GUIDELINES

ICRC

PROTECTING PERSONAL DATA

WHEN WORKING WITH EXTERNAL SERVICE PROVIDERS

CONTENTS

1 OBJECTIVE OF THIS DOCUMENT

Protecting personal data[1] is an essential aspect of protecting peoples' lives, their physical and mental well-being and their dignity. It plays a role in all International Committee of the Red Cross activities, both operational and administrative. Data protection is therefore coming under increasing scrutiny, which means that the ICRC must assess possible data protection risks before deciding which external service providers (ESPs) we can work with, if cooperation with them will involve sharing and processing personal data.

This document will help delegations address the personal data protection issues that may arise when an ESP has access to personal data held by the ICRC.

For more information on these topics, please refer to the Handbook on Data Protection in Humanitarian Action, in particular Chapter 5 (Data Protection Impact Assessments (DPIAs)), Chapter 9 (Cash and Voucher Assistance), Chapter 12 (Mobile Messaging Apps) and Chapter 14 (Social Media).

2 DATA PROTECTION RISKS

The ICRC must abide by its Rules on Personal Data Protection ("the Rules") whenever it processes personal data. It may be difficult for delegations to ensure compliance with those Rules when we work with (or through) an ESP, because they will be subject to a different legal framework and their practices could cause the ICRC to indirectly violate its own obligations.

The staff member in charge[2] will need to answer the following question:

> "What are the risks for beneficiaries or other data subjects with regard to the protection of their personal data if we decide to work with or through this specific ESP?"

Working with or through an ESP usually requires them to access personal data otherwise processed solely by the ICRC, and this may lead to risks.

Those risks may fall into the following categories, among others:

- Risks related to interactions between the ESP and governmental authorities or armed groups: authorities may exercise undue pressure on the ESP, potentially jeopardizing our neutral, impartial, independent, humanitarian action (NIIHA) approach.
- Risks related to poor security, professional standards or ethical standards on the part of the ESP: an ESP may not be used to working with a humanitarian organization operating in conflict or other emergency settings. They may therefore be reluctant to adopt a flexible approach.
- The ESP may not have advisers with the appropriate legal or data protection expertise, which may slow negotiations down, making it less capable of responding to emergency situations.
- Finally, the ESP will often be a commercial or for-profit entity, which means that the data are no longer under a humanitarian organization's control once they have been transferred.

1 Personal data consist of any information relating to an identified or identifiable natural person. Examples include identifiers such as a name, audiovisual materials, an identification number, location data or an online identifier. Personal data may include information related to the physical, physiological, genetic, mental, economic, cultural or social identity of a data subject. This means that personal data go far beyond names. Aggregated data, as opposed to anonymous data, may still be "personal". Anonymization is the process of irreversibly altering personal data so that re-identification of individuals becomes impossible.

2 The "staff member in charge" is the colleague responsible for assessing the situation and the risks linked to the processing of the personal data. Depending on the scale of the project, this will be the coordinator, their deputy or the person supervising the project concerned.

ASSISTANCE PROGRAMMES, INCLUDING CASH AND VOUCHER ASSISTANCE (CVA)

The data processed make it possible to draw various inferences about people registered for a service, such as the fact that they belong to a specific vulnerable group, or their whereabouts.

The nature of some ESPs or of some projects may cause specific problems. For example, CVA at scale relies on technologies that may produce large amounts of metadata which, if misused, may put affected people at risk. In addition, financial service providers (FSPs), such as banks, generally have a legal obligation to screen their customers to ensure that they are not involved in money laundering, the financing of terrorism or other crimes, directly or indirectly. This contrasts with the humanitarian principle of selecting beneficiaries solely on the basis of need and requires the ICRC to maintain a precarious balance when we use FSPs, as they will be assessing beneficiaries in accordance with non-humanitarian criteria; should they find a person who has been blacklisted, they may have a legal obligation to report them to the authorities.

Our relationship of trust with beneficiaries is rooted in our NIIHA approach; involving third parties with different obligations could damage that relationship. Such a situation creates serious perception and security risks for us, as it might paint us as the "long arm" of a state or international entity.

