DATA PROTECTION POLICY

Version 4.2 | 2025

CONTENT

I. INTRODUCTION

A. Preamble

1. Independent, private and non-profit, Acted respects a strict political and religious impartiality, and operates following the principles of neutrality, non-discrimination, transparency, according to its core values: responsibility, impact, enterprising-spirit and inspiration.

2. Acted is committed to immediate humanitarian relief to support those in urgent need and protect people's dignity, while co-creating longer term opportunities for sustainable growth and fulfilling people's potential. Acted endeavours to respond to humanitarian crises and build resilience; promote inclusive and sustainable growth; co-construct effective governance and support the building of civil society worldwide by investing in people and their potential.

3. The commitment of Acted is guided by 4 core values:

    - **Responsibility**: we ensure the efficient and responsible delivery of humanitarian aid with the means and the resources that have been entrusted to us.
    - **Impact**: we are committed to having the most sustainable impact for the communities and the people with whom we engage.
    - **Enterprising-spirit**: we are enterprising and engage in our work with a spirit that creates common values and overcomes challenges.
    - **Inspiration**: we strive to inspire all those around us through our vision, values, approaches, choices, practice, actions and advocacy.

B. Policy Statement

1. Acted takes privacy protection very seriously. Respect for privacy and the protection of personal data is a factor of trust, a value to which Acted is particularly committed, by focusing on respect for fundamental rights and freedoms. This Data Protection Policy illustrates Acted's commitment to privacy and the protection of Personal Data.

2. The purpose of this Policy is to present the main principles related to the protection of Personal Data that Acted implements in the framework of all its activities.

3. The purpose of this policy is aimed at guiding Acted staff, and must be considered together with:

    - Acted's Code of Conduct;
    - Acted's Child Protection Policy;
    - Acted's Policy on Protection from Sexual Exploitation, Abuse and Harassment;
    - Acted's Conflict of Interest Policy;
    - Acted's Grievance Policy;
    - Acted's Anti-Fraud, Bribery and Corruption Policy;
    - Acted's Anti-Terrorism and Money Laundering Policy;
    - Acted's Environmental and Social Protection Policy;
    - Acted's Gender Policy;
    - Acted's procedures, manuals (e.g. Finance, Logistics, Administration & Human Resources, Security & Safety), handbooks (e.g. Transparency & Compliance, Appraisal, Monitoring & Evaluation, Project Management, Project Development) and charters (e.g. Use of Information Systems);

- Code of Conduct for The International Red Cross and Red Crescent Movement and NGOs in Disaster Relief, of which Acted is a signatory;
- U.N. Inter-Agency Standing Committee (IASC) Six core principles relating to Sexual Exploitation and Abuse.
- These include data processing agreements, data sharing agreements and the data retention notice.

II. INTERPRETATION AND APPLICATION

Article 1 – Scope of Application

1. This policy applies to all Acted staff and governance members.
2. The provisions of this policy may also be applied to any person employed by an entity that carries out missions for Acted.
3. The scope of this policy is defined by the General Data Protection Regulation (GDPR).

Article 2 – Definitions

For the purposes of this Policy, the terms below have the following meanings:

1. "**Data recipient**": means, in accordance with the GDPR, the natural or legal person, public authority, department or other body that receives disclosure of Personal Data, whether or not it is a third party;
2. **"DPO"** or **"DPD"**: for "Data Protection Officer" or "*Délégué à la protection des données*", person in charge, in accordance with the GDPR, in particular of (i) informing and advising Acted and its employees regarding their obligations with respect to the protection of Personal Data, (ii) monitoring Acted's compliance with the obligations regarding the protection of Personal Data, (iii) accompanying Acted during the performance of impact analysis, (iv) and cooperating with the supervisory authorities;
3. "**Personal Data**": means, in accordance with the GDPR, any information relating to an identified or identifiable natural person; an "identifiable natural person" is deemed to be a "natural person" if it can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or to one or more elements specific to its physical, physiological, genetic, psychological, economic, cultural or social identity;
4. **"Acted staff"**: under the terms of this policy, the term "Acted staff" refers to any person employed by Acted and/or one of its sister organisations and/or one of the member organisations of the Acted network. The interns of Acted and/or one of its sister organisations and/or one of the member organisations of the Acted network are considered to fall within this category, for the purposes of this policy.
5. "**Data subject**": means, in accordance with the GDRP, a natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or one or more elements specific to his or her physical, physiological, genetic, psychological, economic, cultural or social identity. For the purposes of this policy, a data subject is defined as a natural person whose Personal Data are processed by Acted.

6. **"Applicable law"**: refers to the legislation in force relating to the protection of privacy with regard to the processing of Personal Data, in particular Act n°78-17 of 6 January 1978 on information technology, data files and civil liberties (French Data Protection Act) and Regulation (EU) 2016-679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to data processing;

7. "**Third party**": refers to a natural or legal person, a public authority, a department or body other than the data subject who is the subject of the processing operation, the data controller, the subcontractor and the persons who, placed under the direct authority of the controller or the subcontractor, are authorised to process the Personal Data.

