Power of humanity
Council of Delegates of the International Red Cross and Red Crescent Movement

EN

CD/22/X.X
Original: English
For information

COUNCIL OF DELEGATES

OF THE INTERNATIONAL RED CROSS AND RED CRESCENT MOVEMENT

Geneva, Switzerland
22-23 June 2022

Safeguarding Humanitarian Data

Background document

Document prepared by
the International Committee of the Red Cross with the endorsement of
the Restoring Family Links Leadership Platform

Geneva, March 2021

EXECUTIVE SUMMARY

The 2022 cyber operation against servers hosting data held by the International Committee of the Red Cross (ICRC) and over 60 National Red Cross and Red Crescent Societies (National Societies)[1] has highlighted the risk that cyber operations and data breaches pose to humanitarian organizations. For several years, the ICRC and other members of the International Red Cross and Red Crescent Movement (Movement) have been warning of the critical and urgent need for States and other actors to protect humanitarian data and digital infrastructure from cyber operations, intrusion and misuse. The recent data breach has unfortunately shown that this risk is all too real.

Breaches of humanitarian data undermine the work of humanitarian organizations and may pose significant risks to the dignity and safety of people affected by armed conflict, disasters and other emergencies.

As the Movement implements measures to protect the people affected by the data breach and works to rebuild the compromised computer infrastructure, this Council of Delegates resolution aims to strengthen the legal and policy framework protecting the data and digital infrastructure of impartial humanitarian organizations. It provides a basis for the Movement's collective work towards a firm consensus – in words and actions – that humanitarian data must never be breached and that humanitarian activities need to be protected online as they are protected offline.

1) INTRODUCTION

In early 2022, the ICRC discovered that servers hosting the personal data of more than 500,000 people, who were receiving services from the Movement, were compromised in a sophisticated data breach.[2] While this came as a shock, it was not a rare occurrence; it reflects a growing trend in cyber operations targeted at humanitarian organizations.

Cyber operations against humanitarian organizations may have severe consequences for vulnerable people. The data breach against the Movement, for example, included the personal data (such as names, locations and contact information) of missing people and their families, unaccompanied and separated children, detainees and other people receiving humanitarian services because of armed conflict, natural disasters or migration. In the wrong hands, the accessed data could potentially be used by States, non-State groups or individuals to contact or find people in order to cause them harm, such as the arrest or targeting of political opponents or the trafficking of unaccompanied children.

In addition, cyber operations that breach humanitarian data risk disrupting the operations of humanitarian organizations and eroding trust in their work. Trust is essential for humanitarian organizations to operate and a data breach may jeopardize their access to people in need and the safety of their staff and operations, which may ultimately exacerbate the humanitarian situation of people affected by armed conflict, natural disasters and other emergencies.

As the Movement progresses with measures to protect the people affected by the data breach and works to rebuild the compromised computer infrastructure, this resolution aims to strengthen the legal and policy framework protecting the data and digital infrastructure of impartial humanitarian organizations. It provides a basis for the Movement's work collective towards a firm consensus – in words and actions – that humanitarian data must never be breached and that humanitarian activities need to be protected online as they are protected offline.

[1] For more information, see https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know.
[2] *Ibid*.

The resolution also constitutes a next step in the Movement's legal, policy and technical work on the protection of humanitarian data and operations, building on Resolution 4 of the 33rd International Conference of the Red Cross and Red Crescent (International Conference) and acting as a stepping stone towards another potential resolution at the 34th International Conference.

2) BACKGROUND

The resolution is the result of joint efforts by the ICRC, the International Federation of Red Cross and Red Crescent Societies (IFRC) and a number of National Societies to respond to the 2022 data breach. It sends a strong message to States, other actors and other impartial humanitarian organizations on the importance of safeguarding humanitarian data.

As this resolution is being presented in response to the 2022 data breach, all Movement components are invited and encouraged to engage in a series of fast-track consultations during March and April 2022, according to the following schedule:

- Mid-March 2022: Draft zero resolution shared with all Movement components
- End of March 2022: Online informal consultations open to all Movement components
- 8 April 2022: Deadline for Movement components to submit comments in writing on the draft zero resolution
- Early May 2022: Official mailing of all Council of Delegates documents, including a final draft resolution on safeguarding humanitarian data.

