consumers have access to project dashboards but are added as users only by the implementing organization. More information on the different types of user roles in Nyss can be read in chapter 4.10.

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.

### 4.8. Data Collector pages

Registered Data Collectors are visible in the platform. Their personal data is editable, and they can be deleted. This is necessary, since Data Collectors should be able to request to their Supervisors or other representatives of the implementing organization, to be deleted, rectified or to know what data is saved about them.

On the other hand, this personal data of the Data Collectors should be protected. We do this by assigning a Supervisor to each Data Collector. Each Supervisor can only see his/her Data Collectors. Managers, Technical Advisors and Head Managers can see all Data Collectors. E.g.

\(^{41}\) Data/users can be separated into different projects within an implementing organization.

\(^{42}\) The location, the respective Data Collector was initially registered to, not the real time location of where the report was sent from.

\(^{43}\) Can be used to separate reports from Data Collectors and Data Collection Points.
if a Data Collector needs to be switched to a different Supervisor, a Manager would need to do it.

One thing that is specific, is that Data Collectors are community members that receive only a light training. This means that it easily happens, that it is necessary to retrain them on how to report. Supervisors need to be able to figure out where a retraining might be necessary and for whom.

We show a map with an icon for each Data Collector (Figure 5). Based upon a configurable time span, we show a green icon (reported correctly within the time frame), a yellow icon (no reports about health risks/events but sent activity reports) and a red icon (sent error reports). Apart from showing the different states within the chosen timeframe, the data is not further analysed.

In addition, we show a list of all Data Collectors, that shows if a Data Collector has sent reports about health risks/events (green), only activity reports (yellow) or error reports (red) for every week of the last 8 weeks.
In both cases, the identified use case is to be able to identify where Data Collectors might need retraining, so the CBS implementation can fulfil its main purpose of receiving information in real time and triggering a warning upon it.

It should also be stated that Nyss does not in any way automatically decide anything about these Data Collectors. The map and the table purely make data available that could e.g. also be seen through checking through the project report list.

4.9. Exporting data

4.9.1. Reports

Nyss enables certain users to export the report lists. This was necessary because users need to use the data for reporting to their organizations in different ways than could be identified. The following data fields are included in such an export:

timestamp of report, status (success, error), data collectors name, data collectors phone number, region, district, village, zone, health risk/event, sex, age group, GPS location of village, raw message, epi year, epi week.

The personal data of affected community members is the registered health risk/event, the sex, the age group and the village location. Since this data is visible within the platform to the users that export it, we don’t see additional risk by allowing it to be exported. An in-depth discussion of the different data fields included in reports can be found in chapter 4.5.

4.9.2. Data Collectors/collection points

Nyss enables certain users to export the list of Data Collectors. Implementing organizations sometimes want to analyse their volunteers in ways which we cannot foresee. Instead of trying to cover all use cases within Nyss, and thereby perhaps making analysis tools implicitly available in some contexts that may not be appropriate, we opted to make it possible to export the data. However, since there is a lot of personal data in this export, we opted to make it only available to Managers, who are usually staff of the implementing organizations.

If it is really necessary to export the Data Collectors name/phone number as well is under current investigation (2020).
The included data is data collectors name, data collectors phone number, additional phone number, sex, birth-group (10 year intervals), region, district, village, zone, GPS location of village, supervisor, training status.

Since all this data is visible to users that may export it within the platform already, we don’t see additional risk by allowing them to export it.

4.9.3. **Generating PDFs of the dashboard**

Another export functionality, which is available to Supervisors and Managers, is generating a PDF from the project dashboard. This function basically takes a screenshot from the dashboard and creates a downloadable PDF from it.

The data shown on the dashboards is pseudonymized and we don’t see an additional risk in making it possible to save it as PDF.
4.10. **Users with and without access to Nyss**

Figure 7 shows the different kind of user roles within a single organization project in Nyss (plus alert escalation notification recipients and community members, since they also have data within Nyss). Users 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 pre-defined within the platform that cannot be altered. The user roles are based on a hierarchy of responsibilities.

