RET International Policy on Personal Data Protection

Bridging the Gaps

RET

This policy was adopted on and is effective as of September 2021.

Table of Contents

DEFINITIONS

Active Data means all Personal Data processed by RET that is not Archived Data; Active Database means a database containing Active Data.

Archived Data means Personal Data contained in documents that have been transferred to RET's Archives; Archived Data ceases to be Active Data. Documents containing Archived Data constitute RET Records, and, as such, cannot be deleted or modified.

Consent means any freely given, specific and informed indication of his or her wishes by which a Data Subject signals agreement to the Processing of Personal Data relating to him or her.

Data Breach means a breach of security leading to the accidental or unlawful destruction, loss or alteration of – or to the unauthorized disclosure of, or access to – Personal Data transmitted, stored or otherwise processed.

Data Controller means the natural or legal person, which, alone or jointly with others, determines the purposes and means of Processing Personal Data.

Data Subject means a natural person (i.e., an individual) who can be identified, directly or indirectly, by reference to Personal Data.

Data Transfer includes all acts that make Personal Data accessible to third parties outside RET – on paper, via electronic means or the internet, or through other methods.

Health Data means data related to the physical or mental condition of an individual that reveal information about the state of his or her health.

Personal Data relating to health includes in particular:

- Data pertaining to the physical or mental condition of a Data Subject;
- Information about registration for health services;
- A number or symbol assigned to an individual to uniquely identify the individual for health purposes;

- Any information on a disease, disability, mental- health or psychosocial disorder, disease risk, medical history or clinical treatment, or information on the physiological or medical state of the Data Subject;
- Any information on a traumatic experience that had an adverse effect on the Data Subject's mental health or led to psychosocial disorders.

RET Staff-in-Charge means RET staff member in each RET country, Administrative Centre or headquarters who is entrusted with the management of a particular project or area of activity within RET's mandate. This includes Country Directors, Program or Project Managers as well as Monitoring & Evaluation Managers, Protection Managers, Communication Managers etc. At RET headquarters, or Administrative Centers, RET Staff-in-Charge means the Heads of Departments (Human Resources, Finance, Administration, etc.) or staff members delegated by them to act as RET Staff-in-Charge.

Personal Data means any information relating to an identified or identifiable natural person. This may include an identifier such as a name or audio-visual materials, an identification number, location data or an online identifier; it may also mean information that is linked specifically to the physical, physiological, mental, economic, cultural or social identity of a Data Subject.

To determine whether a person is identifiable, all the means reasonably likely to be used – either by the Controller or by any other person – to identify the individual directly or indirectly should be considered. To ascertain what means are reasonably likely to be used to identify the individual, all objective factors – such as the costs of identification and the amount of time required for it, given the technology available at the time of the Processing and technological developments – should be considered. Therefore, Personal Data does not include anonymous information, that is, information that does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the Data Subject is not or is no longer identifiable. RET Rules on Personal Data Protection do not, therefore, cover the Processing of such anonymous information, including for statistical and research purposes.

Processing means any operation or set of operations – by automated and other means – that is performed upon Personal Data or sets of Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmitting, disseminating or otherwise making available, aligning or combining, or deleting.

Processor means a person, public authority, agency or other body that processes Personal Data on behalf of the Data Controller.

Recipient means a person, public authority, agency or other body – that is, someone or something other than the Data Subject, the Data Controller or the data Processor – to which the Personal Data is disclosed.

PREAMBLE

BACKGROUND

Data protection legislation has been developing rapidly in recent years: around 120 countries now have laws on data protection or some kind of statutory requirement concerning privacy; and new laws continue to be drafted as awareness of the need to protect data spreads throughout the world.

As new technologies are developed and the world is increasingly interconnected, making it possible to process ever increasing quantities of data faster and more easily, the potential for intrusion into individuals' private spheres becomes more significant.

