Data Protection Statement related to procurements, partnerships and grants

The International Federation of Red Cross and Red Crescent Societies (IFRC) is the world's largest humanitarian network. IFRC supports local Red Cross and Red Crescent action in more than 191 countries, bringing together almost 14 million volunteers for the good of humanity. It is therefore essential that our actions, and those of our partners, related to data protection are transparent.

This Statement seeks to provide procedures, protocols, and safeguards with respect to receipt, handling / processing of any personal data from grant applicants and other individual or business bidders related to the procurement of goods and services. Additionally, this Statement outlines IFRC's expectation that these parties be able to adequately protect personal data that they process. It is expected that all bidders/applicants are able to provide evidence of their ability to protect personal data.

1. Why does the IFRC process personal data of grant applicants and other bidders?

In order to carry out IFRC's humanitarian mandate, it is essential to have sufficient information to allow for communication with the relevant individuals and to verify qualifications and other eligibility criteria, as part of our robust due diligence. IFRC may process your personal data to ensure the following:

1. that the prospective partner has the resources available (technical, financial, and professional) to fulfil its relevant obligations;
2. that its activities are not misaligned with IFRC's humanitarian mandate;
3. that there are no legal or other restrictions on its staff or operations that may interfere with the awarding or fulfillment of the agreement ***("agreement" is used throughout this Statement for simplicity, it should be interpreted to also include projects, grants or other contracts)***;
4. that it meets any internal eligibility requirements; and
5. that there are no real or apparent conflicts of interest or other risks that could interfere with the fulfillment of the agreement, harm the reputation of the IFRC and/or cause harm to the populations IFRC serves.

With regard to successful applicants/bidders, IFRC will additionally process personal data in order to:

1. facilitate the coordination of work internally and with other partners (including governmental entities, where relevant);
2. monitor implementation of the agreement;
3. provide any necessary training or technical assistance;
4. verify ongoing alignment with the Fundamental Principles and compliance with internal audit, archiving, finance, legal, and IFRC policy requirements;

5. maintain a register of partners, their activities, any respective violations of policy or other applicable requirements;

6. prevent, detect, and address any data breach;

7. research and provide learning to improve IFRC's processes; and

8. report (including by publication and/or bilaterally with donors including governmental entities) on elements of the agreement for transparency purposes or in order to satisfy other applicable requirements. For instance, the information to be reported may include: the name of your entity, the general geographic location of the entity and/or where the services are to be performed, the amount of the agreement, and the nature and purpose of the agreement.

2. What personal data will be collected

A. The following is typically required in order to fulfill the above purposes:

Full name (and/or names of entity board members or other senior management); gender; salutation; business email and local address; phone number(s); title; nationality

B. Depending on the type of agreement, the relevant legal jurisdiction(s), and the nature of the goods or services to be provided, the following personal data may also be required:

Birthdate, business or personal license number; relevant banking, insurance and/or other business-related information; a copy of a passport and/or national identity document; proof of health insurance

Although IFRC typically processes personal data obtained directly from you, there may be cases where it obtains your personal data from third parties and/or resulting from research undertaken as part of its due diligence. Please note that additional (generally considered *non-personal*) information will likely also be necessary; this section only details relevant *personal data.*

IFRC Processors:

The information identified above will typically be submitted to the IFRC through its procurement portal (at IFRC.org) or through email. Accordingly, the information will be transmitted over the internet and processed by our trusted service providers, such as Microsoft. Third-party service providers will have their own privacy policies, which you are encouraged to review.

3. Legitimate bases for personal data processing

The IFRC considers that the collection and processing of personal data as outlined above is necessary for one or more of the following legitimate bases: 1) it is in the IFRC's legitimate interest, 2) for the fulfillment of the agreement, 3) for the establishment or defense of a legal claim (including with respect to IFRC's internal legal complaint and compliance mechanisms, including for audits and/or investigations), and 4) where IFRC is subject to a legal obligation.

4. How long will my personal data be kept?

Information and documentation received before and after contracting may contain personal data. Relevant information and documentation may be entered into IFRC's supplier registry and will be retained for audit, project management, archiving and other business needs in accordance with

IFRC's data retention policies, and otherwise only as long as necessary to fulfill the specified purpose(s).