USING AN ESP FOR THIRD-PARTY MONITORING

The ICRC will have to give the ESP information on the beneficiaries of the assistance, so that it can perform proper monitoring on our behalf. That information may be highly detailed.

In many cases, the ICRC will be using a third-party monitoring company because we have restricted or zero access to a specific zone. The ESP may have access to that zone because of their connections to certain groups who may have a specific interest in accessing beneficiary data. If we do not take the appropriate precautions, using an ESP may expose ICRC beneficiaries to increased risks (e.g. discrimination or targeting), should the ESP be pressured to disclose this information to authorities, or should the information be disclosed to the general public as a result of a data breach/poor security practices. That could have severe consequences, including damage to the reputation of the ICRC and a loss of trust in the organization.

RECRUITMENT

Where the ESP is a recruitment platform, job applicants may be asked to enter personal information and automatically share it with the ICRC, even if the ICRC does not actually need all the information.

Given the imbalance of power between a potential employer and an applicant, applicants may feel compelled to provide such information, believing that not sharing it might preclude them from getting the job. In some countries, for instance, applicants commonly record information such as their religious background, ethnicity or sexual orientation on national recruitment platforms. When they click "Apply", their entire file is transferred to the potential employer. As a result, the ICRC will acquire sensitive personal information that will require specific protection once in our system, even for applicants we have not short-listed.

WHAT STEPS SHOULD WE TAKE?

Every humanitarian organization must complete its due diligence.

For the ICRC, this means:

- determining the likelihood of the risk – how likely is the data to be compromised?
- determining the impact of the risk on the individual – how severe would the consequences be for the individual, and/or for the perception and acceptance of the ICRC by the population and the parties to the conflict?

The ICRC should then balance those risks against the benefits of processing, mitigate the risks to the extent possible and decide whether and how to cooperate with the ESP.

STEP 1 PERFORM A SITUATIONAL ANALYSIS AND SELECT PRIORITY POPULATIONS FOR DELEGATION ASSISTANCE

The starting point should always be a situational analysis and an assessment of which specific populations the delegation should prioritize for assistance.

Once that is clarified, one should examine the data protection risks of the proposed types of assistance and the potential involvement of ESPs. As part of the selection process for an ESP (such as during a call for tenders), one should gather information on their data protection practices and procedures, to assess whether and how to mitigate data protection risks. This will influence our choice of ESP.

Please see the ESP Questionnaire presented in an annex to these Guidelines, from which the relevant questions should be sent to potential ESPs for them to complete as part of the tender package.

It will also be necessary to perform a data protection context assessment (DPCA), to assess the risk level as regards the protection of personal data. The Data Protection Office (DPO) can provide a template for this.

The staff member in charge (usually the coordinator of the project) may convene a meeting with the relevant métiers and people to identify data protection risks that will require attention. Depending on the project concerned, these may include ICT, LOG, DPO, Protection, JurOp, FAD, HoSD/HoO, etc.

STEP 2 UNDERTAKE A DATA PROTECTION IMPACT ASSESSMENT

If the DPCA reveals that a certain operation is likely to involve specific risks to the rights and freedoms of the programme's target population, the staff member in charge should undertake a data protection impact assessment (DPIA).

This should take place when the ESP is identified as a potential partner to a project and before it starts providing services to the ICRC.

A DPIA describes the processing, assesses its necessity and proportionality and helps manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data, by assessing them and determining what measures should be taken to address them. The DPIA should be carried out prior to processing and should be seen as a decision-support tool regarding processing. It will help to identify privacy risks to individuals, identify data protection compliance liabilities for the ICRC, protect the ICRC's reputation and ensure that the organization does not compromise on the neutrality of its humanitarian action. Several meetings may be necessary to finalize a DPIA, depending on the points that need to be clarified.

The DPO (together with colleagues from other métiers) will fully support the staff member in charge during the DPIA.

A DPIA is a group exercise, involving the following activities:

- Identify data protection risks and mitigating measures.
- Eliminate as many areas of uncertainty as possible.
- Adapt/adjust implementation of the project.

Even though this is a group effort, ultimate responsibility and accountability for the mitigation and/or acceptance of the risks rests with the staff member in charge, as the person best acquainted with the context and its surrounding circumstances.