RET recognizes the immense potential of these technologies in terms of efficiency and seeks to incorporate them in its activities. But it is also keenly aware of the risks involved, and of the importance of developing appropriate data protection standards and putting them into effect.

Safeguarding the Personal Data of individuals, particularly in fragile environments, is an essential aspect of protecting people's lives, their physical and mental integrity, and their dignity – which makes it a matter of fundamental importance for RET. It touches all areas of RET's activity, whether operational or administrative.

As a result, RET has adopted the following policy to protect Personal Data entrusted to it, while also enabling the organization to remain effective in the pursuit of its mission.

PURPOSE AND SCOPE

This policy is intended to ensure that RET can carry out its mission to alleviate suffering and catalyze sustainable development in crises, conflicts, and fragile contexts, in a manner consistent with internationally recognized standards for protecting Personal Data.

This policy applies solely to the Processing of Personal Data. Such Processing encompasses two fields of data protection:

1) RET's active protection of personal data of Data Subjects; and
2) Responding to individuals who are acting on their right to access their personal data which is processed by RET.

Defined terms – listed in the section above – appear in capital letters throughout this policy.

This policy is an inherent component of RET's institutional framework to ensure the protection of individuals, and as such should be read as complementary to other RET policies, including (but not limited to) RET's Children & Youth Safeguarding Policy, PSEA Policy, AAP Policy, Institutional Communications Policy and Electronic Backup Policy.

RET carries out its activities in full conformity with its fundamental principles of humanity, impartiality, neutrality, and independence.

To safeguard these fundamental principles, Personal Data Processing by RET is governed exclusively by the present policy. Their implementation is overseen by the independent RET Data Protection Advisory Group, while the RET Data Protection Commission is the authority habilitated to take binding decisions on specific cases and approve updates to the policy.

BASIC PRINCIPLES

ARTICLE 1: LAWFUL & FAIR PROCESSING

1.1 RET processes Personal Data based on the principles set out in this chapter.

1.2 RET shall process Personal Data only if there is a lawful basis for doing so in this policy. The legitimate bases that may apply are the following:

a. consent of the Data Subject
b. vital interest of the Data Subject or of another person
c. public interest, in particular based on RET's mission
d. legitimate interests of RET, provided that these interests are not overridden by the rights and freedoms of the Data Subjects
e. performance of grant and partnership agreements
f. compliance with a legal obligation in the countries where RET is registered.

1.3 Wherever possible, Consent is the preferred basis for Processing Personal Data. However, because of the vulnerability of most of the program participants of RET activities, and the nature of the organization's work in crises, conflicts and fragile contexts, RET may not always be in a position to rely on this preferred basis for its Processing operations.

1.4 RET takes particular care in Processing the Personal Data of certain vulnerable categories of Data Subjects, such as children, young people, the elderly, mentally disabled people or people who have been psychologically traumatized. RET also takes particular care when processing Personal Data that might cause harm to Data Subjects if mishandled. Data of this kind may vary from one context to another, but there is a presumption that health-related Personal Data belongs to this category.

ARTICLE 2: TRANSPARENT PROCESSING

2.1 Data Processing must be transparent to the Data Subjects involved. Data Subjects must be given a certain minimum amount of information about the Processing. RET Staff-in-Charge will decide how this information is to be

communicated, after taking into account such matters as security conditions in the field, logistical constraints, and the urgency of the Processing.

2.2 In addition, all information and communication concerning the Processing of data must be accessible and easy to understand; and clear and plain language should be used, in a language that can be understood by the Data Subject.

2.3 The minimum information to be provided is described in detail below (art. 7).

ARTICLE 3: PURPOSE OF PROCESSING AND FURTHER PROCESSING

3.1 When collecting data, RET Staff-in-Charge determine the specific and legitimate purpose/s for which data is processed; the data is then processed only for those purposes. General purposes for which RET may Process Personal Data include:

a. To fulfil the mission of the organization; and
b. To fulfil legal and contractual obligations to donors, partners and authorities.

