The Netherlands Red Cross

510


# Data & Digital Responsibility Policy

## Going beyond privacy

Version 3.3

## Introduction

Data and digital technology offer tremendous potential to increase the speed, quality and cost effectiveness of humanitarian aid. Assessing the benefit of data-driven solutions versus their potential harm in a humanitarian context requires awareness of potential risks involved in applying data and digital technology. Humanitarian actors should take advantage of the opportunities provided by (open or closed) data, and they should do so responsibly. The collection and processing of any kind of data may negatively impact vulnerable individuals or communities – despite the good intentions.

When collecting and utilising personal data, the EU General Data Protection Regulation (GDPR) imposes vital obligations upon organisations in terms of data protection. Data and digital responsibility go beyond compliance with the GDPR however and also consider the potential to do harm through use What does it mean to be accountable? of non-personal data and digital technology.

510 defines data and digital responsibility as:

> "***The responsible processing of data and use of digital technologies with respect to privacy, ethical standards and humanitarian principles, bearing in mind potential consequences and taking pro-active measures to avoid harming individuals or communities***".

The figure below shows how we go beyond the protection of personal data. We leverage the Red Cross Red Crescent's (RCRC) global presence to access local knowledge, which then is applied to inform our work. Finally, we apply a range of ethical standards and principles, including our own Movement Principles as well as the humanitarian "do no harm" principle.

## Purpose of the policy

This policy provides procedures for the 510 staff, students and volunteers to follow, to ensure that all our data and digital solutions are designed and applied responsibly, i.e., without causing harm to anyone. The increasing complexity of data and digital solutions and the seemingly endless applications do not lend themselves to a ***prescriptive*** framework that instructs the user what can and what cannot be done. Instead, like the GDPR, in this policy we opt for an ***interpretative*** framework of principles that shall be applied in all stages of our work, from design to operation.

## Our principles

The following 5 principles each emphasize vital considerations concerning the responsible use of data and digital technology:

1. **Human centred**

   We involve the human perspective in all steps of the problem-solving process. Through co-design sessions and interviews with users, we start by distilling a clear, unambiguous *purpose statement* for the data and digital solutions we provide.

2. **Do no harm**

   We make every effort to do-no-harm to individuals or communities through the data or digital products that we make.

   - We assess the local and humanitarian context through a Political, Economic, Social and Technological, Legal and Environmental (PESTLE) analysis. We identify data and technology related risks and incorporate mitigation measures into our designs.
   - We provide in solutions that are proportional to the problem they solve, especially when they process personal or sensitive data.
   - We actively apply data minimisation.
   - We ensure that the users are fully aware of the strengths and weaknesses and have the skills and knowledge needed to use them correctly.

3. **Transparency**

   We document and make our products, research and data publicly available where possible. We provide clarity on how our solutions function and perform. We are transparent about what data we process and how we process this data.

4. **Accountability**

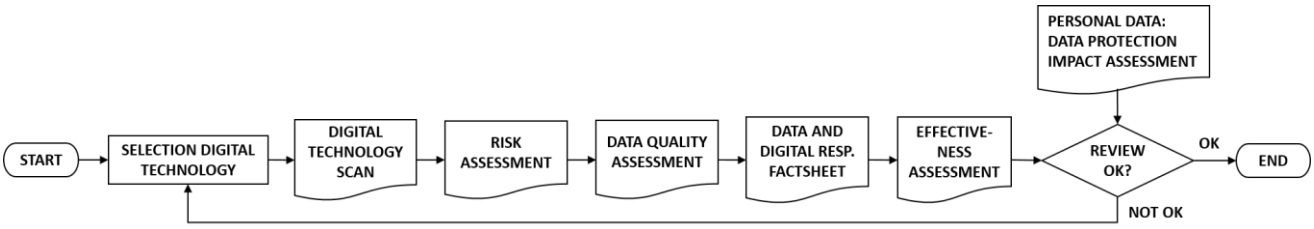
   We respect the rights of the data subjects whose data we process. We act in compliance with all applicable laws and regulations. We apply the seven Red Cross Red Crescent Movement principles to our work.

5. **Effectiveness**

   Our products improve the speed, quality and/or cost effectiveness of humanitarian aid.

Maintenance and updating of the policy will follow the Deming cycle for Plan, Do, Check, and Act (P.D.C.A).

## Data and digital responsibility review process




| Template | Purpose |
|---|---|
| Digital Technology Scan | An Excel template with key-questions for determining what data are used by the digital technology, how the technology processes the data and with whom the data are shared. |
| Risk Assessment | An Excel template providing several examples of risk events, enabling users to select their occurrence probability and severity of impact, both in qualitative terms, when using a digital technology. |
| Data Quality Assessment | An Excel template addressing quality dimensions, definitions and examples for: “Data accuracy”, “Data completeness”, “Data consistency” and “Required Update Frequency”. |
| Data and Digital Responsibility Factsheet | A Word template that is used for summarising the key-findings of the aforementioned templates. |
| Effectiveness Assessment | An Excel template to address the quality, speed and (cost)-effectiveness of applying the digital technology for humanitarian aid. Feedback and further insights are used to identify and close any gaps in skills to reach the next level of Digital Maturity. |
| Data Protection Impact Assessment | In case any personal data, or sensitive data are processed, their processing will need to be evaluated with expertise from a Data Privacy Officer and Security Officer. |

## Practicing the principles

| Principles | Description | What 510 does |
|---|---|---|
| **Human Centred** | Ensure that the purpose of our service is clearly defined.<br><br>Ensure that our services respond to the needs of the users of our products. | Co-design / interviews<br><br>Added layer of information: PESTLE / Involve local knowledge (Community Engagement and Accountability) |

| | | |
|---|---|---|
| **Do no harm** | Conduct risk assessments to understand the local context and incorporate mitigation measures.<br><br>Ensure that the products are proportional to the problem they solve.<br><br>Minimise the data that is processed.<br><br>Ensure correct use of the products. | PESTLE / Involve local knowledge (CEA).<br><br>Co-designs: feasibility-possibilities of technology<br>Digital Technology Scan<br>Risk Assessment<br>Data Quality Assessment<br><br>Data minimisation<br><br>Data & digital literacy, user testing. |
| **Transparency** | Provide clarity about how our products function, and don't function.<br><br>Clarify what data we process and how. | We provide F.A.I.R. manuals for our products (Findable, Accessible, Interoperable, Re-usable).<br><br>Digital Technology Scan<br>Risk Assessment<br>Data Quality Assessment<br><br>Our products and tools are published open-source.<br><br>Open data: we provide information on what data we use. |
| **Accountability** | Respect the rights of the data subjects.<br><br>Respect applicable laws and regulations.<br><br>Respect principles of the Movement. | Data Protection Impact Assessment<br>Data protection, minimisation, consent, confidentiality, integrity<br><br>Our work respects applicable laws and regulations such as GDPR<br><br>Our work respects principles of the Movement |

| | | |
|---|---|---|
| **Effectiveness** | Our products improve the speed, quality and/or cost effectiveness of humanitarian aid. | We select one or more of these indicators during co-design/interviews.<br><br>Effectiveness Assessment<br><br>We monitor the indicator(s) during prototype and user testing.<br><br>We continue to seek feedback from the users of our data and digital solutions after they have been deployed, so that we can continuously improve our data and digital solutions. |

## References on Intranet

- Digital Technology Scan
- Risk Assessment
- Data Quality Assessment
- Data and Digital Responsibility Factsheet
- Effectiveness Assessment