STEP 3 ADJUST THE PROJECT AND NEGOTIATE CONTRACT CLAUSES

Depending on the data protection risks identified, the ICRC may well need to adjust the project (or its implementation) and negotiate with the ESP to include specific clauses in the contract.

Of course, the mere signing of a document will not guarantee that all aspects of a problem are solved, but a contract that contains the necessary data protection clauses is mandatory nonetheless.

There is no one-size-fits-all "template" contract or clause – the DPO and the Office of Corporate Legal Affairs will adjust the wording to ensure that it addresses the data protection risks identified for the situation at hand (during Steps 1 and 2) in an optimum fashion.

STEP 4 ENSURE RESPECT FOR THE RIGHTS OF THE DATA SUBJECTS

With the support of the DPO, the staff member in charge will ensure that the rights of the data subjects are respected throughout the life of the project, in accordance with the ICRC Rules. This is mandatory even if no DPIA is necessary.

This step will include ensuring that data subjects are told which of their data may be shared with an ESP and, when relevant, that their informed consent is required. The staff member in charge and the DPO will discuss the best way of ensuring transparency towards data subjects. In some cases, it will be necessary to draft information notices and consent forms (with full support from the DPO), whereas in other cases written documents and the collection of signatures may be neither appropriate nor possible.

STEP 5 REVIEW THE PROCESS AND DOCUMENT CHANGES

It will be necessary to review the process and document any changes under the following circumstances:

- Processing is extended (new functionality, new service, new ESP operating model allowing for new capabilities, etc.).
- The situation changes substantially (e.g. the ESP's connections with authorities/armed groups change, new risks emerge and affect the need to enhance the confidentiality of our work, the ICRC decides to work with another ESP, etc.).

When looking at the risks identified earlier, the staff member in charge should ask themselves the following questions:

- Is this still possible?
- Is it more likely?
- Would it have a bigger impact than before?

They must also investigate whether new risks have emerged, working in consultation with the DPO and any other relevant métiers.[3]

3 QUESTIONS TO ASK IN ORDER TO ASSESS THE DATA PROTECTION RISKS ASSOCIATED WITH AN ESP

To identify and address the risks, the staff member in charge (usually with the support of Logistics) will decide how and when to start discussing data protection with the ESP – ideally prior to the conclusion of any contract.

This will depend on how familiar the ESP is with the issue, whether they have an in-house lawyer, how easy it is to arrange in-person meetings, language issues, etc. The DPO and Procurement can help colleagues navigate those challenges and decide how best to organize discussions with an ESP. Please see below for recommendations and examples of questions that may help the staff member in charge to assess the situation and identify the most prevalent data protection risks. However, this should not be a box-ticking exercise, and these specific questions are examples or suggestions. Understanding the specific context, the concerns of the affected population and the relevant risks is the most important part of the risk identification process. The staff member in charge must identify the relevant questions (during Steps 1 and 2 above) and ask for clarification where answers are not satisfactory.

To help collect the information covered by the questions below, the DPO has created an interactive Excel questionnaire, which is explained in an annex to these Guidelines.

The questionnaire:

- guides staff through these questions
- links the information they gather from the suppliers (see Step 1 above) to the risks highlighted in this document
- indicates the mitigation measures that would be most effective for each specific ESP.

The questionnaire may not always be the best tool for the job. The staff member in charge is therefore encouraged to seek the advice of the DPO before or during any interaction with an ESP (for example during a call for tenders), to help them with the selection process.

If the delegation does decide to use the ESP Questionnaire, it will be necessary to extract the relevant questions from it and incorporate them in the call for tenders, to ensure that the delegation has the information needed for the assessment. The results of the analysis can then be fed into the data protection section of the selection table for the ESP.

Legal/contractual questions

- Does the ESP have any confidentiality/data protection rules, SoPs or internal rules/regulations regarding the processing and security of personal data?

This includes checking whether the ESP's internal maintenance and IT support are up to ICRC standards and whether they are certified to the relevant IT and cybersecurity standards, such as ISO 31700 or 27001. Although these standards do not constitute an automatic advantage for an ESP, they are a good indicator of its posture on risk management.