3.2 RET may process Personal Data for purposes other than those specified at the time of collection if such further Processing is compatible with those original purposes, provided that:

a. Personal Data is anonymized; and
b. Such Processing is necessary for academic or internal improvement purposes of a non-profit nature; or
c. For accountability to affected populations.

3.3 RET may also process Personal Data after a project has ended for internal analysis and communication purposes, provided that data is anonymized and only metadata is shared externally.

3.4 However, further Processing is not permissible if the risks for the Data Subject outweigh the benefits of further Processing.

ARTICLE 4: ADEQUATE AND RELEVANT DATA

4.1 The data handled by RET must be adequate and relevant to the purposes for which they are collected and processed.

4.2 This requires ensuring that the data collected are not excessive for the purposes for which they are collected and for compatible further Processing, and that the period for which the data are stored, before being anonymized or archived, is no longer than necessary.

ARTICLE 5: DATA QUALITY

5.1 Personal Data must be as accurate and up-to-date as possible.

5.2 Every reasonable precaution must be taken to ensure that Personal Data proven to be inaccurate are corrected or deleted without undue delay.

ARTICLE 6: RETENTION, DELETION, AND ARCHIVING OF DATA

6.1 To ensure that data are not kept longer than necessary, a minimum retention period is set, at the end of which a review is carried out to determine whether the data are still required. Depending on the findings of the review, the retention period is renewed or the data are deleted or archived.

6.2 Personal Data must be deleted when:

a. they are no longer necessary for the purposes for which they were collected or otherwise further processed;
b. the Data Subjects withdraw their Consent for Processing;
c. the Data Subjects object to the Processing and their objections are upheld by RET Staff-in-Charge, the Data Protection Advisory Group or the RET Data Protection Commission;
d. a donor or partner contract stipulates doing so;
e. this policy otherwise provides for deletion.

6.3 However, data should not be deleted when there is a legitimate reason for archiving them: for instance, the data may be necessary for ensuring long-term provision of services, statistical purposes or for accountability to affected populations.

6.4 A Data Subject must be able to have his or her Personal Data deleted from RET's Active Databases when retention of such data is not in compliance with these rules.

6.5 However, the right to deletion does not apply, and Personal Data will continue to be retained, in the following circumstances:

a. when RET Staff-in-Charge is concerned that the Data Subject is requesting deletion because of external pressure, and that deleting Personal Data would harm that Data Subject's vital interests or those of another person;

b. for reasons connected to the right to freedom of expression/freedom of information, including for the purposes of documenting the activities of RET

c. when it serves the public interest to do so

e. for long-term humanitarian, relief, development cooperation and stabilization and peacebuilding purposes or to establish accountability

f. for the establishment, exercise or defense of legal claims.

RIGHTS OF DATA SUBJECTS

ARTICLE 7: INFORMATION

7.1 The following minimum information about data Processing must be provided to Data Subjects – orally or in writing, and in plain and understandable language – when Personal Data are obtained or collected:

a. whether RET is the Data Controller, and whether there are other Data Controllers;

b. the purpose(s) for which data are processed;

c. whether the data are likely to be shared with one or more partners;

d. that they may address any questions/concerns/complaints about the handling of data to, first, any RET staff member and, second, to the Data Protection Advisory Group (if for valid concerns they cannot address the issue with the Staff) or directly to the RET Data Protection Commission (if, for valid concerns, they cannot address the issue with the Staff or Advisory Group),

If RET is unable – because of logistical or security constraints – to provide this information when Personal Data are obtained or collected, it must notify the Data Subject and provide this information at a later date and without any unreasonable delay.

ARTICLE 8: ACCESS

8.1 Data Subjects must be given an opportunity to obtain, on request, at reasonable intervals and without excessive delay, confirmation of the processing of Personal Data relating to them. The data that have been processed should be communicated to them in an intelligible form. Data Subjects should also be able to verify their Personal Data and given access to the data, except in the circumstances listed in article 8.3 below.