![Diagram of user roles in Nyss](image)

*Figure 7: Different users (plus community members) within a single organization project in Nyss as a hierarchy of responsibilities. The Coordinator user is only needed if multiple organizations want to share data within Nyss. While Head Managers are different from Managers and Technical Advisors in some respects, they are mostly the same and could also be directly responsible for Supervisors.*

Each hierarchy level is only responsible for the one directly below them. The visibility of personal data across hierarchy levels is quite limited, e.g. a Global Coordinator cannot see any personal data of a Supervisor or create one. On the other hand, Head Managers, Managers and Technical Advisors can see all users below them\(^{45}\), as they are responsible for the CBS implementation from the point of view of the implementing organization.

In a project with multiple organizations (Figure 8), each organization has its own users below the Head Manager. Users are not visible or editable across organizations. E.g. Managers of organization A cannot see or alter Supervisors of organization B in any way.

\(^{45}\) Since community members don’t have any personal data within Nyss, no one can see any directly in Nyss.
This 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.

The table below shows the functionalities (responsibilities) of each user role in more detail.

<table>
<thead>
<tr>
<th>User</th>
<th>Functionalities</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Administrator</td>
<td>Creates Global Coordinators’ accounts.</td>
</tr>
<tr>
<td></td>
<td>Can see all users within all organizations registered in the platform, including Data Collectors. Only used for support/maintenance tasks upon the request of organizations.</td>
</tr>
<tr>
<td>Global Coordinator</td>
<td>Creates Head Managers/Coordinators as the first user within a new implementing organizations profile.</td>
</tr>
<tr>
<td></td>
<td>Can see personal data of the Head Managers and Coordinators and pseudonymized dashboard aggregated across the whole country.</td>
</tr>
<tr>
<td>Coordinator</td>
<td>Creates a Head Manager and organization for each organization that wants to participate in a multiple organization project. The Coordinator also coordinates relevant settings across multiple organizations. They only see Head Managers for each organization and pseudonymized dashboard data.</td>
</tr>
<tr>
<td></td>
<td>They sign an agreement with the hosting organization and with each of the implementing organizations within their project.</td>
</tr>
<tr>
<td>Head Manager</td>
<td>The Head Manager signs an agreement on data protection on behalf of their organization either with the hosting organization (in a single organization project) or with the Coordinators organization (in a multiple organization project).</td>
</tr>
<tr>
<td></td>
<td>They are the seed user for the other users within an implementing organization in Nyss.</td>
</tr>
</tbody>
</table>
Visibility of personal details of users is quite limited. The table below shows which users are visible to which other users.

<table>
<thead>
<tr>
<th>Manager / Technical Advisor</th>
<th>Global Coordinator</th>
<th>Coordinator</th>
<th>Head Manager</th>
<th>Manager</th>
<th>Technical Advisor</th>
<th>Data Consumer</th>
<th>Supervisor</th>
<th>Data Collector</th>
<th>Alert Escalation Notification Recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

* Only of the users own organization.

4.10.1. **Risk assessment and collected 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).  