- Would the ESP agree to use ICRC contract templates and clauses?

While the ICRC has a series of model clauses for contracts, regulating data sharing with ESPs, the latter often have their own contract templates, which frequently contradict ours. If an ESP refuses to adopt the ICRC clauses – or agrees to sign them without being willing or able to comply with them – colleagues will have to assess the risk of the ICRC Rules being breached, and what recourse we would have if any.

Process/service questions

- What personal data will the ESP need to provide the service?
- Does the ESP seem to be asking for more data than would be necessary to provide the service?
- What are the ESP's data flows?
- Where does the ESP store data?
- Who has access rights internally?

- Does the ESP have an obligation to screen beneficiaries of the services?

In the case of FSPs, for instance, "beneficiaries" would be the people receiving ICRC assistance or funds.

- Does the FSP have a legal obligation to share the personal data of data subjects with authorities/public services/central bank/judicial mechanisms/etc. in case of a match?
- If screening is carried out, who would the ESP consider their "beneficiary/client"?
- In the case of FSPs, for instance, would this be the ICRC or those receiving financial support from the ICRC through their services? In other words, would screening (if any) apply only to the ICRC as the main client, or also to the beneficiaries?
- Does the ESP share any of this personal data with third parties as part of the provision of services?

3 For further guidance on these issues, please see the ICRC Handbook on Data Protection in Humanitarian Action, Chapter 6 (Designing for Data Protection) and Chapter 5 (Data Protection Impact Assessment).

- If so, which third party/parties (including their location) and for what purpose(s)?

We must understand how and where the personal data of data subjects will end up being "processed" (i.e. stored, secured, accessed/shared both internally and externally, etc.).

- Will the data be used for any purpose other than to provide the service (e.g. marketing or research)?

If so, the ICRC will need to understand this better, and will need to know whether additional information may be required for such processing operations, and whether such additional purposes are optional.

- How does the ESP handle complaints from clients/users regarding the security of their personal data?

Organizational questions

- In which country is the ESP registered?
- Is the ESP a subsidiary of a larger/parent company (specifically in Australia, China, the UK or the USA)?
- If so, what is the name of that company?

- Would the mother company and/or other affiliates of the same group have the legal right and/or technical ability to access data shared by the ICRC?

The ESP may be affiliated to a company with which the ICRC would not want to have any connection.

- How long would it take the ESP to notify the ICRC in case of a data breach? Precedents?
- What procedure will be followed in case of a data access/disclosure request from a national authority (e.g. law enforcement)?

Technical questions

- Where are the data hosted, including back-ups?
- Does the ESP use cloud services, and if so, which?
- How does the ESP secure the data?
- Are the data encrypted at rest and in transit?
- Who manages the encryption keys?
- If the ESP stores, manages and/or maintains the data, does it use role-based access control and manage access to the data on a strict "need-to-know" basis?

Further questions that may be relevant to our analysis of the environment

- What would be the impact of a data subject not wishing to have their personal data shared with the ESP? For example, if the ICRC uses an FSP for CVA, can we ensure that beneficiaries can access the same assistance through different means? In other words, do beneficiaries really have a choice if we seek their consent to share their data with an external service provider?
- Taking into account local digital literacy levels and the complexity of the particular ESP, will the beneficiaries be able to fully understand the risks involved in providing their data to the ESP?

- Do the data subjects already use the services of the ESP?

For example, in some countries, it is common practice for job applicants to use a platform where their CV is already registered.

- If the ICRC plans to provide CVA through an FSP, are beneficiaries already clients of that FSP (which would mean they had already provided their personal data to it)?
- If not, why not?

ASKING THE QUESTIONS AND ANALYSING THE ANSWERS

This is not a mere box-ticking exercise. Colleagues should decide how to best collect answers to these questions. It may be worth sharing them with the ESP before a meeting to help them prepare, but in any case, answers should be discussed to ensure that the ICRC fully understands the situation, and they are likely to raise additional questions. The answers should be assessed by the relevant métiers, and the staff member in charge should ensure that they have collected all the information they need to take an informed decision as to whether the ICRC should work with a particular ESP, and to take any possible mitigating measures.