8.2 Disclosure of Personal Data should not be automatic. RET Staff-in-Charge, the Data Protection Advisory Group and/or the Data Protection Commission should first consider all the circumstances surrounding the request for access and any restrictions to access that may be applicable. RET should not reveal any information about Data Subjects, unless they are provided with sufficient proof that the person asking for the information is the Data Subject.

8.3 The right to access documents does not apply when important public interests require that access be denied. These interests include:

a. ensuring the viability of operations being carried out by RET
b. preserving the confidentiality of RET staff members' views or line of reasoning, which, if breached, might jeopardize RET operations and/or disclose Personal Data of staff members
c. the rights and freedoms of others that override the data protection interests of the Data Subject.

8.4 Requests from parents and legal guardians should be allowed on the best interests of the child or vulnerable Data Subject; there is a presumption that access is in the best interest when conducted by the parents and legal guardians. RET may, however, refuse to reveal Personal Data relating to children or youth if RET has sufficient reason to believe that it would not be in the best interests of a particular child or young person.

8.5 Access to Archived Data is subject to strict conditions and procedures around retention and anonymization.

ARTICLE 9: CORRECTION & DELETION

9.1 At the request of a Data Subject, mistakes or inaccuracies in his or her Personal Data must be corrected by RET Staff-in-Charge, except when:

a. the identity of the Data Subject cannot be verified by RET Staff-in-Charge;
b. RET Staff-in-Charge have evidence that the previous data is, in fact, accurate or that the new data proposed by the Data Subject is incorrect;
c. the data are contained in a record held by RET's archives.

9.2 Data Subjects have a right to deletion, as specified under Article 6.

ARTICLE 10: OBJECTION

10.1 Data Subjects may object at any time, on compelling legitimate grounds relating to their particular situation, to the Processing of Personal Data concerning them.

10.2 An objection of this kind will be accepted if the fundamental rights and freedoms of the Data Subject in question outweigh RET's legitimate interests, or the public interest, in Processing.

ARTICLE 11: ASSERTION OF DATA PROTECTION RIGHTS BY INDIVIDUALS

11.1 Data Subjects may make a formal assertion of their data protection rights through any RET staff member who may then refer the case to a Staff-in-Charge or the RET Data Protection Advisory Group.

11.2 When it cannot provide an accepted opinion for an individual complaint itself, the RET Data Protection Advisory Group must refer the matter to the RET Data Protection Commission.

11.3 If the Data Protection Advisory Group fails to refer the matter to the Data Protection Commission, Data Subjects may also make a formal assertion of their data protection rights directly with the Data Protection Commission.

11.4 If a complaint is found to be justified, appropriate measures must be taken.

RET COMMITMENTS

ARTICLE 12: RESPONSIBILITY/ACCOUNTABILITY

12.1 It is the responsibility of RET Staff-in-Charge to ensure that everyone with access to Personal Data, and under the authority of RET, handles or processes data in compliance with these rules.

12.2 This requires that when RET cooperates with an external entity in Processing data, the responsibilities of all parties concerned must be defined in a contract or other legally binding arrangement. For example, an entity that sets out to Process Personal Data on behalf of RET must agree to provide certain forms of protection of the data and Data Subjects, and agree also to process the data only as directed by RET. The data remains property of RET or the Controller of the data, should this not be RET.

ARTICLE 13: DATA PROTECTION BY DESIGN AND BY DEFAULT

13.1 While designing a database, data processing, and drafting procedures for collecting Personal Data, these rules must be considered and incorporated to the greatest extent possible; this is known as "data protection by design and by default." In this design, "data minimization" should be a leading principle. Data is collected because it is needed, not because it is possible to collect it. In other words, if personal data is not required for the efficient implementation of a project, the establishment of baselines or other activities to further RET's mission, it should not be collected.