<table>
<thead>
<tr>
<th>User</th>
<th>Collected personal data</th>
<th>Risk assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>System administrator</td>
<td>None. This is a generic login that resides with NorCross or another party that hosts Nyss.</td>
<td>This user is not tied to any personal data.</td>
</tr>
<tr>
<td>Global Coordinator</td>
<td>Name, Email, organization (optional), phone number, additional phone number (optional). The processing of this data would be done within the scope of duties assigned by the employer (e.g. in the engagement contract).</td>
<td>The collected personal data does not include special categories of personal data (e.g. health related data) and therefore its processing entails a <strong>low risk</strong> if disclosed accidentally or if accessed by an unauthorised party.</td>
</tr>
<tr>
<td>Coordinator</td>
<td>Name, Email, organization, phone number, additional phone number (optional). The processing of this data would be done within the scope of the duties carried out at an implementing organization.</td>
<td>The collected personal data does not include special categories of personal data (e.g. health related data) and therefore its processing entails a <strong>low risk</strong> if disclosed accidentally or if accessed by an unauthorised party.</td>
</tr>
<tr>
<td>Head Manager / Manager / Technical Advisor</td>
<td>Name, Email, phone number, additional phone number (optional), organization, institution (optional). The processing of this data would be done within the scope of the duties carried out at an implementing organization.</td>
<td>The collected personal data does not include special categories of personal data (e.g. health related data) and therefore its processing entails a <strong>low risk</strong> if disclosed accidentally or if accessed by an unauthorised party.</td>
</tr>
<tr>
<td>Data Consumer</td>
<td>Name, Email, phone number, additional phone number (optional), institution. The processing of this data is done upon a request from a third party to the implementing organization, to gain access to some of the data within Nyss.</td>
<td>Such personal data does not include special categories of personal data (e.g. health related data) and therefore its processing entails a <strong>low risk</strong> if disclosed accidentally or if accessed by an unauthorised party.</td>
</tr>
<tr>
<td>Supervisor</td>
<td>Name, Email, phone number, additional phone number (optional), organization, institution, birth group (10-year intervals), sex (male, female, other). In addition, the non-personal data of the assigned project and alert recipients is stored. The processing of this data would be done within the scope of the implementing organizations’ arrangement for their work with local volunteers</td>
<td>The processing of such personal data entails a <strong>moderate risk</strong> if disclosed accidentally or if accessed by an unauthorised party.</td>
</tr>
<tr>
<td>Data Collector</td>
<td>Name, display name, sex, birthyear group, phone number, additional phone number (optional), GPS coordinates of central location in the area of responsibility, region, district, village, zone (optional), supervisor. The processing of this data would be done within the scope of the implementing organizations’ arrangement for their work with Data Collector that will be signed at the time of the training.</td>
<td>The processing of such personal data entails a <strong>moderate risk</strong> if disclosed accidentally or if accessed by an unauthorised party. The processed data is discussed in more detail in chapter 4.10.2.</td>
</tr>
</tbody>
</table>

46 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.
While name and phone number of the data collection point are collected, these do not refer to a human being, but instead to a facility like location (e.g. an oral rehydration point). We do not consider this personal data.

The processing of such data entails a **low risk** if disclosed accidentally or if accessed by an unauthorised party.

**Data Collection Point**

<table>
<thead>
<tr>
<th>Community members</th>
<th>Health risk/event, sex (male, female), age group (below 5 or above 4 years).</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sometimes the number of people referred to a hospital, coming from other villages and died are collected in aggregated reports.</td>
</tr>
<tr>
<td></td>
<td>Nyss attaches this data to a village and a central GPS location within this location.</td>
</tr>
<tr>
<td></td>
<td>Nyss only holds the connection to the personal data of the Data Collector and not to the personal data of the community members.</td>
</tr>
</tbody>
</table>

Since usually Data Collectors are responsible for many community members, it is not easily possible to connect this data back to the actual community members (except in edge cases such as a village with only one male below 5 years who is reported). Thus, we consider this data to be pseudonymized.

The processing of such data entails a **high risk** if disclosed accidentally or if accessed by an unauthorised party, if it can be linked back to the actual community members.

While the reports in itself are visible to multiple users within Nyss, the link to the Data Collectors is only visible to staff and volunteers of the implementing organization. Supervisors can only see those reports of those Data Collectors for whom they are directly responsible. The processed data is discussed in more detail in chapter 4.5.

**Alert escalation notification recipient**

| Role, organization, email, phone number, project organization. |
| The processing of this data is done upon a request from a third party to the implementing organization, to gain access to some of the data within Nyss. |

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.

4.10.2. **Data Collectors personal data**

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 implementing organizations. Data Collectors can be registered in the system by representatives of the implementing organization (National Society or a deploying organization such as the 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 and match it to a responsible Supervisor for further follow up.

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>
</table>

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 implementing organizations. Data Collectors can be registered in the system by representatives of the implementing organization (National Society or a deploying organization such as the 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 and match it to a responsible Supervisor for further follow up.