8. **"Processing"**: means, in accordance with the GDPR, any operation or set of operations carried out using or not automated processes and applied to Personal Data or sets of Personal data, such as the collection, recording, organisation, structuring, storage, adaptation or modification, extraction, retrieval, consultation, use, communication by transmission, dissemination or any other form of making available, matching or interconnection, limitation, erasure or destruction.

Article 3 – Information and adherence to the policy

1. This policy is published under the authority of Acted. Acted staff, as well as the other entities referred to in Article 1 of this Policy, if applicable, are required to conduct themselves in accordance with this policy and must, therefore, be aware of its provisions and any changes and have understood them. When they are unsure about how to proceed, they must seek the advice of a competent person, notably their line manager and the DPO.

2. Acted staff, as well as the other entities referred to in Article 1, if applicable, have certified their knowledge of the present policy and agreed to commit to the full respect of this policy.

3. It is the responsibility of Acted staff, as well of the entities mentioned in Article 1 if applicable to ensure their compliance with this policy and to take the appropriate disciplinary measures against any violations of this policy.

4. Acted will review the provisions of this policy at regular intervals.

III. GENERAL PRINCIPLES APPLICABLE TO DATA PROTECTION

Article 4 – Compliance with the policy

1. Acted staff undertake to respect the principle of the Personal Data Processing at all times when carrying out their duties.

2. In the event of a new Personal Data Processing, Acted staff must respect the principles set out below.

Article 5 – The lawfulness of Processing

1. Each Personal Data Processing carried out by Acted must respect/follow the applicable law. Acted Staff shall carry out their duties according with the legal obligations relevant to the processing operations.
2. When processing Personal Data, which are meeting Acted's legitimate interests, specific protection measures must be implemented to ensure the optimal privacy protection.

Article 6 – The Purpose of Processing

1. The Purpose of processing operations carried out by Acted must be predetermined, legitimate, explicit and compatible with the missions carried out by Acted.
2. Personal Data must not be used in a way that is incompatible with the purposes initially determined for each processing operation.

Article 7 – Minimisation and accuracy of data

1. The defined and predetermined purposes allow to assess the relevance of the Personal Data collected by Acted. Only data which is adequate and strictly necessary to achieve these purposes shall be collected and processed.
2. Acted is committed to processing only accurate, complete and up to date datas. Under these conditions, Acted reserves the right to request data subjects the verification of their Personal Data's accuracy.

Article 8 – Data retention

1. Following the Purpose of Processing, a retention period of the datas is necessary to determine Acted's activities in accordance with the applicable law.
2. Personal Data shall be kept no longer than necessary according to the predetermined purposes. In case of doubt, please Acted's policy on Personal Data Retention.
3. Personal Data are kept as long as it is required by the applicable law. A notice on data retention has been drafted by Acted and must be consulted by Acted staff in case of doubt about the retention period of Personal Data during a Processing operation.
4. For any questions regarding the storage of Personal Data, please contact the Data Protection Officer at the following address: dpo@acted.org.

Article 9 – Transfers of Personal Data

1. Acted has implemented procedures to transfer Personal Data outside the European Union. Acted staff in charge of data protection must ensure the implementation of these procedures, especially when concluding contracts with suppliers.
2. In accordance with the applicable law, data subjects from whom Personal Data have been collected are informed of the existence of a transfer of Personal Data to a non-EU Member State, by means of a document. Acted staff in charge of data protection must ensure that this information has been properly communicated.

Article 10 – Personal Data Officer

1. In order to preserve privacy and the protection of Personal Data, Acted has appointed a Data Protection Officer since 2018, the DPO carries out his missions in complete independence from all Acted entities.
2. The DPO is a guarantee of trust. He is a contact person specialised in the protection of Personal Data, responsible for ensuring the proper application of data protection rules and is the privileged contact person for the CNIL and all persons involved in the collection or processing of Personal Data.
3. Acted's DPO can be contacted at the following address: dpo@acted.org.

IV. PRINCIPLES APPLICABLE TO THE INFORMATION AND RIGHTS OF DATA SUBJECTS

Article 11 – Data Subjects Information

1. Acted must provide clear, complete, easily accessible and understandable information for the processing of Personal Data.
2. In this respect, any data subject shall be informed of the following:
    - The identity of the controller and, where applicable, that of his representative;
    - The contact details of Acted's Data Protection Officer;
    - The Purpose of Processing for which the data are intended;
    - The data recipients or categories of data recipients;
    - The rights of the data subjects with regards to the processing of their Personal Data as specified in Article 9 of this policy.
    - An automated computer processing of Personal Data. Acted will inform the data subjects and may, if necessary, obtain their consent. Data subjects have the right to obtain the reasons for the implementation of automated processing of their data and may express their refusal by requesting human intervention.
    - The possible cross-referencing of data in order to improve the quality and effectiveness of Acted's missions, assess the situation of the people concerned or predict it.
    - The existence, if any, of the transfer of Personal Data to a State outside the European Union.
3. Acted has drafted several information notices, specific to certain categories of data subjects in order to meet this obligation. Acted staff in charge must ensure that these information notices are communicated to the right categories of persons.

