Data Privacy Policy

Document Governance

Function Owner	Department	Content Review Cycle	Date Last Revised
Vice President, Risk Management & Compliance	Risk Management & Compliance	Annually	8/10/2023

Copyright © 2023 CRDF Global
The information contained herein is confidential and proprietary, and for internal use by CRDF Global. This document may not be reproduced or distributed in whole or in part without the written permission of CRDF Global.
Hardcopies of this document can be printed for immediate use only and should not be kept or stored for future use.

1. Policy Statement

CRDF Global solicits, collects, uses, shares, and stores information about individuals, contractors, partners, and other third parties. This information is subject to legal requirements, and CRDF Global is dedicated to ensuring all Personal Data is managed in a responsible and secure manner. CRDF Global will only use Personal Data when it has a valid and legal reason to do so.

Personal Data can encompass a wide variety of information and is subject to a wide array of local, federal, and national laws in many countries. Given the complexity of the various regulations and the global scope of our activities, CRDF Global will follow the European General Data Protection Regulation (GDPR) as our standard of compliance in the handling of Personal Data. All staff will comply with CRDF Global guidelines when soliciting, collecting, sharing, managing, and storing Personal Data.

CRDF Global shall comply with the General Data Protection Regulation (GDPR), which governs data protection and privacy in the European Union and European Economic Area and addresses transfer of personal data outside these areas and with all applicable federal and local regulations.

As a Controller of Personal Data, we have certain obligations under the GDPR as to how we handle and use that data. In particular, we shall comply with the following principles when collecting, handling and using Personal Data:

- **Lawfulness** – We will have a lawful basis for collecting and using Personal Data.
- **Transparency** – We will provide the individual whose Personal Data is collected with specific details about why their information is being collected as well as how it will be used, disseminated, and stored.
- **Fairness** – We will process Personal Data in a way that is fair to individuals and will only process their Personal Data in a way that people would expect and/or be able to justify any unexpected processing or adverse impact on individuals.
- **Consent** – Consent is of utmost importance to CRDF Global. Where we rely on consent as an appropriate lawful basis, the Data Subject must explicitly and intentionally authorize the collection, use, and storage of their Personal Data for specific purposes. The Data Subject is able to withdraw their consent at any time, and we will comply with their request to withdraw their consent.

- **Purpose Limitation** – We will collect Personal Data for a specified, explicit, and legitimate purpose and not further process the data in a way that is incompatible with that purpose.

- **Accuracy –** We will collect Personal Data in a manner that ensures its accuracy and relevance to the purposes for which it is collected. Data Subjects will be encouraged to inform us if their details change, so that we can keep these up to date as necessary.

- **Data Minimization –** We will collect only the minimum Personal Data needed for a specific purpose. We will not collect unnecessary Personal Data.

- **Data Integrity and Security** – We will always take appropriate steps to protect Personal Data. In particular, personal data shall only be collected, transmitted, and stored utilizing authorized CRDF Global IT Business Systems and in a secure manner. Further, access to Personal Data will be limited to staff members with legitimate need to access the information to perform their roles and accomplish the approved business purpose.

- **Accountability** – We will comply with data protection legislation (including the GDPR) and be able to demonstrate our compliance through the implementation of documented policies and procedures.

- **Storage Limitation** – We will only retain Personal for the use and purpose for which it was collected. The starting position is that the Personal Data should not be retained or used for any other purpose.

- **Data Breaches** – Any suspected unauthorized use, disclosure of, or access to Personal Data must be reported immediately to both the Risk Management & Compliance Department and to the Information Technology Department in accordance with the IT Incident Response policy and associated procedures.

- **Data Subject Rights Requests** – We will be able to recognize a Data Subject Rights Request and the procedures that must be followed when we receive one – these rights are not absolute (and just because an individual has raised these rights does not mean that CRDF Global must comply with them).We will respond to them appropriately and within the timelines set out in the GDPR (usually within a month of receipt). If anyone receives a Data Subject Rights Request from an individual, he/she must notify the Privacy Officer as soon as possible.

- **Disclosing to Processors** – Where we engage Processors to process Personal Data on our behalf, we will ensure that a contract is in place with that Processor which contains appropriate terms. Prior to contracting with or utilizing a Processor we shall ensure that our Processors have implemented appropriate technical and organizational measures, to ensure a level of security appropriate to the risk posed by the processing.

- **Disclosing to Controllers** – Where we disclose Personal Data to other controllers, we will have appropriate agreements in place with the receiving entity ensuring effective compliance with this policy.

- **International Data Transfers** – Where we are transferring Personal Data from Europe to another jurisdiction (including the US), we will ensure that those transfers are subject to appropriate safeguards (including by implementing the EU Standard Contractual Clauses (SCCs) and/or the UK International Data Transfer Agreement/SCCs Addendum where appropriate). We will also conduct transfer risk assessments when sending Personal Data to the jurisdictions where Personal Data protections may not comply with the standards set forth in this policy.