The table below explains what types of data are collected from Data Collectors and why.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>General; identifier</th>
<th>Description</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>General; identifier</td>
<td>Having the name 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 implementing organization, which would include the name of the concerned person.</td>
<td></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 to other Supervisors. A Data Collector can select any name; it can be a pseudonym.</td>
<td></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. 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>
<td></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. By allowing “other” as a choice, we provide Data Collectors with an option to refrain from revealing their sex.</td>
<td></td>
</tr>
<tr>
<td>Location</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 match reports from neighbouring Data Collectors. Static location of a central location of the village the Data Collector is responsible for. Neither the location of the Data Collectors house nor of the community members.</td>
<td></td>
</tr>
<tr>
<td>Phone number</td>
<td>General; identifier</td>
<td>To verify that a message comes from a registered Data Collector. Follow up of the Supervisor with the Data Collector. In many cases the phones used by the Data Collectors are bought by and registered to the implementing organization.</td>
<td></td>
</tr>
</tbody>
</table>
### Region

<table>
<thead>
<tr>
<th>Region</th>
<th>General; identifier</th>
<th>Necessary to filter reports by region.</th>
<th>No connection to coordinates.</th>
</tr>
</thead>
</table>

### District

<table>
<thead>
<tr>
<th>District</th>
<th>General; identifier</th>
<th>Necessary to filter reports by district.</th>
<th>No connection to coordinates.</th>
</tr>
</thead>
</table>

### Village

<table>
<thead>
<tr>
<th>Village</th>
<th>General; identifier</th>
<th>Necessary to filter reports by district.</th>
<th>No connection to coordinates.</th>
</tr>
</thead>
</table>

### Zone (optional)

<table>
<thead>
<tr>
<th>Zone (optional)</th>
<th>General; identifier</th>
<th>Necessary to filter reports by zone.</th>
<th>No connection to coordinates.</th>
</tr>
</thead>
</table>

### Additional phone numbers (optional)

| Additional phone numbers (optional) | General; identifier | In some cases, Data Collectors use more than one phone, or they switch phones. | No connection to coordinates. |

---

### 4.10.3. Controller/Processor role of different users

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/Coordinator’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 organizations) 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>Yes (towards the Head Manager/Coor dinator)</td>
<td>Yes (representing the processor organization)</td>
<td>Yes</td>
<td>The Global Coordinator is a representative of NorCross managing the Nyss platform. The Global Coordinator creates the profile for implementing organizations and the Head Manager of an implementing organization, in a single organization project.</td>
</tr>
<tr>
<td>Coordinator</td>
<td>Yes (towards Head Managers)</td>
<td>No</td>
<td>Yes</td>
<td>The Coordinator is a representative of a local or international organization, that manages the different organization involved in a project with multiple organizations. The Coordinator (on behalf of his/her organization) enters into an agreement with the hosting organization (currently NorCross). The Coordinator adds</td>
</tr>
<tr>
<td>Role</td>
<td>Access</td>
<td>Available</td>
<td>Processing</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------</td>
<td>-----------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Head Manager</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>The Head Manager (on behalf of the implementing organization) enters into an agreement with the hosting organization (currently 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 implementing organization, whose data will be processed by the hosting organization.</td>
</tr>
<tr>
<td>Technical Advisor</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>The Technical Advisor can be a representative of NorCross or another party, but not within the concerned implementing organization. Implementing organizations can create this user to invite an external party to support them in their CBS implementation. This could e.g. be delegates. These users can fulfill the same functions as a Manager user. They are specifically only added by the implementing organization. Their data is processed by the hosting organization, on behalf of the implementing organization.</td>
</tr>
<tr>
<td>Supervisors</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Persons that are staff of, volunteers or otherwise associated with an implementing organization. Their personal data is added by a Manager, Head Manager or Technical Advisor.</td>
</tr>
<tr>
<td>Data Collectors</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Community members (in some cases receiving compensation and reimbursements) associated with the implementing organization, who receive training to identify health risks/events in local communities. In the sense that their own personal data is processed within Nyss, they are data subjects.</td>
</tr>
<tr>
<td>Alert escalation</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Representatives of external authorities that receive a notification when an alert is escalated. They are added solely by the implementing organization.</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 organization 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>
</tbody>
</table>

