Responsible Data Policy

Effective Date	July 18, 2019	**Version**	1.1
Issued by	Responsible Data Program Team		
Supersedes	None		

1. Purpose Statement

Mercy Corps works with the world's most vulnerable communities, often in fragile, complex, and insecure environments. Given that context, Mercy Corps is committed to the protection of personal data for program participants, team members, visitors and partners around the world. The purpose of this policy is to set principles for the transparent, secure and responsible use of personal data across Mercy Corps, and incorporate those principles into our daily work.

This policy is designed to establish a responsible data framework to set out and respond to Mercy Corps' current global ethical, regulatory and legal requirements and with a view to being adaptive to potential future changes. Recognizing that the policy applies to a rapidly-changing technological context, Mercy Corps has a responsibility to stay abreast of the implications of these changes for its work.

2. Scope of Policy

This policy applies to Mercy Corps Global, Mercy Corps Europe and Mercy Corps Netherlands, their subsidiaries and affiliate organizations (collectively "**Mercy Corps**"); and Members of Mercy Corps' Boards of Directors, officers, management, employees, seconded employees, interns and volunteers (collectively "**Team Members**"); Subgrantees, partner organizations, contractors, outside experts (including attorneys), consultants, agents, representatives, governments and any other organization or individual that acts on Mercy Corps' behalf or at Mercy Corps' direction (collectively "**Partners**"); and Visitors to any Mercy Corps facilities, which includes photographers, filmmakers, journalists, researchers, donors and prospective donors, and anyone else hosted by Mercy Corps or visiting Mercy Corps' implemented or financially supported programs ("**Visitors**").

3. Policy Statements

3.1. When Mercy Corps records Personal Data, we will use all reasonable efforts to process it according to these data protection principles:

3.1.1. Processed lawfully, fairly and in a transparent manner; and

3.1.2. Collected for specified, explicit and legitimate purposes; and

3.1.3. Adequate, relevant and limited to what is necessary; and

3.1.4. Accurate and, where necessary, kept up to date; and

3.1.5. Kept for no longer than is necessary, and then deleted per relevant retention policies; and

3.1.6. Processed and stored in a manner that ensures appropriate privacy, security, and accountability.

3.2. As part of a Subject Access Request:

3.2.1. Any Data Subject can request to look at or request changes or erasure of the Personal Data that is held about them, or about anyone for whom they are legally responsible.

3.2.2. All requests are subject to legal, ethical, compliance, operational or other legitimate reasons that might prevent Mercy Corps from fully honoring such a request.

3.3. Mercy Corps will use due diligence to ensure it does not unwittingly share Personal Data with unintended third parties, including the implementation of reasonable practices for document and data security.

3.4. Mercy Corps discloses information to third parties when required for legitimate governmental or donor oversight purposes, legal or contractual reasons. A Data Sharing Agreement, or similar, is required in order to share Personal Data with any third party.

If Personal Data is disclosed to others, we will share anonymized information whenever possible. The sharing of program participant Personal Data in fragile, complex or insecure environments may result in higher risks or sharing exceptions. To ensure participant safety, risk assessment and exceptions will be managed by the Enterprise Risk Management Committee.

In addition, we will consider:

3.4.1. Why the third party is asking for the information and why they need it;

3.4.2. Whether the Data Subject has given Informed Consent;

3.4.3. Whether the Data Subject expects Mercy Corps to disclose their Personal Data to third parties; and

3.4.4. Whether release of the Personal Data is likely to cause direct or indirect harm to the Data Subject.

4. Procedures Required to Ensure Compliance

Mercy Corps teams, in partnership with the Information Technology team, will ensure compliance with this policy through appropriate processes and procedures, including:

4.1. Maintenance of data management procedures as it relates to data and technology systems; ensuring all new and existing software, data storage (digital and hard copy), etc., meet the minimum criteria set forth in the related procedure.