4 MITIGATING MEASURES

It will only be possible to identify mitigating measures if one has properly assessed the data protection risks.

The points below are therefore illustrations of what may be possible and recommended in certain situations. They are not a "one-size-fits-all" solution.

TECHNICAL MITIGATING MEASURES

- Whenever possible, exchange personal data with the ESP only through secure, ICRC-approved applications and tools (e.g. ICRC iTransfer). This minimizes security risks to personal data during the actual transfer.
- If possible, coordinate with ICT to ensure that the ESP's technical setup can guarantee an adequate security level for personal data provided by the ICRC.
- If the ESP will be collecting personal data on behalf of the ICRC, ensure that they use ICRC-approved tools whenever feasible.
- Ask whether any optional processing operations or functionalities offered by the ESP (e.g. marketing operations or enhanced data analytics capabilities) that are not necessary for the provision of the ICRC services can be blocked/excluded by technical means.
- Ensure that the ESP provides adequate internal maintenance and IT support.
- Move from identification to authentication or authorization.[4]

  When setting up a humanitarian project, what matters is that, upon distribution, each person receives what they are entitled to as per the needs assessment. In some cases, it may be important to identify the beneficiary during the needs assessment, but at a later stage, those in charge of delivering the assistance often need to simply authenticate or authorize the beneficiary rather than identify them.

  Possible ways of authenticating or authorizing beneficiaries:

  - **ICRC ID:** Some ESPs have agreed to use an ICRC-issued ID instead of a state-issued one. An ICRC-issued ID may include a limited quantity of information, depending on the situation, and only the ICRC can link the ID to the person's actual identity. In such a system, an ICRC ID can be issued showing only a serial or card number, with no other information. The ICRC maintains complete control over the list showing which person corresponds to which ID number.

    While this ensures data minimization, it does require specific technical systems for issuing such IDs and might prove time consuming, as programmes will need more time to register people and assign numbers.

4 **Identification** means answering the question "Who is this person?". It often requires looking up a particular individual in a database or dataset using a subset of information registered for them, such as their name or identifier.
Authentication means answering the question "Is this person who they say they are?", which is a simpler process than identification, as it involves a one-to-one comparison between the data provided as a claim and what is recorded in the system.
Authorization means granting access based on some criteria such as a positive authentication, possessing a token or knowing a specific password/passphrase.

- **Token:** Beneficiaries are registered and assigned a token bearing a number. The beneficiary collects cash from the ESP upon presentation of the token, which forms a means of identification.

In both of the above cases, the ESP submits a final report to the ICRC after the distribution, listing the card numbers of people who have availed themselves of the assistance. In a token-based system, the ESP collects the tokens as proof of receipt and submits them to the ICRC with the final distribution reports.

ORGANIZATIONAL MITIGATING MEASURES

- Ensure that the ICRC has control over what personal data must be processed, thereby limiting the leeway enjoyed by the ESP.
- For instance, if the ESP is involved in needs assessments or monitoring activities, ensure that all surveys/questionnaires are exclusively drafted by the ICRC and that the ESP has no opportunity to collect additional data.
- Discuss access-rights management with the ESP, i.e. who within the ESP will have access to what personal data. Any access to personal data shared by the ICRC should be on a strict need-to-know basis.
- Ensure that data subjects are fully informed as to how the ICRC – and any additional ESP – may process their personal data. This is usually done through an information notice. The DPO can provide a template, plus help with contextualizing such a document and deciding how best to disseminate this information.

CONTRACTUAL MITIGATING MEASURES

- Ensure that the agreement with the ESP contains appropriate clauses governing the onward transfer of personal data. The content of such clauses will vary depending on the situation and the specific activity. Ideally, any further transfer of personal data should take place only with the prior written agreement of the ICRC. Such safeguards can be implemented through a combination of both data protection and confidentiality clauses, which the DPO will help draft.
- Identify any other third parties (in addition to the ESP) that may have access to the personal data the ICRC supplies. Ideally, all such third parties should be listed in the agreement.
- Ensure that the agreement with the ESP contains clear instructions and sets out a specific course of action to take if authorities ask the ESP to disclose personal data provided by the ICRC (e.g. in the context of legal proceedings). The content of such clauses, and the level of protection that can be ensured, will depend on the context, including any privileges and immunities that the ICRC enjoys.
- Include in the agreement with the ESP an explicit obligation to ensure an adequate level of security for personal data communicated by the ICRC.
- Contractually limit the purpose(s) for which personal data communicated by the ICRC may be used. Ensure that the contract prohibits any purpose that is not necessary for the actual delivery of ICRC operations.
- Clearly set out in the agreement with the ESP exactly what personal data they will need to process in order to provide the contracted services to the ICRC. The list should be as exhaustive as possible.
- Use ICRC template contracts whenever possible.