Head Managers for each organization and therefore becomes a controller towards them. As a representative s/he then enters into an agreement with each Head Manager representing their organization.
<table>
<thead>
<tr>
<th>notification recipients</th>
<th>Yes</th>
<th>Data Consumers act as “third parties” who, under the direct authority of the implementing organization, are authorised to access Nyss and see pseudonymized data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Consumers</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Affected community members</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Affected community members are the ones whose personal data is going to be processed in the pseudonymised and sometimes aggregated form via SMS.</td>
</tr>
</tbody>
</table>
5. The role of the Norwegian Red Cross (hosting organization)

Within the scope of Nyss, NorCross can have different users. In particular, it can act as Global Coordinator (GC) and as a System Administrator (SA). These two user roles result in separate processing activities. When it acts as GC, NorCross is considered to be a controller in relation to the processing of personal data of Head Managers or Coordinators. On the other hand, for the processing activities concerning the role of SA 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).

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 implementing organizations), is also the “developer” of the system itself. As developer, it defines the functional requirements of the system and implements them. 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.47

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 aims to take into account the GDPR requirements applicable to both controllers and processors. This approach is also 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 the so-called “Brussels effect”.48 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.\textsuperscript{49}

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.\textsuperscript{50}

Following the current set up of Nyss, NorCross acts as a controller for the part concerning the collection and processing of Head Managers’/Coordinators’, including their contact details. The GDPR provides the following definition:

\begin{quote}
‘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)).
\end{quote}

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 implementing organizations 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 implementing organizations 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 chapter 7 on the rights of data subjects. Personal data of members of implementing organizations, e.g. Supervisors, Data Collectors and Managers, would be outside the scope of

\textsuperscript{49} See the Gap Analysis of Senegalese Data Protection and the GDPR.

\textsuperscript{50} European Union Regulation (EU), 2016/679 GDPR, Article 5.1.
this obligation, as only users within the implementing organization have access to such data and not NorCross as the hosting organization.

Responsibility for the processing (accountability): according to Article 24 of the GDPR, the controller is responsible for implementing appropriate technical and organizational 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 heavy fines. It should be noted, however, that the two principles, reinforce the core data protection principles and data subjects’ rights.

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. The controller (and the processor) can chose whether to keep such records in paper or in an electronic form. It is assumed that organizations 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.

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.


53 Based on the opinions and guidance provided by the UK DPA (ICO), the French DPA (CNIL) and the Irish DPA.
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.

The documentation should 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.

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:
- processing personal data of specified implementing organizations users (i.e. Head Managers and Coordinators) and their contact details concerning their official capacity for the purposes of setting up a profile for implementing organizations in the platform and maintaining contact with individuals handling this profile 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 organizational (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 organizational 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 organizational 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 implementing organizations.

Typically, controllers appoint processors to process the personal data on their behalf through contractual means and, therefore, processors are regarded as the secondary actors.\(^5\) This restrictive dichotomy imposed by law as noted by different scholars and practitioners is difficult to apply in practice.\(^6\) In the case of Nyss, NorCross acts as a processor for certain personal data operations. Its role as a processor will be clarified within the scope of the contractual agreement with an implementing organization. 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.\(^7\)

<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 categories of personal data processed on behalf of the controller;</td>
</tr>
<tr>
<td>• information regarding international data transfers;</td>
</tr>
<tr>
<td>• where possible, a description of the security measures implemented in respect of the processed data.</td>
</tr>
</tbody>
</table>

**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.

**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 implementing organizations, 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 implementing organizations 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 of personal data**

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 s/he selects one (or several) of the

---


\(^6\) Ibid.