Movement components are also encouraged to discuss the draft zero resolution with either:

- Tilman Rodenhäuser, legal adviser, ICRC, trodenhauser@icrc.org
- Magnus Løvold, policy adviser, ICRC, mlovold@icrc.org.

3) ANALYSIS

The 2022 data breach has highlighted the risk that cyber operations, including data breaches, pose to humanitarian organizations, including the Movement. For several years, the ICRC and the Movement have been warning about the critical and urgent need for States and other actors to protect humanitarian data and digital infrastructure from cyber operations, intrusion and misuse. The recent data breach has unfortunately shown that this risk is all too real.

Accessing or extracting – without authorization – data that have been collected, stored or otherwise processed by impartial humanitarian organizations undermines their work and may create significant risks for the dignity and safety of people affected by armed conflict, disasters and other emergencies. While digital technologies rely on and operate in computer systems, the Movement's focus should always be centred on people, especially the most vulnerable.

Strengthening cyber security, data security and personal data protection within the Movement and in the wider humanitarian sector is a long-term objective requiring legal, policy and technical measures. The draft resolution, "Safeguarding Humanitarian Data", represents just one element in the Movement's response. It will also pursue multiple and interrelated objectives, including:

- drawing attention to the growing risk of cyber operations against humanitarian organizations and to the negative impact that data breaches have, and underlining the value of humanitarian data and their need to be protected
- sending the message that breaching data entrusted to humanitarian organizations:

  - undermines the safety, dignity and privacy of vulnerable people and may expose them to serious risks, including physical and psychological harm
  - undermines trust in these organizations and in impartial humanitarian action in general, potentially disrupting their operations and jeopardizing their efforts to alleviate human suffering
- reaffirming the commitment of the Movement to implement data protection rules and cyber security measures, and to ensure effective practices and compliance with them
- engaging the Movement in the issue and sending a strong message of commitment from the Movement to States, other actors and other impartial humanitarian organizations about:
  - the responsibility of humanitarian organizations to take concrete and effective steps to ensure data security and protect personal data entrusted to them
  - the responsibility of States to respect and to protect humanitarian organizations and their staff, information and assets, online as well as offline
  - the need for humanitarian organizations to work with each other and with partners to strengthen cyber security and to develop or acquire appropriate solutions that strengthen the prevention mechanisms against such attacks and that mitigate their impact, should they occur
- aligning the Movement around a common interest to research and develop measures to protect a neutral, independent and impartial humanitarian space in the digital sphere, such as the ICRC's research on a digital emblem.

4) RESOURCE IMPLICATIONS

By adopting this resolution, Movement components commit to take appropriate steps, within the scope of their respective capacities and operational needs, to enhance their ability to ensure appropriate and strong levels of data security when processing data (for example, collecting, storing or transferring) in order to carry out their activities, to comply with applicable law and personal data protection frameworks, and to implement relevant standards and good practices in the processing of personal data, taking into consideration the *Handbook on Data Protection in Humanitarian Action*.

Furthermore, the proposed resolution encourages the ICRC and other Movement components to conduct research and development into measures to protect a neutral, independent and impartial humanitarian space in the digital sphere. It also encourages the ICRC to continue researching the technical feasibility of a digital emblem and to assess its benefits.

The implementation of these commitments may have resource implications for individual Movement components, depending on the extent of their existing programmes and activities and the staff already assigned to this issue.

5) IMPLEMENTATION AND MONITORING

The success of this resolution depends on Movement components implementing it effectively and applying it coherently. All Movement components are expected to implement the resolution and apply it as part of their work on data security and personal data protection, as is feasible and appropriate.

All Movement components are invited to report to the 2023 Council of Delegates on the progress made in implementing this resolution.

6) CONCLUSION AND RECOMMENDATIONS

In light of the 2022 breach of humanitarian data held by the ICRC and over 60 National Societies, a Council of Delegates resolution on safeguarding humanitarian data is an important part of the response by the Movement to this new threat.

The resolution highlights the risks that cyber operations against humanitarian data pose to the people whose personal data are breached and to humanitarian organizations and their ability to fulfil their mandates to assist and protect people affected by armed conflict, natural disasters and other emergencies. It also affirms the Movement's commitment to use new technologies responsibly by striving to implement data protection rules and cyber security measures, and it sends a clear and strong message to States to respect and to protect humanitarian organizations and their staff, data and assets, online as well as offline.