Power of humanity
Council of Delegates of the International Red Cross and Red Crescent Movement
27–28 October 2024, Geneva

Safeguarding Humanitarian Data

PROGRESS REPORT

September 2024

EN
CD/24/19
Original: English
For information

Document prepared by
the International Committee of the Red Cross
and the International Federation of Red Cross and Red Crescent Societies

PROGRESS REPORT

Safeguarding Humanitarian Data

EXECUTIVE SUMMARY

In 2022, the Council of Delegates of the International Red Cross and Red Crescent Movement (Movement) adopted a resolution on "Safeguarding humanitarian data". The resolution was a joint effort by the Movement to recognize the threats that cyber operations, in particular data breaches, pose to the work of humanitarian organizations, call for legal and policy measures to protect humanitarian organizations against such threats and align the measures that Movement components can and should take to protect humanitarian data against any unauthorized access.

In this progress report, the International Committee of the Red Cross (ICRC) and the International Federation of Red Cross and Red Crescent Societies (IFRC) present some of the specific measures taken by Movement components to safeguard the humanitarian data entrusted to them, recall some of the legal and policy measures taken by the ICRC to strengthen frameworks protecting humanitarian data, and report on some of the research and innovative work done by the ICRC and the IFRC, in particular the work to develop a digital emblem.

The report concludes that the adoption of the resolution on "Safeguarding humanitarian data" has provided an impetus to strengthen specific efforts on data protection within the Movement. However, continued work is needed by all Movement components – in a spirit of solidarity and shared responsibility. To strengthen policy alignment in the Movement and with States, some of the commitments and calls contained in the resolution will be further discussed at the International Conference of the Red Cross and Red Crescent (International Conference) in October 2024.

1) INTRODUCTION

As a result of the unprecedented breach of personal data entrusted to the International Committee of the Red Cross (ICRC) and National Red Cross and Red Crescent Societies (National Societies) in early 2022, in June of the same year the Council of Delegates adopted a resolution on "Safeguarding humanitarian data".

The resolution was a joint effort by the Movement to recognize the threats that cyber operations, in particular data breaches, pose to the work of humanitarian organizations, call for legal and policy measures to protect humanitarian organizations against such threats and align on measures that Movement components can and should take to protect humanitarian data against any unauthorized access.

The risks to humanitarian organizations posed by cyber operations, including data breaches, are serious. The 2022 data breach against the Movement specifically involved personal data, such as the names, locations of and contact information for missing people and their families, unaccompanied and separated children, detainees and other people receiving humanitarian services as a result of armed conflict, natural disasters or migration. In the wrong hands, the stolen data could potentially be used by States, non-State groups or individuals to contact or find people in order to cause them harm, ranging from the arrest or targeting of opponents to the trafficking of unaccompanied children. In addition, cyber operations breaching humanitarian data risk disrupting the operations of humanitarian organizations and eroding trust in their work. Trust is essential for humanitarian operations and a data breach risks

undermining the work of humanitarian staff, jeopardizing their ability to access people in need and compromising their safety, which may ultimately exacerbate the situation of people in need of their assistance.

At the legal and policy level, the resolution reaffirmed the Movement's commitment to implement data protection rules and cyber security measures. It underlined the responsibility of humanitarian organizations to take concrete and effective steps to ensure data security and protect any personal data entrusted to them. It further reaffirmed the international legal protection of impartial humanitarian organizations under international humanitarian law (IHL), which must be interpreted as also protecting them against any harm caused by digital means. It further emphasized that during armed conflicts, natural disasters and other emergencies, impartial humanitarian organizations' activities must be respected and protected online as well as offline.

In addition to aligning the Movement on policy questions, the resolution also committed Movement components to being responsible for taking appropriate steps, within the scope of their respective mandates, capacities and operational needs and contexts, to enhance their ability to ensure appropriate levels of data security. This includes, in particular, implementing relevant standards and good practices in the processing of personal data, taking into consideration the *Handbook on Data Protection in Humanitarian Action* and applicable national law, as well as sharing good practice on personal data protection, including data security, to support each other in building capacity and to consider the possibility of developing a Movement Code of Conduct for Data Protection.

2) BACKGROUND

This progress report reports to the 2024 Council of Delegates on some of the Movement's work, in particular by the ICRC and the IFRC, to implement the main commitments adopted in the 2022 "Safeguarding humanitarian data" resolution. The resolution built on the 2019 resolution "Restoring Family Links while respecting privacy, including as it relates to personal data protection", which was adopted at the 33rd International Conference. The 2022 resolution has also been a stepping stone towards the drafting of the proposed 2024 resolution on "Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict".

3) PROGRESS

To report on some of the progress that has been made, the following section will first present a selection of concrete measures taken by Movement components to safeguard the humanitarian data entrusted to them. It will secondly address some of the legal and policy measures taken by the ICRC and other Movement components to strengthen frameworks protecting humanitarian data; and third, it will report on some of the research and innovation carried out by the ICRC and the IFRC, in particular their work on a digital emblem.

A) STRENGTHENING DATA PROTECTION CAPACITIES WITHIN THE MOVEMENT

To strengthen data protection capacities within the Movement (and the broader humanitarian community), the ICRC has established two humanitarian action programmes: one with the University of Maastricht that focuses on training and certification for data protection officers, and one with the University of Cambridge that involves carrying out joint research into digital transformation and its implications for humanitarian action. As of April 2024, the training and certification programme developed with the University of Maastricht has been held 13 times across four continents, training more than 450 humanitarian professionals, of which more than 250 were National Society staff members covered by a full sponsorship.

