Power of humanity
34th International Conference
of the Red Cross and Red Crescent
28–31 October 2024, Geneva

Restoring Family Links while respecting privacy, including as it relates to personal data protection

PROGRESS REPORT

September 2024

EN
34IC/24/10.4
Original: English
For information

Document prepared by the International Committee of the Red Cross in consultation with the Application Group for the Restoring Family Links Code of Conduct on Data Protection

PROGRESS REPORT

Restoring Family Links while respecting privacy, including as it relates to personal data protection

EXECUTIVE SUMMARY

The impact on individuals, families and communities of people being separated or going missing is one of the most damaging and long-lasting humanitarian tragedies. The Restoring Family Links (RFL) services of the International Red Cross and Red Crescent Movement (Movement) cover a broad spectrum of activities, including the prevention of family separation, restoring and maintaining family contact, clarifying the fate and whereabouts of missing persons and providing answers to their families, and facilitating family reunification whenever possible.

The effective and efficient performance of RFL activities[1] necessarily entails the continuous processing of personal data, including cross-border data transfers. Without the ability to transmit and match personal data, it would simply be impossible to provide RFL services. The rapid growth in the development of digital technology and the use of data has made it possible to gather large quantities of personal data faster and more easily. The Movement recognizes the enormous potential of these developments for its RFL services, but is also aware of the potential risks involved and of the importance of observing and developing appropriate data protection standards.

In 2015, the Movement adopted the *Restoring Family Links Code of Conduct on Data Protection* (Code of Conduct). Applicable to all components of the Movement, it uses the highest standards of data protection as a benchmark. By standardizing good practice, it strengthens proper data management within the Family Links Network (FLN)[2] and ensures the secure transfer of data within the Movement and to other actors. The Code of Conduct also provided a reliable support to guide the response to the 2022 data breach at the International Committee of the Red Cross (ICRC). The Central Tracing Agency (CTA), together with the Application Group for the RFL Code of Conduct (Application Group),[3] has been supporting the FLN in its efforts to improve compliance with the Code of Conduct's provisions. A plan of action was developed with three main pillars:

- development of guidance and promotion of best practices
- training
- reporting.

Under internationally recognized principles of data protection, any processing of personal data must have a legitimate basis. The mandate granted to the Movement to engage in the delivery of assistance to victims of humanitarian emergencies, which is based on international humanitarian law, as well as on the Statutes of the Movement and relevant resolutions of the International Conference of the Red Cross and Red Crescent (International Conference),

[1] Restoring Family Links (RFL) is the generic term given by the Movement to the range of activities that aim to prevent separation and disappearance, clarify the fate and whereabouts of missing persons, restore and maintain contact between family members and facilitate family reunification.
[2] The Family Links Network comprises the Central Tracing Agency (the CTA), the RFL units at the International Committee of the Red Cross (ICRC) delegations and the RFL/tracing services of National Red Cross and Red Crescent Societies.
[3] The Application Group provides guidance and support to the FLN on all matters related to the implementation and promotion of the Code of Conduct at the regional and global level.

underlines the grounds of public interest on which the processing of personal data for RFL purposes is carried out.

Despite this recognition, we still note that many National Red Cross and Red Crescent Societies (National Societies) are not being granted the option of relying on such a legal basis, which negates the fact that such processing is carried out by the Movement for exclusively humanitarian purposes. The Movement therefore emphasizes the importance for States to grant appropriate legal bases to National Societies and to refrain from requesting access to the data collected for RFL activities with the intention of using them for other, non-humanitarian purposes. This is crucial to mitigate the serious risks to the dignity and safety of people affected by humanitarian emergencies, whose personal data are extremely sensitive.

Furthermore, the cyber operation against the ICRC's servers in 2022 highlighted the risks that cyber operations and data breaches pose to humanitarian organizations and the people they seek to help. The Movement addressed this topic in Resolution 12 of the 2022 Council of Delegates on "Safeguarding humanitarian data"[4] aimed at granting special protection to personal data collected for humanitarian purposes and digital infrastructure from cyber operations, intrusion and misuse.