\(^7\) For more detailed description of the documentation obligation, see the section on controller’s obligations.
appropriate grounds (also referred to 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 implementing organizations, given that by providing access to Nyss, implementing organizations can report and get an overview of particular health risks/events and NorCross can implement the mandate assigned to it.
6. The role of implementing organizations

After a careful mapping of data flows within Nyss, it can be said that implementing organizations 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, an implementing organization becomes the controller for part of Nyss, over which it has de facto direct influence. The responsible personnel of each implementing organization 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 implementing organization in this case would include information about personnel working for (e.g. Managers) or associated with the implementing organization (e.g. Supervisors and Data Collectors) as well as personal data of Data Consumers.

Provided this factual influence, it is deemed that implementing organizations would act as controllers within Nyss. Their obligations as controllers are also explained in the Nyss platform agreement, which needs to be agreed to by the first user of an organizations profile (Coordinator or Head Manager) at the first login.

6.1. Considering 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 implementing organizations. 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 implementing organizations 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. Thus the ‘factual influence’ of the processing operations remains separate on the domestic/regional and global level.

6.2. 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 implementing organizations 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 implementing organization. Considering the possibility of the unequal balance of power between the controller (e.g. 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 means any ‘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’.  

However, it must be noted that implementing organizations 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 implementing organization, 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 implementing organizations’ 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.

Implementing organizations 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

---

58 European Union Regulation (EU), 2016/679 GDPR, Article 4.11.
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;
- 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.

6.3. 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 natural person, that 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/her to exercise control over his/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 Coordinators, Coordinators, Technical Advisors, (Head)-Managers, Supervisors, Data Collectors, Data Consumers, alert escalation notification recipients and affected community members. 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 (hosting organization) and implementing organizations will be responsible for the implementation of rights of different data subjects.

<table>
<thead>
<tr>
<th>NorCross (hosting organization) will facilitate data subject rights of the following users:</th>
<th>Implementing organization will facilitate data subject rights of the following users:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Coordinator</td>
<td>Manager</td>
</tr>
<tr>
<td>Coordinator</td>
<td>Technical Advisor</td>
</tr>
<tr>
<td>System Administrator</td>
<td>Supervisor</td>
</tr>
<tr>
<td>Head Manager</td>
<td>Data Collector</td>
</tr>
<tr>
<td></td>
<td>Data Consumer</td>
</tr>
<tr>
<td></td>
<td>Affected community members</td>
</tr>
<tr>
<td></td>
<td>Alert escalation notification recipients</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 implementing or hosting organizations.

7.1. **The right to information**

Controllers, at the time of collection of personal data, should provide individuals with a privacy notice (also referred to 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:

- 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 organizations (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/Coordinators when obtaining their personal details by the hosting organization (NorCross). Implementing organizations 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. Implementing organizations in most cases will be subject to less stringent requirements than foreseen in the GDPR. Implementing organizations 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. 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 organizational 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 organization is acting as a controller and a processor.

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 implementing organization 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.

8.1. Changes made during conducting the DPIA

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 implementing organizations 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 an implementing organization basis. The preferred language set in the implementing organization is the default language for all users in
the concerned implementing organization. Currently, Nyss settings support English and French.

• Collecting pseudonymous data about Data Collectors should suffice to confirm that a message comes from a registered 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 implementing organization), 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.

  o 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 implementing organizations 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 implementing organization, which would include the name of the concerned person.

• Implementing organizations are responsible for informing Data Collectors about the processing of their personal data. During their registration with the implementing organization, 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 implementing organizations’ accounts that facilitate implementation of such rights. However, Head Managers have to ensure that the responsible personnel of the implementing organization they represent receive appropriate training.
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 from 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 SNS messages) can be obtained via webGUI &gt; Reporting module &gt; Export to PDF or CSV format</td>
</tr>
<tr>
<td>Article 17</td>
<td>If a data subject choose to withdraw their consent to use their personal information, a Controller must delete their data.</td>
<td>Personal data can be erased via: a) User information webGUI &gt; Users (search a user) &gt; Delete b) Phonebook contacts webGUI &gt; Phonebook &gt; (search contact) &gt; Delete c) SMS messages webGUI &gt; Search &gt; Advanced Search &gt; [mark displayed messages] &gt; Delete</td>
</tr>
</tbody>
</table>
### 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 Hvostanska 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

Radosław Janowski, CEO & Owner