The ICRC also supports National Societies globally in their work to comply with the *Code of Conduct on Data Protection* for the Family Links Network, developing and contextualizing data protection tools across the Family Links Network and helping National Societies in their dialogue with their authorities, particularly following the 2022 data breach. Several National Societies have worked significantly on data protection. For example, in 2023, the Zimbabwe Red Cross Society approved a volunteer and staff agreement to uphold the *Code of Conduct on Data Protection* to be signed by staff and volunteers working in Restoring Family Links (RFL); the Uganda Red Cross Society was certified as a data collector, data processor and data controller by its local data protection authority; and the Australian Red Cross developed a data protection simulation exercise for its staff and volunteers working in RFL. Movement components have also worked together as part of the Movement's RFL Code of Conduct on Data Protection Application Group and developed, among other things, a generic archiving policy and deletion guidelines for members of the Family Links Network.

The IFRC has continued developing its internal data protection practices and working with National Societies to help implement data protection obligations. For instance, the IFRC has completed several data protection impact assessments with National Societies on projects involving novel data processing techniques. The IFRC has also provided data protection training sessions to National Societies and has worked with several to help them develop and implement their own data protection policies and accompanying practices. The IFRC has further developed standardized data-sharing agreements and privacy statements designed to enable transparent, secure and legal transfers of personal data in emergencies between the IFRC and National Societies. The IFRC continues to develop, together with National Societies, software tools that are designed with data protection and do-no-harm principles at their core.

B) BUILDING A STRONG INTERNATIONAL LEGAL AND POLICY FRAMEWORK TO SAFEGUARD HUMANITARIAN DATA

Even strong data protection by humanitarian organizations will not, however, provide sufficient protection against data breaches. Building on the 2022 resolution, and to alert States to these new threats and reiterate the long-standing consensus on the protection of humanitarian organizations against harm, the ICRC raised the issue at the United Nations Open-ended Working Group on security of and in the use of information and communications technologies, calling on States "to reaffirm that humanitarian organizations, their staff, and humanitarian data must never be targeted, be it in the physical or in the digital world". In May 2024, the UN Security Council adopted resolution 2730, which expresses concern about data breaches that target humanitarian organizations.[1]

We are determined to continue efforts that lead to the strengthening of legal and policy frameworks or to have them put in place to this effect. A key opportunity for the Movement to achieve this objective will be the 34th International Conference in 2024, at which a resolution on "Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict" will be discussed. This resolution includes affirmations of the legal protection framework and policy commitments by Movement components and States to safeguard humanitarian data.

National Societies have taken concrete measures to strengthen protection frameworks for humanitarian data in their respective countries. For example, the Belgian Red Cross is negotiating agreements with the authorities on the protection of humanitarian data in joint activities and exceptions to data transfer requirements where such transfers are not compatible with the humanitarian mission of the National Society nor with its adherence to the Movement's Fundamental Principles. The British Red Cross, for its part, is working with the United

[1] The relevant preambular paragraph states: "Expressing concern about the increase in malicious information and communication technologies activities, including data breaches, information operations, that target humanitarian organizations, disrupt their relief operations, undermine trust in humanitarian organizations and United Nations activities, and threaten the safety and security of their personnel, premises and assets, and ultimately their access and ability to carry out humanitarian activities."

Kingdom's Information Commissioner's Office and seeking confirmation from the office that the British Red Cross may use the public interest basis when processing personal data related to the carrying out of its humanitarian activities.

C) ADVANCING RESEARCH AND INNOVATION

As stressed in the 2022 resolution, all Movement components should strive to invest further in data protection. The ICRC is working in parallel on possible technical measures to strengthen the protection of humanitarian organizations and their data from harm. For example, in 2022, the ICRC opened a delegation for cyberspace, which is designed to serve as a secure testing ground for carrying out research and development on safe digital services for affected communities.

Moreover, in November 2022, the ICRC, together with the Australian Red Cross, published a report entitled "Digitalizing the red cross, red crescent and red crystal emblems: Benefits, risks, and possible solutions". In 2023, the ICRC and the Australian Red Cross organized regional consultations with National Societies across the world. In 2024, the ICRC and the Australian Red Cross also established a National Society Working Group for the Digital Emblem.

The digital emblem project – including the latest technical solution called Authenticated Digital Emblem (ADEM) – was also presented to the private sector, including many of the world's largest cloud providers. To date, the ICRC has consulted bilaterally with over 20 States on the project discussing in particular how to incorporate the digital emblem into IHL and the need to support work on the digital emblem at the International Conference. It has further convened a consultation for all States to present and discuss the proposed technical solution for a digital emblem and invited all States to a consultation on legal and policy questions in the second half of 2024.

6) CONCLUSION AND RECOMMENDATIONS

The adoption of the resolution on "Safeguarding humanitarian data" has been a moment to reflect on and consolidate some of the cyber security and data protection work carried out by the Movement, and it has provided an impetus to strengthen efforts in this area. To strengthen the protection of humanitarian data across the Movement effectively, continued work is needed by all Movement components – in a spirit of solidarity and shared responsibility. To strengthen policy alignment in the Movement and with States, some of the commitments and calls contained in the resolution will be further discussed at the 34th International Conference.