4.2. Maintenance of data management procedures as it relates to team members, program participants, and donors.

4.3. In compliance with the General Data Protection Regulation (GDPR), Mercy Corps will adhere to the Mercy Corps Europe Statement on Data Protection and all related Policies and procedures in relation to citizens of the European Union, and data processed within the European Union or by our European entities.

4.4. Mercy Corps' Data Sharing Agreements with Partners will include a clause requiring them to adhere to the substance of this policy and to communicate this policy to their team members.

4.5. All Team Members will be trained on the contents of this policy via Mercy Corps' mandatory training.

5. Policy Administration and Responsibilities

5.1. Responsibility for ensuring this policy remains up-to-date, and that compliance is monitored and enforced, rests with Mercy Corps' Senior Director of Information Technology and Enterprise Risk Management Committee.

5.2. Mercy Corps Chief People and Strategy Officer and Global and Country Human Resources Teams are responsible for ensuring that all team member and human resources related data and its handling complies with this policy.

5.3. Mercy Corps Chief Resource Development Officer and the Resource Development Team is responsible for ensuring that all donor data and resource development data and its handling complies with this policy.

5.4. Mercy Corps Vice President of Program Operations and the Program Operations Team are responsible for ensuring that all participant and program data and its handling complies with this policy.

5.5. Mercy Corps Chief Financial Officer and the Finance Team are responsible for ensuring that all financial data and its handling complies with this policy.

5.6. Senior Management in all countries and areas where Mercy Corps operates are responsible for overseeing the full implementation of, and compliance with, this policy in their area of operations.

5.7. Executive Director, Mercy Corps Europe is responsible for ensuring that Mercy Corps Europe is GDPR compliant and that all European data handled by MCE is in compliance with this policy and relevant MCE policies and procedures.

5.8. Managing Director, Mercy Corps Netherlands is responsible for ensuring that Mercy Corps Netherlands is GDPR compliant and that all European data handled by MCNL is in compliance with this policy and relevant MCNL policies and procedures.

6. Definitions

6.1. **Data:** Any unit of information, composed of letters, numbers, symbols, images, or any combination thereof. Data exists in both digital and physical form.

6.2. **Personal Data:** Personally Identifiable Information (PII) or Demographically Identifiable Information (DII), including information that can be used to identify a Data Subject or any distinct demographic group.

6.3. **Personally Identifiable Information (PII):** information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.

6.4. **Demographically Identifiable Information (DII):** information that can be used to identify a community or distinct group, whether geographic, ethnic, religious, economic, or political.

6.5. Data Processor: the natural or legal person, public authority, agency or other body who processes the content and use of Personal Data or Personally Identifiable Information, or

Demographically Identifiable Information, at the request of the Data Controller. This is regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.

6.6. **Data Controller:** the natural or legal person who, alone or jointly with others, determines the purposes and means for the collection, storing, processing or dissemination of Personal Data or Personally Identifiable Information, or Demographically Identifiable Information.

6.7. **Data Subject:** any individual who can be identified, directly or indirectly, in particular by reference to Personal Data.

6.8. **Subject Access Request:** The process by which a Data Subject would request to look at, request changes to, or erasure of their Personal Data and supplementary information.

6.9. **Data Sharing Agreement:** An agreement between Mercy Corps and a Partner, which states the terms and conditions of use of Personal Data, including which data components are to be shared, the mode of transfer, how the data may be used, data security measures and other related issues.

6.10. **Anonymization:** The process by which Personal Data is rendered anonymous, such that a Data Subject is no longer identifiable.

6.11. **Informed Consent:** any freely-given, specific and informed indication of agreement from the Data Subject, with regards to the collection and processing of Personal Data relating to the Data Subject. This agreement may be given either by a written or oral statement or by a clear affirmative action. Agreement must be obtained at the time of Personal Data collection, or as soon as reasonably possible thereafter.

7. Approved Policy

This policy was approved by the Mercy Corps Enterprise Risk Management Committee on May 23, 2019. This policy may only be amended or changed with the approval of the Committee.