ARTICLE 14: COOPERATION WITH SUPERVISORY AUTHORITIES

14.1 Any request by a data protection supervisory authority must be referred to the RET Data Protection Commission before it is acceded to.

ARTICLE 15: DATA BREACHES

15.1 Any breach of security leading to the accidental or unlawful destruction, loss or alteration of – or to the unauthorized disclosure of, or access to – Personal Data transmitted, stored or otherwise processed must be reported to RET Data Protection Advisory Group.

15.2 If a data breach puts individuals at a serious identified risk, the persons affected must be notified by the Staff-in-Charge, in coordination with the Data Protection Advisory Group, without undue delay, unless:

a. that would involve disproportionate efforts, owing to logistical circumstances or security conditions for example. In such cases, RET Staff-in-Charge, in coordination with the RET Data Protection Advisory Group, must consider alternative means of action.

b. it would adversely affect a matter of substantial public interest, such as the viability of RET operations.

c. approaching the Data Subjects, because of the security conditions, could endanger them or cause them severe distress.

ARTICLE 16: DATA SECURITY

16.1 Personal Data must be processed in a manner that ensures an appropriate degree of security. Several factors need to be considered to determine the level of security required, but particular attention should be paid to:

- the nature of the data;
- the risks to Data Subjects;
- the risks to RET's mandate;

This relates to access rights to databases, physical security, computer security or cyber security, the duty of discretion and the conduct of staff.

16.2 When retention of Personal Data is no longer necessary, all records and backups must be securely destroyed or anonymized.

DATA TRANSFERS

ARTICLE 17: REQUIREMENTS FOR DATA TRANSFERS

17.1 Data may be transferred to external entities when the following conditions have been met:

a. The identification of at least one applicable lawful basis for the transfer:
   i. consent of the Data Subject;
   ii. vital interest of the Data Subject or of another person;
   iii. public interest;
   iv. legitimate interests of RET, provided that these interests are not overridden by the rights and freedoms of the Data Subjects;
   v. performance of grant and partnership agreements;
   vi. compliance with a legal obligation.

b. A risk assessment is undertaken by the Staff-in-Charge.

c. Processing by the Recipient is restricted as much as possible to the specific purposes of RET Processing or permissible further Processing.

d. The amount and the type of Personal Data to be transferred is limited to the Recipient's need to know for the specified purposes.

e. the transfer is not incompatible with the reasonable expectations of the Data Subject.

f. appropriate measures are used to safeguard the transfer of Personal Data to third parties. The means of transmission, and the security methods employed, must be proportionate to the nature and sensitivity of the Personal Data, the risks and the urgency of action.

g. The transfer is in no way done against any form of financial or material compensation (i.e., RET is never allowed to sell personal data to third parties).

ARTICLE 18: DATA TRANSFER AGREEMENTS

18.1 All data transfer agreements must contain:

a. A written undertaking from the Recipient that they will process the Personal Data only for the specific purposes for which they were transferred and will not transfer them to a third party;
b. A written undertaking from the Recipient that they have the technical and organizational measures needed to ensure adequate protection for the Personal Data that have been transferred;
c. A written undertaking that the transferred data, as well as any secondary data derived from the Data Processing, is and will remain the property of RET;

IMPLEMENTATION

ARTICLE :19 EFFECTIVE IMPLEMENTATION

19.1 Effective implementation of this policy is crucial to ensure that Data Subjects can benefit from the protection afforded by them. Effective implementation is ensured by the work of the RET Staff-in-Charge, the RET Data Protection Advisory Group and the RET Data Protection Commission.

19.2 It is the task of RET Staff-in-Charge to make sure that these rules and RET's data protection policies are implemented. RET Headquarters, RET Administrative Centers and RET Country Directors with their senior management are responsible for drawing up effective and suitable measures to guarantee that activities comply with the principles and commitments laid down in this policy.