The ESP may not be familiar with the clauses that the ICRC suggests and may therefore be reluctant to accept them. If the ICRC cannot use its own template but needs to review the ESP's contractual documents, ensure that those documents address all of the points above, in consultation with the DPO.

In some contexts, there may only be one ESP capable of providing services to the ICRC, in which case the ICRC's negotiating power may be severely limited.

MITIGATING MEASURES FOR FINANCIAL SERVICE PROVIDERS

Counter-terrorism measures and sanctions lists

Many FSPs are subject to Know Your Customer (KYC) regulations, which require them to collect information about their customers to prevent money laundering, the financing of terrorism or other crimes. The amount of information required may depend on local regulations, with some countries allowing greater flexibility based on what they see as the level of risk related to the transactions.

The ICRC should examine the relevant KYC regulations of the operating context, determine what data the law requires and cross check that against what the FSP is requesting. This analysis should include both the law and actual practice/judicial precedents. An FSP's internal policies may prompt it to ask for data additional to those that the law requires. If they do, they must put forward justification for this and the ICRC should negotiate with them to ensure that we supply only such data as are strictly necessary to provide assistance.

In any case, the ICRC should:

- Ask the FSP during the tendering process against which sanctions lists it checks individuals (UN, national, both, other).
- Undertake specific context assessments during programme design and implementation, to gain a better understanding of which target populations should not undergo beneficiary screening because they would be at high risk.
- Ensure that there are alternative means of providing assistance to specific individuals, in the light of the above assessment, such as cash-in-envelope and/or in-kind equivalents.

Virtual accounts

One option is for the ICRC to own and manage virtual accounts.

This involves the ICRC creating create sub-accounts for beneficiaries, to allow them to receive cash. That approach has the advantage of generally requiring us to provide less personal information to FSPs, as the FSP conducts its checks not on individual beneficiaries, but on the ICRC (Know Your Business rather than KYC). While attractive from a data protection perspective, virtual accounts do come with their own issues, such as whether the ICRC has the capacity to manage these accounts and the fact that the ICRC would be able to access information as to how people are using their cash, which may pose a risk in terms of data minimization.

Examples of using virtual accounts:

- Issuing prepaid ATM cards, where each card is linked to the National Society's account and given to people with a PIN that they use to withdraw cash.
- Issuing bank cheques that people can cash at a bank whether or not they have an account there.
- Issuing limited-use mobile SIMs so people can receive an SMS with a transaction code, with which they can collect cash from a mobile money agent.

Other distribution options

Where screening against counter-terrorism provisions and sanctions lists may put some beneficiaries at risk, and the ICRC would be unable to contract an ESP without providing beneficiary data, we will need to consider other distribution options, such as cash in envelopes, vouchers or even payments in kind.

MITIGATING MEASURES WHERE THE ICRC USES A THIRD PARTY FOR POST-DISTRIBUTION MONITORING

ICRC-managed tools

Train the ESP to use ICRC-managed tools and, if possible/relevant, provide them with ICRC devices, so that the ICRC keeps control of the data flow and ensures data are stored safely.

Solid contractual requirements
Ensure that contracts with third-party monitoring entities include adequate clauses regarding confidentiality and data protection obligations, including clear instructions on how to manage data breaches. Please refer to the DPO and the REM Clearing House on these matters.

MITIGATING MEASURES WHERE THE ICRC INITIATES A RECRUITMENT PROCESS THROUGH AN EXTERNAL COMPANY

Adapt the contract
Minimize the information the ICRC receives via the ESP, ensuring we do not necessarily receive all the information that an applicant enters into the system.