Article 12 – Rights of the data subjects and procedures for exercising them

1. Acted commits to implement technical and organisational measures to enable the data subjects to exercise the following rights:
    - the right of access: the right of the data subject to be informed and to request the disclosure of his /her Personal Data in an intelligible format;

- the right to rectification: the right of the data subject to obtain rectification of Personal Data when deemed inaccurate;
- the right to erasure: the right of the data subject to obtain the erasure of his/her Personal Data;
- the right to limitation: the right of the data subject to obtain a limitation of the processing of his or her Personal Data;
- the right to portability: the right for the data subject to receive his/her Personal Data concerning him or her in a structured format and to request their transmission by Acted to a third party of his / her choice;
- the right to object: the right of the data subject to object to all or part of the processing of his or her Personal Data for reasons relating to his or her particular situation;
- finally, every data subject has the right to define the directives relating to the use of their Personal Data after their death.

2. All the above-mentioned rights can be exercised at any time by sending a request by e-mail to the following address: dpo@acted.org.

3. For any request, Acted reserves the right to carry out an identity check.

4. In the event of complaint, any person concerned may choose to refer the matter to the supervisory authority.

5. In case of a data subject's request of the above-mentioned rights, Acted must respond as rapidly as possible in the limit of one month.

V. PRINCIPLES APPLICABLE TO CONFIDENTIALITY AND SECURITY

Article 13 – Confidentiality

1. Respect for data confidentiality, especially when using any electronic means of communication, is an essential requirement of Acted.

2. The protection of Acted's interests requires everyone to respect a general and permanent obligation of confidentiality, discretion and business secrecy with regard to the data made available to the User for the exercise of his professional activity, in particular social, legal, financial, commercial, scientific, technical, economic or industrial information, in the context of the use of Information Systems.

3. Compliance with this obligation implies, in particular, to:

   - ensure that unauthorized third parties do not become aware of such information;
   - avoid appropriating, storing or reproducing such information for personal use;
   - use the information in regard of the predetermined purposes;
   - respect the rules of professional ethics, deontology and discretion in use within Acted.

4. Transmission of confidential data may only be executed under the following conditions, subject to the prior authorization of the authorized person mentioned in Article 1:

   - authorisation of the issuer;

- designation of an authorized data recipient;
- compliance with a secure procedure;
- indication of the mention "CONFIDENTIAL".

5. The use of encryption procedures is a function that can only be implemented in certain authorized cases. The use of cryptographic means other than those expressly authorized by Acted is forbidden by the present policy.

6. In accordance with the territorial scope of the GDPR, Acted requires any subcontractor to whom Personal Data have been entrusted to provide the appropriate safeguards to protect the confidentiality of Personal Data.

Article 14 – Security

1. Acted commits, to the limits of its means and capacity, to take all necessary precautions to preserve the security of Personal Data and in particular to prevent their distortion, destruction or communication to unauthorised third parties.

2. In accordance with the territorial scope of the GDPR, Acted also requires any subcontractor to whom Personal Data have been entrusted to provide the appropriate safeguards to ensure the security of Personal Data.

3. Only duly authorized data recipients can access, within the framework of a security policy, the information necessary for their activities. Access rights are granted according to the principles of "least privilege" and "need to know".

4. Acted has drafted an Information Systems Policy which Acted's staff commits to respect.

VI. POLICY MODIFICATION

Article 15 – Policy modification

1. This policy, accessible to all, is regularly updated to consider legislative and regulatory changes, and any change in Acted's organization or in the performance of its missions.

2. In the event of any modification of this policy, Acted shall make its best efforts to inform the concerned persons. The date of this policy will be modified accordingly each time it is updated.

3. In the event that a modification of this policy is likely to have a fundamental impact on the nature of the data processing or a substantial impact on the situation of a data subject, Acted commits itself to inform the data subjects as soon as possible so that they can exercise their rights (for example, to oppose the processing).

4. Acted has drafted an Information Systems user charter that Acted's staff is committed to respect.

VII.IMPLEMENTATION OF THE POLICY

Article 16 – Implementation date of the policy

1. This Data Protection Policy comes into effect immediately after approval by ACTED Board's on 3 October 2025.

Article 17 – Adherence to the policy

1. Acted staff, and the other entities referred to in Article 1 of this policy if appropriate, certify that they adhere to these principles by signing the Acted Policy Acceptance Form and/or by signing their employment contract.

****

Data protection policy

© Acted

2025