ACT Alliance
Communities Data Safeguarding Policy

Approved by the ACT Executive Committee on 3rd November 2021
Revised version in compliance with the Core Humanitarian Standard and Board comments

Introduction

ACT Alliance is committed to being transparent in its work and in upholding the highest professional, ethical and moral standards of accountability[1]. A key dimension is addressing the safeguarding of data drawn from programme participants, especially the 'communities' to whom ACT serves through its members. This policy is specifically related to the data of communities with whom our members interact with through the ACT Humanitarian Emergency response mechanism. It applies to the ACT members' data collection and storage related to project participants herewith referred to as "rights holders" in relation to ACT members. The ACT Secretariat does not collect or store data from project participants directly, the data is from the ACT members. The ACT Secretariat shall abide by the relevant ACT policies including the ACT Communications Policy, Public Information Disclosure Policy and ACT Social Media Policy when collecting, using and storing this data.

The ACT Alliance believes that no harm should be created to the communities through the storage, use and transmission of their personal data, subject to the limitations outlined in this policy. It is important to build trust and confidence between ACT members and project participants. It is a right embedded in the Core Humanitarian Standard (CHS) commitment that the rights holder, as a 'data subject', should know why data relevant to them is collected by the respective member organisation, how their data will be used, shared, stored, archived, and destroyed. They should be able to ask for their data stored and request any correction/deletion that may be required. The rights holders should also be aware that in case of concern about possible data misuse the Complaints Response Mechanism (CRM) of the member organization can be used. If due to any reason the complaint isn't addressed by the respective member organization then the 'data subject' should know how to lodge a complaint by using ACT Alliance's CRM.

It is obligatory for ACT members to seek the informed consent related to data collection from rights holders as well as to inform project participants about their rights in relation to data protection. Furthermore, rights holders should be made aware of how they can access personal information held about them by ACT members and how to raise any concerns if they become aware of any misuse of their data collected in the humanitarian work.[2]

1. Definition

For purposes of this policy, 'data safeguarding' means the process of protecting any information content in paper, electronic or other medium, concerning a matter relating to the communities supported by ACT members through humanitarian programmes.

2. Policy Requirements

The ACT Alliance Secretariat is certified against the Core Humanitarian Standard (CHS) – a set of nine commitments to ensure accountability towards right holders. The Communities Data Safeguarding Policy relates to CHS commitment number 3, requirement 3.8, i.e. 'systems are in place to safeguard any personal information collected from communities and people affected by crises that could put them at risk'. It aims to ensure that ACT members safeguard data about individuals and rights holders collected in the form of text, phone numbers and multimedia (audio, images, graphics and video).

[1] As outlined in the ACT Founding Document 2009, Global Strategy for ACT Alliance 2019-2026, ACT Accountability Framework 2021, Core Humanitarian Standard, Humanitarian Charter under Sphere Minimum Standards and the ACT Code of Conduct 2016.

[2] This policy represents the minimum standard for ACT Members. It should be interpreted taking into account any additional local legal requirements in the country in which the ACT Member is operating.

3. Purpose

The ACT Communities Data Safeguarding Policy seeks to ensure that the use of collected data concerning communities is not putting those communities at risk. It is expected that such safeguarding will ensure that communities and people affected by crises are not negatively affected or put at-risk as a result of humanitarian action and that they know their rights with regard to data that is collected.

4. Scope

This policy applies to all data held by ACT members during a humanitarian response implemented through the ACT Humanitarian Emergency response mechanism. All personal information collected from the rights holders should be treated as confidential (especially those related to protection, reported violations, complaints of abuse or exploitation and gender-based violence). ACT members are required to comply with this policy at a minimum until they have developed their own policy of a commensurate standard to replace it and whilst still meeting their organizational requirements as an ACT member as well as any local legislative requirements.[3]

5. Communities Rights on Data Safeguarding

ACT Alliance commits to uphold the rights of communities in relation to data safeguarding. These rights originate from ACT's Quality and Accountability (Q&A) Framework which includes our commitment to the Humanitarian Charter, Protection Principles, Code of Conduct & the CHS. All the ACT members should adhere to the rights listed below:

5.1 Right to Protection

Communities have the right to expect ACT members to record and retain data in a manner that ensures the safety of the individuals and the community itself. This includes ensuring that the community and its members understand that they have the freedom to not give permission for data collection without fear of negative implications.