Provide alternative ways of applying for a job
Ask people to apply by email rather than through the ESP.
Clearly state in the job ad the information that applicants should send at the first stage of the recruitment process.

Delete
Ensure that all applications not short-listed are immediately deleted.

If specific information cannot be deleted from an application, contact short-listed applicants and ask them to re-submit their application with only the requested information.

5 IN CONCLUSION

- There is no such thing as risk-free data processing and we may have to make difficult choices to achieve our objectives.
- What is fundamental from an accountability perspective is that risks and mitigation measures be properly documented and, in the case of substantial or disputed risks that cannot be mitigated, decisions be taken and documented at the appropriate level of seniority.
- The DPO can help ensure that risks are properly managed and documented.
- Decisions on risk management must be taken mindfully and based on each country or population group, as the severity of impact may be context-specific.
- Affected people must have the option of opting out of providing personal data (biometric or otherwise) without prejudice to their access to essential assistance.
- Every time we choose to provide assistance through an FSP (e.g. in the form of digital payments) we must ask ourselves whether the planned mitigation measures will ensure that the advantages outweigh the risks.

ADDITIONAL READING

- ICRC, Cash Transfer Programming in Armed Conflict: The ICRC's Experience, ICRC, Geneva, November 2018: http://www.icrc.org/en/%20publication/cash-transfer-programming-armed-conflict-icrcs-experience
- ICRC, Digital Dilemmas Dialogue #2.1: A Humanitarian Look at Assistance Programming and Social Protection Systems, ICRC, Geneva, 17 February 2021: https://www.icrc.org/en/digitharium/digital-dilemmas-dialogue-2
- ICRC, Handbook on Data Protection in Humanitarian Action, ICRC, Geneva, November 2024: https://www.icrc.org/en/data-protection-humanitarian-action-handbook
- IFRC, Practical Guidance for Data Protection in Cash and Voucher Assistance, A supplement to the Cash in Emergencies Toolkit, IFRC, January 2022: https://www.ifrc.org/document/practical-guidance-data-protection-cash-and-voucher-assistance
- Privacy International, ICRC, The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era, October 2018: https://www.icrc.org/sites/default/files/document/file_list/the_humanitarian_metadata_problem_-_icrc_and_privacy_international.pdf
- Burton, Jo, "'Doing no harm in the digital age': What the digitalization of cash means for humanitarian action", International Review of the Red Cross, No. 913, 2020, pp. 43–73: https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/doing-no-harm-digitalization-of-cash-humanitarian-action-913.pdf

ANNEX

STEP-BY-STEP GUIDE TO USING THE ESP QUESTIONNAIRE

The questionnaire is available online.

1. Read the Read Me Guide tab.
2. Send the questions in the Discovery tab (Rows 2-20) to the ESPs. Questions 16, 18 and 19 are more directed towards ICRC staff, while the others are to be addressed directly to the ESP.
3. Fill in the ESP's answers in the spreadsheet: one column per ESP.
4. Compare their risk scores (Discovery tab, Rows 22-26).
5. Consider these scores part of the selection criteria for the ESP. In the case of a tender process for an FSP, use the information to answer the data protection question in the selection table.
6. Having made a pre-selection, navigate to the **Mitigation measures** tab, where you can explore the potential measures that you should negotiate with the pre-selected ESP in order to reduce the risk. These measures are also shown in the tab, to indicate their importance for the given ESP.

Additionally, staff can use the word version of the ESP Questionnaire and distribute it to bidders during the tender process to collect the relevant responses.

In case of problems accessing the questionnaire and for any questions about how to use it, please contact the DPO via dpo@icrc.org.

The ICRC helps people around the world affected by armed conflict and other violence, doing everything it can to protect their lives and dignity and to relieve their suffering, often with its Red Cross and Red Crescent partners. The organization also seeks to prevent hardship by promoting and strengthening humanitarian law and championing universal humanitarian principles.

ICRC

International Committee of the Red Cross
19, avenue de la Paix
1202 Geneva, Switzerland
T +41 22 734 60 01
shop.icrc.org

www.icrc.org
facebook.com/icrc
x.com/icrc
instagram.com/icrc

4857/002 02.2025