19.4 Allegations of non-compliance with this policy must be reported immediately to RET Staff-in-Charge, who should investigate them without undue delay. If a complaint is found to have merit, appropriate measures should be taken to mitigate any risk of harm to the Data Subject and the Data Protection Advisory Group should be informed.

19.5 Any breach of these rules that results in serious harm to Data Subjects must be referred to the Data Protection Advisory Group, RET staff members involved in a serious breach may be subject to disciplinary measures.

ARTICLE 20: RET DATA PROTECTION ADVISORY GROUP

20.1 A Data Subject who believes that his or her rights under these rules have been infringed may petition the RET Data Protection Advisory Group directly, if for valid concerns she/he cannot address the issue with the Staff-in-Charge.

20.2 Staff-in-Charge may also ask the RET Data Protection Advisory Group for opinions on the proper application of this Policy, both generally and in specific claims.

20.3 The Data Protection Advisory Group must be officially petitioned in writing at the following address: DPAdvisoryGroup@theret.org.

20.4 The RET Data Protection Advisory Group may consult RET staff from the field, Administrative Centers or Headquarters as well as contact Heads of Departments concerned to obtain clarification or supplementary information that may clear up the matter.

20.5 The official replies provided by the Advisory Group have the value of a RET expert opinion and do not constitute a RET binding decision.

a. These opinions are officially submitted to the Staff-in-Charge and their Supervisor (Head of Department or Country Director) who decide to apply it or not to the case at hand. Should the Staff-in-Charge and their Supervisor judge the opinion to be non-satisfactory, they can petition the Commission for an official decision.
b. In the case of Data Subjects petitioning the Advisory Group directly, the opinion from the group is provided to the most relevant Staff-in-Charge, with her/his supervisor in copy, to apply. Should they not agree with the opinion, they can petition the Commission for a decision. The Data Subject must then be officially informed by the Data Protection Advisory Group that the matter has been referred to a higher authority and is pending a decision. If the opinion is accepted by the Staff-in-Charge and his/her supervisor, the Data Subject is informed of the outcome by the Data Protection Advisory Group.

20.6 If it cannot find a solution to a petition, the RET Data Advisory Group must refer the matter to RET Data Protection Commission.

20.7 To guarantee the neutrality of its opinions, the RET Data Protection Advisory Group and its individual members do not receive any instructions on cases they work on.

ARTICLE 21: RET DATA PROTECTION COMMISSION

21.1 The RET Data Protection Commission is responsible for interpreting this policy and for rendering binding decisions about the implementation or breach of its articles.

21.2 The RET Data Protection Commission may convene at the request of RET's CEO or when petitioned for a specific issue on which it must provide a decision. It is as such not a permanent body.

21.3 Members of the RET Data Protection Commission are nominated by the CEO directly for each individual case, among members of RET Global Senior Management, at the exclusion of members of the RET Data Protection Advisory Group. Experts among RET staff may also be requested to join as non-voting members to provide information and advice.

21.4 The RET Data Protection Commission can be called upon either by the RET Data Protection Advisory Group, by a Staff-in-Charge, or by a Data Subject. The standard procedure is to first go through the Data Protection Advisory Group, who then judges if the Commission is to be petitioned. Petitioning the Commission directly should only be undertaken when there is a legitimate concern that the Data Protection Advisory Group would lack the neutrality to render a sound opinion.

21.5 The commission must be officially petitioned in writing at the following address: DPcommission@theret.org. The Commission reserves the right to not take a petition into consideration should article 21.4 not be respected.

21.6 When it is petitioned the RET Data Protection Commission has authority to examine all questions of fact, interpret the policy and make binding decisions.

REVIEW AND UPDATE

ARTICLE 22: REVIEWING AND UPDATING

22.1 To ensure RET's responsiveness to regulatory, social and technological developments in data protection, the Data Protection Commission may request the Advisory Group to conduct reviews at regular intervals or on specific points of concern.

22.2 Any modifications to this Policy must be formally approved by the Data Protection Commission.