

COVID19: Processing personal data and data management remotely

This document, addressed to both National Societies and ICRC RFL teams, provides guidance on data management and how to get beneficiaries' consent/no objection for the processing of their personal data in time of COVID19, especially regarding the adjustment of the RFL services to restriction of movement and challenges in term of access to our services.

Contents

1. Safe way to communicate	1
2. Data Management	2
3. Processing personal data	2
What is personal data?	3
What is a "transfer" and "publication" of data?	3
What is a "legal basis" for data processing? Should I ask the enquirer for consent?	3
3.1. Information Notice	4
3.1.1 Extract from the Information Notice	4
3.2. Get the consent/no objection over the phone	5
3.2.1 Extract from the template for processing personal data	6

1. Safe way to communicate

Data protection and confidentiality principles still apply.

Refrain from collecting more personal information than is necessary for the RFL/Tracing/humanitarian purpose(s) of collecting and processing that data.

Ensure that personal data collected is used only for humanitarian purposes and that such specified purpose(s) are communicated to data subjects (unless when logistically impossible, for example the provision of information to missing persons about the processing of their data). The collection and processing of data should be done proportionally, fairly, transparently (via the provision of an oral or written Information Notice), and lawfully.¹

Secure means to exchange personal data such as e-mails using a ZIP password protected file and direct phone calls are to be used to contact the beneficiaries, unless phone calls are not secure in a given context.

¹ See the RFL Code of Conduct on Data Protection at <https://www.icrc.org/en/document/rfl-code-conduct> and (for ICRC staff) the ICRC Rules on Personal Data Protection (RPDP) at <https://intranet.ext.icrc.org/structure/dirgen/dtd/dpo/index.html>. For recent statements and guidance from Data Protection Authorities on the application of national data protection law in the context of COVID-19, see <https://globalprivacyassembly.org/covid19/> and <https://iapp.org/resources/article/dpa-guidance-on-covid-19/>. Note however that, in most contexts, the ICRC benefits from privileges and immunities and is not subject to domestic jurisdiction / national data protection laws. It therefore applies its Rules, rather than national law, when processing personal data.

Within the Family Links Network (FLN), Secured File Exchange (SFE) or interoperability between FLA and Prot6 remain the only, secure channels to exchange personal data and confidential information.

As a last resort, if you must use a messaging application (e.g. Signal Private Messenger) to communicate with beneficiaries/enquirers, there are several helpful guides to assist in determining how and what communication tools are to be used (e.g. <https://securityplanner.org/#/>; https://www.centre4innovation.org/wp-content/uploads/2020/04/FINAL_SecCom_09042020.pdf²; <https://ssd.eff.org/module-categories/tool-guides>). For ICRC staff, please refer to the recently approved *ICRC Exceptional Use of Non-ICRC Apps (EUNIA) Rules* for instructions on how to conduct a risk assessment and seek validation for the use of an application for a specific case.³ However, even after the risks of using a tool in a particular context has been assessed and validated, it should be used for the collection of minimum data only (identifiers, i.e. names and contacts details of the enquirer and the sought person and basic non-sensitive data on the request), allowing required follow-up and not to document sensitive cases/information (tracing requests, allegations of arrest/detention). The collected data should be recorded accordingly (refer to point 2. Data management):

- **For new cases to be documented:** Name of the enquirer, his/her contact detail and name of the missing person
- **For Follow up with enquirer on documented cases:** Name of the enquirer and his/her contact detail

Social media should be used only for the promotion of RFL services but not to share personal data.⁴

2. Data Management

Working remotely and in emergency time usually brings along challenges in regards with the management of the data. Nonetheless, to ensure a qualitative service is provided and make sure an adequate follow up of the case, a particular attention is to be given to an appropriate data management (digital and hard copy).

Please ensure coordination with your staff in charge of data management for all decisions on either adapting existing systems or creating temporary solutions.

- Ensure all activities toward the missing, the separated and their families (follow up of cases, contact with beneficiaries, intervention, etc.) are recorded in your case management tool (FLA, Prot6, other).
- If no remote access to case management tool (FLA, Prot6⁵, other), ensure a safe and centralized data management system is **temporarily** put in place that will allow the data to be uploaded in the tool once the situation will allow it again.
- Assess the need (time and human resources) that will raise and be needed in regards with the update of data in the case management tool once the situation will allow it again.
- Ensure the RFL activities related to the disruption of family contact due to COVID19, are specifically flagged for further follow up and for statistical/promotion purpose (i.e.: tagging COVID19).