- **Data Protection Impact Assessments** – When we are undertaking new projects or developing our processes and systems, we will consider whether we need to carry out a Data Protection Impact Assessment (i.e., if the project is likely to result in a high risk to the rights and freedoms of individuals).

All CRDF Global staff are required to read, understand, and comply with this policy and its implementing procedures as a condition of employment. Failure to comply with this policy will be grounds for disciplinary or other action and may subject the organization to significant legal and reputational damage. Any staff member with questions related to the appropriate handling of Personal Data must consult with the Privacy Officer.

2. Purpose

CRDF Global has adopted this policy to ensure that Personal Data is safeguarded. This policy ensures (1) staff are aware of the basic principles and obligations that apply to CRDF Global in its processing of Personal Data; and (2) that CRDF Global abides by these policies and procedures for the receipt, use, and storage of any personal data.

3. Definitions

Controller	An organization that determines the "purposes" and "means" of processing Personal Data, i.e. that makes decisions about how and why that data is collected and used. CRDF Global is a controller of the personal data that we obtain.
Data Protection Impact Assessment (DPIA)	A process designed to identify risks arising out of the processing of personal data and to minimize those risks as far and as earlier as possible.
Data Subject	An identifiable living person to whom a particular piece of data relates.
Data Subject Rights Request	A request made by an individual to CRDF Global to exercise their rights under data protection legislation, including: • The right to request access to their personal data; • The right to have their personal data corrected; • The right to have their personal data deleted, in some circumstances; • The right to restrict the processing of their personal data, in some circumstances; • The right to object to the processing of their personal data for certain purposes; • The right to have their data ported from CRDF Global to another controller; • The right not to be subjected to automated decision making and profiling.
General Data Protection Regulation (GDPR)	*GDPR (The General Data Protection Regulation (EU) 2016/679)* is a regulation in European Union (EU) law on data protection and privacy in the EU and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary aim is to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. The UK has its own version of the GDPR which is very similar to the EU version – the UK GDPR. Complying with the GDPR will generally mean that the processing of the data will also be consistent with the requirements of the UK GDPR.
IT Business Systems	The information, devices, and network resources (CRDF Global "business systems") used to conduct CRDF Global business, whether owned or leased by CRDF Global, an employee, or a third party.
Personal Data	Personal Data is *any* information that relates to an individual who can be directly or indirectly identified. Names and email addresses are personal data, but so too could

	be location information, ethnicities, genders, biometric data, religious beliefs, web cookies, and political opinions. It's also important to note that Personal Data can include information that cannot identify an individual by itself, but that can be used in conjunction with other information that we may have (or that a third party may have) to identify an individual. Other examples of personal data include: an individual's date of birth; address; telephone number; driver's license number or card or nondriver's identification number or card; social security number or card; place of employment; employee identification numbers or other personal identification numbers or cards; mother's maiden name; birth, death or marriage certificates; electronic identification numbers; electronic signatures; and any financial number, or password that can be used to access a person's financial resources, including, but not limited to, checking or savings accounts, credit or debit card information, demand deposit or medical information.
Privacy Officer	The individual designated by CRDF Global to oversee compliance with this policy.
Processing	Any operation or set of operations performed on Personal Data, including (but not limited to), collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, anonymization or destruction.
Processor	An entity that processes Personal Data solely on behalf of a Controller (i.e. only in accordance with the Controller's instructions, and not for the Processor's own purposes in any way). Some service providers (including e.g. website host providers, payroll providers and CRM providers) are Processors).
Special Category Data	Personal data that relates to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health and sex life or sexual orientation, or the processing of genetic data or biometric data (for the purpose of uniquely identifying an individual). Note that this data is subject to a higher level of protection under the GDPR, due to its sensitivity.

4. Scope

This policy applies to all CRDF Global employees, personnel, contractors, and vendors in all locations who solicit, collect, handle, transmit, manage, retain, or otherwise use, or have access to Personal Data.

5. Exclusions

None.

6. Additional Content

7. Related Documents

CRDF Global Policies, Processes, and Procedures

Related Policies	Related Processes	Related Procedures
Record Retention Policy	Data Subject Access Request Process (forthcoming)	Record Retention Procedures
IT Acceptable Use Policy.docx	Vision and Hearing Reimbursement Process	Data Privacy Procedures (forthcoming)
IT Incident Response Policy	Recruitment and Selection Process	Vision and Hearing Reimbursement
Talent Acquisition Policy	Data Protection Impact Assessment Process (forthcoming)	Data Protection Impact Assessment Procedures (forthcoming)
Health and Welfare Benefits Policy	Data Subject Access Request Process (forthcoming)	Data Subject Access Request Procedures
Travel Policy	Travel & Logistics Procedures	
Grant Management Policy		
Procurement Policy	Global Supply Chain Procedure	
Marketing and External Communications Policy		

External References

External Reference	Description
General Data Protection Regulations (GDPR)	Official website of GDPR containing the official regulations and guidance.