Additionally, it is important to underline the need for States to acknowledge that frequent cross-border flows of personal data are necessary for the effective provision of RFL activities and should remain as unrestricted as possible, while still complying with strict data protection requirements. The Code of Conduct's high standards should instil confidence in both individuals and regulators with regard to the work of the Movement, and provide reassurance to members of the Movement who need to transfer personal data between each other.

1) INTRODUCTION

The FLN has long played a central role in helping authorities meet their obligations by delivering RFL services. International humanitarian law, which applies in situations of armed conflict, contains relevant rules concerning respect for family life, maintaining or re-establishing family links and clarifying the fate and whereabouts of persons reported missing as a result of armed conflict.[5] Other international instruments also reiterate relevant rights related to respect for family life, unity and reunification.[6]

For the separated, the missing and their families, the need for RFL services arising from armed conflict, violence and disasters is as important as ever. However, over the last 15 years, we have witnessed an increase in the Movement's involvement in addressing the needs of separated and missing migrants and their families, which have often gone unmet. In the absence of effective mechanisms and cooperation between States to clarify the fate and whereabouts of missing migrants, families seeking information about their missing relatives are alone in dealing with uncertainty.

The demand for a strong global FLN is evidenced by the growing numbers of people approaching the Movement for RFL services, which therefore involves the collection of massive amounts of personal data, sometimes in fragile and volatile contexts. The mandate

[4] Resolution 12 of the 2022 Council of Delegates, "Safeguarding humanitarian data", available at: https://rcrcconference.org/app/uploads/2022/06/CD22-R12-Safeguarding-Humanitarian-Data_23-June-2022_FINAL_EN.pdf.

[5] This includes the obligation stemming from the Geneva Conventions of 1949 – and developed in Additional Protocol I of 1977 – to facilitate enquiries made by relatives of persons dispersed in connection with an armed conflict, with the aim of restoring family links and facilitating the reunion of dispersed families in every possible way. It also includes the obligation of States parties to the Geneva Conventions to enable all persons in their territory to give news of a strictly personal nature to members of their families, wherever they may be, and to receive news from them. Furthermore, according to Additional Protocol II, children shall be provided with the care and aid they require, in particular, all appropriate steps shall be taken to facilitate the reunion of families temporarily separated.

[6] See, for instance, the Universal Declaration of Human Rights, 1948, Article 16; the International Covenant on Economic, Social and Cultural Rights, 1966, Article 10; the International Covenant on Civil and Political Rights, 1966, Article 23; the Convention on the Rights of the Child, 1989, Articles 9, 10, 20 and 22; and the International Convention for the Protection of All Persons from Enforced Disappearance, 2006, Articles 17, 24 and 25.

granted to the Movement to deliver assistance to victims of humanitarian emergencies, which is based on international humanitarian law as well as on the Statutes of the Movement and relevant resolutions of the International Conference, underlines the grounds of public interest based on which the processing of personal data for RFL purposes is carried out.

2) BACKGROUND

The International Conference has affirmed the importance of RFL on numerous occasions. The 24th International Conference requested National Societies to carry out tracing and family reunification and asked governments to facilitate the work of the Movement and give it all the necessary support. The 26th International Conference asked States to grant National Societies access to relevant data and facilitate National Society tracing and family reunification work in situations of armed conflict. Furthermore, the 28th International Conference established a series of goals in relation to people missing as a result of armed conflict and other situations of violence. Among them were the goals of preventing people from going missing, ascertaining the fate of missing persons, managing information and processing files on missing persons. The 33rd International Conference, through Resolution 4, recalled that personal data protection is closely related to privacy, and took into account that processing personal data is an integral part of RFL services and necessary for Movement components to fulfil their mandate.

The commitment of the Movement to managing information and processing data responsibly is evidenced in the development of the Code of Conduct, the first of its kind for a Movement service. It sets out the minimum principles, commitments and procedures that members of the Movement must comply with when processing data within the FLN. A dedicated working group[7] supports the global implementation of the Code of Conduct. With the conclusion of our RFL strategy 2008–2018, the RFL strategy 2020–2025, and its foreseen extension until 2030, as well as the implementation of the Code of Conduct, we continue our commitment to data protection as a critical enabler for the processing of personal data.