3. Processing personal data

Please find hereafter some definitions on personal data and its processing. Then, you will find practical guidance on how to apply it during COVID19 and working remotely.

This section is based on the Data Protection Template for RFL elaborated, although not yet validated, by the Application Group on Code of Conduct for Data protection for RFL purpose composed by NS and ICRC. The guidance should be finalized and shared with the field very soon, with guidance, instruction, scope of application

² See Chapters 3 and 4 for a comparative assessment of messaging apps including WhatsApp, Telegram, Signal, WeChat and Facebook Messenger.

³ For ICRC staff, please see [EUNIA Rules](#) and consult the ICRC DPO for assistance in conducting risks assessments for the use of messaging apps or other tools, or for any other questions or concerns.

⁴ See *The Humanitarian Metadata Problem: "Doing No Harm in the Digital Era"*, ICRC and Privacy International (October 2018), Chapter 7: "Social media platforms".

⁵ For ICRC only: If the difficulties in accessing Prot6 is linked to connectivity, you can consider using the Offline mode of the webpage for Tracing Request / Allegation (refer to Data manager/RPDO for access/training)

and tutorial on how to implement/contextualize it. Nonetheless, in this time of COVID19, it could help providing you with basic guidance.

What is personal data?

Personal Data means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, audio-visual material, a number (e.g. registration number), location data, online identifier (e.g. IP addresses or cookie identifiers) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

What is a “transfer” and “publication” of data?

The RC/RC Movement’s components may need to share (“transfer”) personal data with other entities or publish that data in order to search for family members and clarify the fate of the missing. Publication of personal data consists of making it available to the general public. This includes making personal information available on a public website or in a news publication or through the dissemination of leaflets or posters. The publication of personal data is a data “processing activity” and, as such, is subject to data protection principles. The “transfer” of personal data is also a data processing activity. RC/RC Movement components transfer personal data amongst themselves and to other entities (e.g. NGOs, international organizations, and authorities) for the provision of RFL services.

Individual can **object** to the transfer or publication of their personal data and the personal data of the sought person. These objections (also referred to as “restrictions”) should be recorded by the RC/RC personnel.

What is a “legal basis” for data processing? Should I ask the enquirer for consent?

Data Protection legal principles, and often national and regional laws, require that an individual’s personal data only be collected and used if there is a legal basis for doing so. There are different types of legal bases upon which components of the Movement can rely in order to “process” (e.g. collect, use, transfer, store and archive) personal data.

One well-known basis for data processing is **consent**. In order for consent to be valid though, an individual must be capable of providing consent that is **freely-given, specific and informed**. This means s/he must have the genuine and free choice to provide consent for the processing of their personal data for a specific purpose and must fully understand the implications of doing so. For example, in a place of detention, camp or remote community where only the RC/RC Movement provides RFL services, consent to personal data processing for those services will not be freely-given because the individual’s only alternative option is to refuse assistance in restoring contact with his/her family. Likewise, when a person does not have the physical / mental / emotional / legal capacity to understand the circumstances, risks and benefits of the processing of their personal data, consent cannot be informed and therefore should not be obtained.

However, if domestic legislation allows it,⁶ the components of the Movement may rely on other legal bases. One such legal basis is “**public interest**”, which is relied upon when personal data is being collected and processed as part of a humanitarian activity that is mandated under international humanitarian law, national law, and/or the Statutes of the RC/RC Movement, such as Restoring and Maintaining Family Links activities and clarifying the fate of the missing persons.

If the domestic legislation allows it, personal data can also be collected and processed without consent if it is necessary to ensure that the “**vital interest**” of an individual, like a sought person or enquirer, is safeguarded (i.e. their life, integrity, health, security). Personal data may be collected and processed on this basis in situations such as: providing essential needs in the aftermath of a humanitarian emergency; providing RFL / Tracing services to individuals of particular vulnerability whose primary caregiver has gone missing; providing assistance to an

⁶ NB: The ICRC maintains privileges and immunities in most contexts and thus applies its Rules on Personal Data Protection when processing personal data, which provides lawful bases other than consent for such processing (see Art. 1 of RPDP).

individual who is unconscious and/or in need of immediate medical care; responding to an imminent threat against the physical and mental integrity of individuals. As consent cannot be obtained from a sought person, components of the Movement have no choice but to rely on either the public or vital interest legal bases to collect the sought person's personal data from relatives and process that data.