5.2 Right to Data Privacy & Security

Data will be collected and managed in such a way as to ensure that the privacy and security of communities and individuals is not compromised. Data subjects will be informed as to how their data will be managed.

5.3 Right to No Harm

Data collected from and about individuals and communities must be handled, stored, processed and used in a way that does not put any individual or community at risk of harm of any kind.

5.4 Right to Informed Consent

Data is collected while informing the data subject. The data subject can withdraw from providing information.

5.5 Right to Access and Availability of Personal Data

[3] Principles and procedures in relation to ACT Alliance Secretariat internal and external data are addressed separately in the ACT Communications Policy, Public Information Disclosure Policy and ACT Social Media Policy.

Upon request, the Data Subject must be given confirmation of whether their data is being processed, other supplementary information and a copy of the Personal Data being processed within two-weeks of receipt of the request, unless in specific circumstances.

6.6 Right to Complain about Non-compliance to Data Safeguarding

Data subjects and communities have the right to complain about any ACT member's non-compliance with the data safeguarding policy, preferably by email to: mailto:complaints@actalliance.org OR by letter addressed to: "The Complaints Focal Person" ACT Alliance Secretariat, 150 Route de Ferney, PO Box 2100, 1211 Geneva 2, Switzerland OR by phone call or sms/text message (+41 798 57 53 34).

6. Data handling/sharing with other stakeholders

All ACT Alliance members are accountable to their own stakeholders such as governance structures, donors, members, governments authorities, relevant laws, etc. At the same time, they are responsible for meeting their obligations to ACT Alliance under the Membership Agreement and the ACT Code of Good Practice.

ACT Alliance members share data with stakeholders only when it's a legal or project implementation requirement to do so. Before sharing data, members should analyse any potential risks associated with data misuse and so ensure that no harm is created for the communities or individuals involved.

Communities will be informed about what data is provided to other stakeholders.[4] Under no circumstances will information be shared without first clarifying how the data will be used and safeguarded. In cases where, as part of project implementation, the information about right holders is shared with third parties such as banks and/or commercial organizations (e.g. in cash-based projects, etc), agreements will be made to ensure data is stored securely in compliance with this data safeguarding policy.

ACT's implementing members will ensure that right holders are aware of the content of this policy.

Members are encouraged to ensure their local and national partners have similar mechanisms for data safeguarding in place at the project and programme level.

Data about the communities shouldn't be held longer than required and it should be destroyed and deleted.

All requests related to data will be responded to within 30 days, where possible. Requests related to data held by an ACT member should be addressed directly to that member.

7. Data Loss or Breaches

Members should put in place systems to mitigate the risk of data loss or other data breach. In case of data loss or data breach, all possible efforts should be made to ensure data recovery and to reestablish data security. A thorough investigation should be conducted to find out the reason(s) for a data loss or breach and to develop an action plan for improvement of internal processes to avoid such instances in future. Communities should be

[4] Under exceptional circumstances and for emergency purposes, such as humanitarian crisis, data can potentially be reused without additional consent as long as no individual can be identified. ACT Alliance members must have a clear routine and risk management for such exceptions.

informed immediately after (or within 24 hours of) discovery of any loss or breach of data pertaining to them, and authorities engaged or notified where required.

8. Implementation of the Policy

After approval of this policy by Governing Board, all members will be informed about policy and its significance via the ACT newsletter. Policy will be included in the ACT Quality & Accountability Framework. The Humanitarian Officers shall support in compliance to the policy during implementation of appeals and emergency projects. An e-Course on Data Safeguarding shall be made available for members at Fabo ACT Learn Platform. The ACT Reference Group on Quality & Accountability will be responsible for any revisions to the policy as well as advice to roll-out this policy. All the upcoming trainings (physical/online) on Quality & Accountability will include reference/briefing about the requirements under this policy.

ACT Alliance
Ecumenical Centre
150 route de Ferney
P.O. Box 2100 1211
Geneva
Switzerland
Phone: +41 22 791 6242

9. Glossary

Data
The term 'data' refers to facts, statistics or items of information about an individual/community supported by ACT members.

Data Subject
The term 'data subject' refers to any individual whose personal data is collected, held or processed by ACT members. Where, personal data is any data that can be used to identify an individual such as name, address, identity number, etc.

Right Holders
Individuals or community members that have entitlements in relation to ACT members engagement with them.