3) PROGRESS

It is critical for the functioning of the FLN to reaffirm with States the specific role and capacity of the Movement in RFL and the support it can provide to the authorities in fulfilling their obligations and commitments vis-à-vis separated family members, the missing and their families, including those related to missing migrants. Cooperation with the authorities and other key stakeholders must be pursued, exercising careful consideration and implementing transparent procedures that adequately protect the people who access RFL services and their sensitive data.

The processing of personal data is more crucial for RFL than for any of the Movement's other services, as it requires the ability to transmit and match personal data. This specificity and the need to protect its humanitarian purpose needs to be further recognized by States.

A) REFLECTING HUMANITARIAN ACTION IN DATA PROTECTION LAWS

Since the adoption of the resolution, data protection laws and regulations have been passed or updated in many countries, showing an increasing awareness of the importance of setting principles and standards to regulate the processing of personal data. However, these legal acts do not always consider the impact of their provisions on the work of humanitarian actors, especially those which are fully subject to the national legislation. This comes from the analysis of two key elements:

[7] The Application Group for the RFL Code of Conduct on Data Protection.

i. National Societies need an appropriate legal basis to perform their humanitarian mandate

States recognized, through the adoption of the resolution, the difficulty (and often impossibility) of obtaining the consent of people benefiting from an RFL service, given their vulnerability and the nature of humanitarian operations. The resolution also highlights that the processing of personal data for RFL purposes could rely on other valid bases, such as important grounds of public interest, vital interest and compliance with a legal obligation. Processing personal data for important grounds of public interest is particularly appropriate for RFL activities, as it is part of our humanitarian mandate and needed to accomplish the task set out in the Statutes of the Movement. However, a significant number of National Societies have not been able to resort to the public interest or other viable legal bases in their national legal frameworks, leaving no other choice than to rely on consent.

States are encouraged to pursue their efforts in identifying a direct link between humanitarian action, including RFL, and the processing of personal data based on other valid legal bases, such as important grounds of public interest. In some cases, national data protection laws, whether they entered into force before or after the adoption of the resolution[8] that is the subject of this progress report, have not considered public interest as one of the appropriate legal bases. In other cases, it has been observed that public interest has not been considered to legitimate the processing of sensitive data, a recognized essential aspect when carrying out RFL activities.

ii. International transfer of personal data

The performance of RFL services requires an intense and continuous sharing of information between and among National Societies and ICRC delegations. This entails cross-border data transfers, mainly through safe digital platforms provided by the CTA, such as Secure File Exchange (SFE)[9] and Family Links Answers (FLA).[10] However, still too often, domestic data protection laws pose restrictions on the transfer of personal data to entities abroad with no exemption for humanitarian organizations, despite the recognition that data sharing within the Movement should remain as unrestricted as possible. In some cases, a special authorization from the national supervisory authorities may be required. In others, the assessment of the legal framework in the country of destination is requested, but without the guidance or the tools to do so being provided by the national supervisory authority.

It is crucial that the Movement and States pursue their coordinated efforts to address the impact of domestic legislation on data protection in the humanitarian context.

B) PROTECTING DATA BY PROTECTING HUMANITARIAN ACTORS

In the resolution, the International Conference has recognized the importance of data protection for the Movement in fulfilling its humanitarian mandate. However, the Movement still faces challenges in accessing information or having its data protected, despite progress and support from States. It has been observed that some States are concerned about disclosing their datasets to the Movement, which could provide valuable information for RFL services. They cite data protection challenges that, upon closer examination, may lack sufficient basis. Consequently, this stance hinders the pursuit of a humanitarian purpose, which should inherently justify the legitimate processing of data. In other cases, National Societies were requested to disclose personal data for purposes incompatible with their humanitarian mission

[8] Resolution 4 of the 33rd International Conference, available at: https://rcrcconference.org/app/uploads/2019/12/33IC-R4-RFL-_CLEAN_ADOPTED_en.pdf.
[9] SFE is an online platform to share protection-related documents between and among National Societies and the ICRC. Within the FLN, SFE is used for sharing electronic documents related to the RFL caseload that contains personal data.
[10] FLA is a web-based application that aims to support the RFL services of National Societies. FLA serves as an instrument to reinforce the management and follow-up of RFL cases and provides a detention module for National Societies that carry out activities in places of detention.

and contrary to the resolution. Such practices jeopardize the effectiveness of RFL services and risk losing the trust of affected people, which the Movement needs to pursue its mission, and go against the principle of "do no harm".