5. Additional information on how your personal data is protected

IFRC treats personal data according to its binding Policy on the Protection of Personal Data (which can be found here). Specific technical measures implemented to protect your personal data from unauthorized or accidental use, access, loss or alteration include password protected databases with access restrictions applied based on user roles. Access is monitored and logs are maintained. IFRC's IT infrastructure is mainly provided/hosted by Microsoft Azure.

6. For any questions about your personal data?

Should you have questions about IFRC's processing of your personal data or to make a request to correct or delete certain data, please contact dataprotection@ifrc.org. Please note that any request must comply with the steps outlined in the IFRC's Policy on the Protection of Personal Data and will be subject to identity verification. Certain requests may not be approved, as further outlined in Section 3 of the IFRC's Policy on the Protection of Personal Data.

7. Expectations of successful applicants/bidders

In general, you are expected to treat any personal data that you process as a result of the applicable agreement in compliance with applicable data protection and privacy laws. In the event that there are no applicable laws in the country (or countries) of performance of the agreement, then IFRC's Policy on the Protection of Personal Data shall serve as the outline for your obligations. Those obligations include, but are not limited to:

1. Personal data may only be used for the purposes of fulfilling this agreement, and more generally according to instructions of IFRC when it acts as the Data Controller;

2. A legal/legitimate basis (or bases) shall be identified for all processing operations;

3. Understanding that screening against sanctions lists (or similar) of specific individuals in need of humanitarian assistance ("persons in need", sometimes referred to as "final beneficiaries") is neither required for the provision of humanitarian services, nor is compatible with humanitarian principles, you shall inform IFRC during the tender process (or otherwise as early as possible, and **in any case before conducting any screening**):

    a) whether you consider that you are required to screen persons in need (identifying the specific legal provision(s) requiring this);

    b) which data will be used for screening;

    c) which lists will be used;

    d) how data related to matches or possible matches will be handled and/or shared; and

    e) how your services to a person in need, who may be present on a sanctions list (or similar) may be affected.

4. Personal data processing shall only be done so far as the data used and the means of processing consider the principles of proportionality, data accuracy and minimization;

5. You shall ensure (where you act as a Data Controller), that adequate and understandable information about personal data processing and any related rights shall be provided to data subjects. It is further understood that you shall provide specific information about processing operations related to law enforcement and/or screening against any sanctions list (such information shall minimally include that referenced in 7(3) above);

6. You shall implement sufficient physical, organizational and technical safeguards to prevent the unauthorized alteration or loss of, or access to the personal data;

7. Where a third party (including any government) has requested personal data related to the agreement, you shall promptly inform the IFRC in advance of providing the requested data in order to allow for the assertion of any privileges and immunities or other legal mechanisms that may protect all or part of the data from disclosure;

8. Except as strictly necessary for to fulfil the specified purpose(s) of the agreement, you shall not undertake any onward transfer or sharing of the personal data to third parties without the IFRC's express agreement;

9. You shall not subcontract any part of the work involving the processing of personal data without the IFRC's express agreement and ensuring appropriate protections are in place;

10. If you experience (or reasonably suspect) any security incident (personal data breach) in relation to this agreement, you shall promptly provide the IFRC with information on the nature of the incident, its likely consequences and the steps taken or proposed to be taken to address the incident;

11. You shall not maintain personal data any longer than necessary;

12. You agree to provide the IFRC, when necessary, reasonable, and in accordance with applicable data protection laws and/or internally binding policies, with information (including where necessary personal data) needed for the purposes of 1) demonstrating compliance with data protection obligations, 2) establishing or defending legal claims, 3), complying with contractual or legal obligations, 4) archiving, and 5) research and/or auditability. Such provision of information shall always be balanced against the rights of and the possible risks to data subjects.

13. **In the event that you (or your contracted partner or agent) process any Credit Cardholder data as part of the fulfilment of the agreement, you shall be able to demonstrate continued compliance with Payment Card Industry (PCI) standards.**

8. Privileges and immunities

Nothing in or related to this Statement shall be construed as a waiver, express or implied, of IFRC's privileges and immunities.

V1.1 September 2023