



## Guidance Note on Data Protection

After extensive internal consultation and research on the data protection standards of our peers, we are pleased to present the IFRC Policy on the Protection of Personal Data, or just the Data Protection Policy (the IFRC Policy). The IFRC Policy, which applies to all offices of the IFRC, is aligned with the generally-accepted best practices in data protection. It is available in English French, Spanish and Arabic.

### Why have a Policy?

The IFRC, as an international organization (IO), is not subject to national law (including data protection laws, such as the European General Data Protection Regulation, which came into force in May 2018). Instead, IO's, such as the IFRC, are bound by their own internal data protection standards. It is crucial that the IFRC have its own such standards.

As a humanitarian organization, the IFRC collects, stores, shares, analyzes and publishes a significant amount of information about individuals (staff, donors, partners, affected persons, and others). When that information (some of which can be considered as highly sensitive) can lead to the identification of an individual, it is called personal data, and thus falls within the scope of the IFRC's new policy.

Prioritizing data protection is already a part of the IFRC's work. Staff recognize the need to obtain consent, provide individuals with information about what personal data is being collected and why, and that the programs and partners we use must be evaluated to ensure that they also employ appropriate safeguards. However, until now, there has not been structured guidance on how to apply these ideas, and such practices have not always been consistently applied. Given the importance of protecting personal data and that harm that may come from failing to do so, it is crucially important, from a humanitarian perspective, and also from a reputational one, that the IFRC implements a formal set of practices to ensure the protection of personal data.

It is also important to consider that while the IFRC is not subject to data protection laws, at country level, many of our partners, be they National Societies or private entities, will be subject to some data protection legislation that may prohibit the free sharing of personal data with the IFRC. In order to prevent any interruption in the services we provide and to be able to provide our partners with assurance that data transferred to us will be handled properly, a robust policy is necessary.

### Overview of the IFRC Policy

At a high level, the IFRC Policy requires that personal data be treated according to the following principles:

1. There must be a legitimate basis for personal data collection and processing.
2. Personal data should only be used for the purpose(s) for which it was originally collected.
3. The collection of personal data should be limited to what is strictly necessary to fulfill the original purpose(s). Do not collect more than needed because you think it might be useful later.
4. Personal data should not be kept longer than necessary; it should be deleted once the original purpose has been fulfilled.
5. Personal data should be kept secure (technically, physically and organizationally) so as to prevent any unauthorized access to, disclosure, destruction or modification of the data.



The IFRC Policy also introduces generally-accepted data subject rights, as follows:

1. Individuals should have the right to know what personal data is being collected on them, why it is being collected and how it has been, is being or will be used.
2. Individuals should further have the right to verify the accuracy of that data and to make any needed corrections or deletions.
3. Individuals should have the right to object to any processing and/or withdraw any consent that had been given.
4. Individuals may request the deletion of all, or part of the personal data held by the IFRC.

It is important to note that these rights are not absolute, and that the granting of any or all of them must be weighed against other interests. For instance, a retired staff member's request to have his or her personnel file deleted would likely be granted, while a current staff member's request could not be – the IFRC needs certain information to be able to pay staff and accurately calculate benefits. Such requests may now be directed to a newly created email address: [dataprotection@ifrc.org](mailto:dataprotection@ifrc.org).

As additional data protection guidance is developed and rolled out, you can help the IFRC and the individuals it serves by keeping the following questions in mind:

1. What is the legitimate basis for collecting and using personal data?
2. What data do I really need for my project?
3. Could the personal data put anyone at risk? For example, location information of a refugee that does not want to be tracked by his or her country of origin, or an HIV positive individual in a community where such status is highly stigmatizing.
4. How will the data be stored, accessed and shared?
5. What parties must have access to the personal data, and on what basis?
6. How long must the data be stored (consider practical, audit and legal requirements) and do we have a mechanism for identifying and deleting it when it is no longer needed?

As you review these questions, do not hesitate to ask your supervisor for guidance. If he or she does not know the answer, they will know that they can escalate the matter to the Legal Affairs Department.

### Next Steps

The IFRC Policy is just one piece of the IFRC's data protection puzzle among many to come. Additional tools will be developed in order make the implementation of the IFRC Policy as simple and effective as possible. While additional guidance is being developed,<sup>1</sup> your work should not be drastically affected. The first changes will be to standard templates, consent forms and privacy policies. These will be updated to ensure that they provide more accurate and relevant information to individuals. The Legal Affairs Department will continue to work closely with IT and Data Literacy colleagues in the development of these tools and any associated guidance. It should be noted that the Legal Affairs Department now includes a Senior Legal Adviser serving as the Data Protection Officer (DPO).

---

<sup>1</sup> Please also consult the following policies that outline data (including personal data) handling: Information Management Policy, Information Classification Standard, and ICT Security Policy.



International Federation of Red Cross and Red Crescent Societies  
Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge  
Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja  
الاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر

Finally, please be aware that, according to the IFRC Policy, there are new requirements to be fulfilled when sharing personal data outside the IFRC. As most contracts/agreements the IFRC enters into will involve personal data in some respect, you should liaise with the Legal Affairs Department to get the appropriate data protection clauses put into the agreement. In order to ensure familiarity with the IFRC Policy and its consistent application throughout the organization, in 2019, the DPO will meet with the regional data focal points and conduct data protection sessions in each regional office.