Additional threats come from cyber attacks and security incidents. The 2022 cyber operation against servers hosting data held by the ICRC and over 60 National Societies highlighted the risks that cyber operations and data breaches pose to humanitarian organizations[11] and affected people benefiting from their services, as the data of more than 500,000 people were breached.

Following this attack, the servers had to be taken down and systems had to be rebuilt. The CTA coordinated the Movement response to the breach. The ICRC delegations and National Societies impacted by the breach, with the valuable support of IT and legal experts across the Movement, analysed individually whose and what data were breached and conducted a risk assessment to support them in the decision to notify not only the authorities but also the people concerned, as well as identify mitigation measures to support the affected individuals. Depending on the sensitivity of the context, choosing the right manner to notify the people affected was also crucial. The Movement used different channels depending on the context: public announcements, phone calls, face-to-face meetings, letters and emails. The consequences were dire: trust in the Movement was impacted and RFL services around the world drastically slowed down. The effect of the breach was felt months after its discovery.

Thankfully, the Code of Conduct was instrumental during this crisis and provided the principles and procedures to be followed after a data breach. The framework provided by the Code of Conduct proved helpful in defining whether the incident matched the definition of a data breach and coordinating the response in terms of risk analysis and engaging a dialogue with system users and those affected, should the incident be likely to affect their rights and freedoms.[12]

The disruptive impact of such attacks threatens humanitarian work. It is therefore essential to reiterate the message of the Council of Delegates resolution on "Safeguarding humanitarian data" and call for States to respect and protect humanitarian organizations – including National Societies, their volunteers and staff, data and assets[13] – by recognizing within their national cyber security strategies their key role as critical infrastructures and by adopting legislative measures to allow for an immediate response to external threats to their data.

C) THE MOVEMENT'S EFFORTS TO INCREASE DATA PROTECTION COMPLIANCE

Since the approval of the resolution, the Movement has worked to increase understanding of data protection and its pervasiveness in RFL activities. The Implementation Group for the RFL Strategy 2020–2025, which is responsible for the implementation of the resolution, has played a key role. This body is assisted by the Application Group, which is composed of the ICRC, National Societies from different regions, and the International Federation of Red Cross and Red Crescent Societies (IFRC), to support the Movement on all matters pertaining to the implementation and promotion of the Code of Conduct at the national, regional and global level.

As part of these efforts, the Application Group worked on determining the key monitoring indicators (KMIs) set out in the monitoring and evaluation framework of the RFL Strategy in order to assess the data protection compliance status of each Movement member each year. These KMIs also serve as a reference for each Movement member to develop its own strategy for data protection.

[11] For more information, see https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know.
[12] Paragraph 2.3.8 of the Code of Conduct.
[13] Paragraph 13 of Resolution 12 on "Safeguarding humanitarian data".

The figures collected through the latest monitoring and evaluation self-assessment survey, launched by the CTA in 2024, show a positive trend of global improvement in the Movement's data protection compliance: the overall result on full compliance with data protection within the Movement increased from 1.3% to 5%, whereas medium compliance increased from 18% to 21%. However, 50% of the Movement reported low compliance and 2% reported no compliance at all.[14]

The Application Group has developed a plan of action for the Code of Conduct to enhance the protection of affected people by protecting their personal data and has identified three pillars: guidance, training and reporting. The post of data protection legal expert to support the National Societies in their efforts to increase their data protection compliance was filled and the position retained.

The Application Group developed an information notice template for the Movement to implement the principle of transparency towards affected people in a concise and intelligible format, and it created a template that allows them to express their right to object.

The Application Group also supported the Movement's efforts for better data protection compliance by providing:

- a template to create an archiving policy
- a checklist to analyse the domestic legal framework on data protection
- a mechanism to share good practice on implementing the Code of Conduct
- a guidance on data retention and data deletion
- a data-sharing agreement template to be used by National Societies sharing personal data with entities outside the Movement.