The parent or legal guardian of a **child** (i.e. person under the age of 18) should provide consent on their behalf. A child does not have the legal capacity to provide consent her/himself unless national law allows for it. Even if a child has the legal capacity to consent,⁷ account should be taken of the possible various subjective and objective elements of vulnerability that affect him/her including level of maturity, as well as cultural considerations. Given the particular vulnerability of **unaccompanied and separated children**, the public and vital interest legal bases are preferred when processing their personal data. Regardless of the legal basis relied upon to collect and process the personal data of a child, s/he maintains the right to transparency (i.e. "Information Notice"). All children capable of forming their own views must be consulted and have their opinions/objections sought and heard for each data processing activity affecting them. This also applies when a parent or legal guardian is present and consents on a child's behalf. In case of disagreement as to whether the child's data should be collected and processed, an assessment as to the best interest of the child may be necessary.

Practically-speaking, relying on public or vital interest bases means that you: (1) do not specifically ask for consent ("Do you agree/consent to [...]?"); (2) however allow the enquirer the opportunity to object to data processing when relying on public interest; (3) still provide an Information Notice (e.g. information on rights, purpose of processing); and (4) record in the forms to be filled out and in your case management system (e.g. Prot6, FLA) which legal basis you relied upon when processing the person's data.

3.1. Information Notice

Data Protection legal principles require that individuals whose personal data is collected and processed are provided with information prior to the collection of their personal data. This includes information about their rights, the purpose(s) of collecting and processing their personal data, whether their data will be published or shared with others (and with whom), and who they can contact if they have any questions/concerns/complaints about the handling of their data.⁸ This is a standard procedure that **ensures the individual is fully informed and that their data protection rights are respected.**

Information notices **can be given orally.** Certain minimum information should be explained to the beneficiary so that any consent obtained is "informed", thus valid, or if a more appropriate alternative lawful basis to consent is relied upon, the data subject can effectively exercise their right to object.⁹

Find under an extract of the Information Notice that was elaborated, although not yet validated, by the Application Group on Code of Conduct for Data protection for RFL purpose:

3.1.1 Extract from the Information Notice

The [mention name of National Society/ICRC] needs to **share** information, including your personal data or personal data of your sought relative, with specific third parties for exclusively humanitarian purposes if they can contribute to the search of your relative. Alternately or in addition, we may need to **publish** such information.

⁷ NB: These laws would not apply to the ICRC, as an International Organization, in countries where it maintains certain privileges and immunities.

⁸ See a list of minimum information to be shared with beneficiaries in Annex 5 of the RFL Code of Conduct on Data Protection and (for ICRC staff) Art. 7 of the ICRC RPD.

⁹ For an explanation of lawful bases, other than consent, for the processing of personal data, as well as the right to object to processing, see section 3 above.

The [mention name of National Society/ICRC] will be the sole controller of the personal data you share with us, unless and until it is shared with an external party.

In particular, the [mention name of National Society/ICRC] may need to share data with (for each, [mention with whom the case might be shared]):

- Other Red Cross/ Red Crescent Movement's components, which may in turn have to share data with other entities (including in particular national authorities) in order to find your relative;
- Other International Organizations such as:
- Other local Organization such as:
- State Authorities such as
- Non-state armed groups such as:

Data (including pictures) may need to be published the following way:

- In hard format [specify format and location of publication (for instance booklet, posters)]; and/or
- On-line [specify the Website (for instance Trace the Face, snapshot, online tracing)].

We will only use the information that you give us to do Restoring Family Links ("RFL") activities, namely clarifying the fate and whereabouts of missing persons. Please be aware that [name of National Society] might be under a legal obligation to share some personal data with local or national authorities, in particular for law-enforcement or national security related purposes.

The personal data we collect will be kept by the [name of National Society/ICRC] until the fate and whereabouts of your sought relative has been clarified, the family link restored or no further action is required [to be completed according to criteria for closure of cases in each National Society].

Personal data may still be kept by [name of National Society/ICRC] for archiving purposes, including for historical, statistical and educational reasons.

Please contact the [name of National Society/ICRC] at [phone number, office address, email address] if you:

- Have a question, complaint, or would like more information about how we handle your personal data;
- Want to request access to, change or erase the personal data you have provided us.

3.2 Get the consent/no objection over the phone

As mentioned above, a template on data processing was elaborated by the Application Group on Code of Conduct for Data protection for RFL purpose composed by NS and ICRC. The guidance should be finalized, validated, and shared with the field very soon, with guidance, instruction, scope of application and tutorial on how to implement/contextualize it. We are working as well with data management teams on how to reflect the content of the new template in Prot6 and FLA, particularly how to record beneficiaries' "objections" (none, partial, total) to sharing/publishing the data. For more information on the right to object to personal data processing, see section 2 ("What is a 'transfer' and 'publication' of data?") above.

Nonetheless, and for the time being and especially in time of COVID19 and access constraints, ask for any objection to share/publish data as per today practice ("transmissibility" part of the existing forms) and record it according to current Prot6 and FLA guidance/practice.

Nonetheless, as you cannot get the signature of the enquirer, you can either record in the form or in a separate document the mention that the case was collected over the phone and document on the form or in separate form which objection where raised (e.g. "The beneficiary objects to the publishing of their photo and the sharing of any of their personal data with the authorities."). This information should be captured and updated in the case management tool (Prot6, FLA, other).

To help you, please find below the extract of the template, not yet finalized and validated, which allows personnel to record that the content of the Information Notice (above mentioned) was explained to the enquirer and that consent or certain objections were provided by the enquirer.

3.2.1 Extract from the template for processing personal data

Name of the enquirer/individual: _____
Case number: _____
Name of Personnel: _____

1. Processing of personal data of sought person

I, _____ (full name and title of the personnel) of _____ (RC/RC Movement component), confirm that the information regarding the processing, including transfer and/or publication, of personal data of the sought person was explained to _____, the enquirer / legal guardian of enquirer (circle) on ____ / ____ / ____ (date), in person / **over the telephone** (circle). I confirm that s/he provided the answers recorded herein.

In the case of a **child** able to form her/his own views, indicate whether s/he agrees with the data processing:

- Fully agrees Disagrees

In case of disagreement, please specify and provide personnel's comments regarding the considerations behind her/his decision. (Personnel may need to do an assessment of the best interests of the child):

Signature of the personnel: _____

Date and place: _____

2. Processing of personal data of enquirer when informed and freely-given consent cannot be obtained due to e.g. vulnerability of enquirer (public/vital interest is instead used as legal basis)

I, _____ (full name and title of the personnel) of _____ (RC/RC Movement component), confirm that the information regarding the processing, including transfer and/or publication, of personal data of the enquirer was explained to _____, the enquirer / legal guardian of the enquirer (circle) on ____ / ____ / ____ (date), in person / **over the telephone** (circle). I confirm that s/he provided the answers recorded herein.

In the case of a **child** able to form her/his own views, indicate whether s/he agrees with the data processing:

- Fully agrees Disagrees

In case of disagreement, please specify and provide personnel's comments regarding the considerations behind her/his decision. (Personnel may need to do an assessment of the best interests of the child):

Signature of the personnel: _____

Date and place: _____

3. Processing of personal data of **enquirer** when informed and freely-given **consent can be obtained**

I, _____, the enquirer / legal guardian of the enquirer (circle), hereby consent to the processing, including transfer and/or publication, of my/the enquirer's personal data for the purposes described and with the restrictions (if any) provided.

Signature of enquirer or legal guardian: _____

Date and place: _____

If consenting enquirer or legal guardian cannot write or is not met in person:

I, _____ (full name and title of the personnel) of _____ (RC/RC Movement component), confirm that the information regarding the processing, including transfer and/or publication, of personal data was explained to _____, the enquirer / legal guardian of the enquirer (circle) on _____ / _____ / _____ (date), in person / over the telephone (circle). I confirm that, in my opinion, s/he understood its content and provided his/her consent with the restrictions (if any) provided.

Signature of the personnel: _____

Date and place: _____

In the case of a **child** able to form her/his own views, indicate whether s/he agrees with the data processing to which the legal guardian consented:

- Fully agrees Disagrees

In case of disagreement, please specify and provide personnel's comments. (Personnel may need to do an assessment of the best interests of the child):

Signature of the personnel: _____

Date and place: _____