An increasing number of National Societies have identified a data protection focal point for their RFL activities who ensures they integrate a data protection perspective in their operations. Also, several members of the Movement have launched interesting initiatives to raise awareness of data protection and train staff and volunteers. The ICRC has provided a series of webinars to ICRC delegations and National Societies to explain the methodology and content of the data protection templates aligned with the requirements of the Code of Conduct. Several online and face-to-face training sessions on data protection in RFL have been organized around the world.

Moreover, the ICRC launched a programme in association with Maastricht University and developed a training and certification programme for data protection officers in humanitarian action.[15] Since 2021, 13 sessions have taken place covering different regions worldwide. As at May 2024, 259 National Society staff members and 61 ICRC staff members had benefited from the sponsorship systems set up by the ICRC with the support of Luxembourg's Ministry of Foreign and European Affairs.

To strengthen data security, the CTA provided the Movement with a safe file exchange platform and a safe case management tool that is now in use in more than 70 National Societies.

The ICRC also works with the IFRC to assist National Societies in certain regions in setting up institutional email addresses. However, more support from States, the private sector and the Movement is needed to make further significant progress towards digitalization and data security in those contexts experiencing a scarcity of technical and logistical resources or facing

[14] These figures were obtained based on the KMIs. There are nine KMIs for National Societies and six for the ICRC. Of these KMIs, six are considered foundational for National Societies and four are considered foundational for the ICRC. To obtain full compliance, a National Society or an ICRC delegation needs to answer "yes" to all KMIs; for medium compliance, they need to answer "yes" or "partially" to the foundational KMIs; for low compliance, they need to answer "yes" or "partially" to fewer than six of the foundational KMIs; and for no compliance, they need to answer "no" to all nine KMIs.
[15] Data Protection Officer (DPO) Humanitarian Action Certification, Maastricht University: https://www.maastrichtuniversity.nl/events/data-protection-officer-dpo-humanitarian-action-certification.

emergency situations where the risk for affected people in case of loss, misuse or unauthorized access to their data is likely to be higher.

4) RESOURCE IMPLICATIONS

A well-functioning and effective FLN requires technical expertise and leadership at global, regional and national level; it also needs dedicated, well-trained staff and volunteers, access to digital technology, an ability to respond and scale up in emergencies, and flexibility to offer the best service through the most appropriate means. Financial resources are required to meet the objectives of the RFL strategy 2020–2025, which is likely to be extended until 2030. We will continue to seek support from governments.

5) IMPLEMENTATION AND MONITORING

The Implementation Group, with the technical support of the Application Group, will keep leading the implementation of the resolution. Following the RFL strategy, the Movement will continue to implement and report annually on its data protection compliance progress. Communication of progress to the members of the International Conference is encouraged through bilateral dialogue between the National Society and the relevant government authority to ensure cooperation. At the global level, progress reports will be submitted to the International Conference and the Council of Delegates.

6) CONCLUSION AND RECOMMENDATIONS

It is critical for the functioning of the FLN to reaffirm with States our specific role in RFL and our cooperation with States in this field, including acknowledgment of the Movement's needs to accomplish its humanitarian mandate.

A joint commitment by States and the components of the Movement to this process and ongoing dialogue is necessary for the legitimacy and reputation of all components of the Movement as trusted institutions that seek exclusively humanitarian outcomes. Noting that the resolution remains valid, the ICRC recommends that efforts towards its implementation continue to be put in place in recognition of the value of the FLN and the support it provides to separated and missing persons and their families across the globe.

The ICRC and the Implementation Group will continue to recommend that States afford special protection for personal data that are being processed to provide RFL services from requests or uses of such data for non-humanitarian purposes. Moreover, we call on States to respect and protect the Movement in the digital environment by taking appropriate steps to ensure that domestic law protects the confidentiality, integrity and availability of personal data collected for providing RFL services and to provide safeguards against harmful cyber and information operations.

The ICRC and the Implementation Group will continue to recommend that States identify appropriate legal bases – such as important grounds of public interest, vital interest and compliance with a legal obligation – in their national data protection laws to allow the processing of personal data by the FLN for humanitarian purposes. We also emphasize the importance of legal grounds to facilitate the cross-border transfer of personal data between Movement members.

The CTA recognizes and promotes the prominent role of data protection to safeguard the life, dignity, integrity and safety of affected people benefiting from RFL services. It will therefore pursue its efforts to support the FLN's compliance with data protection.