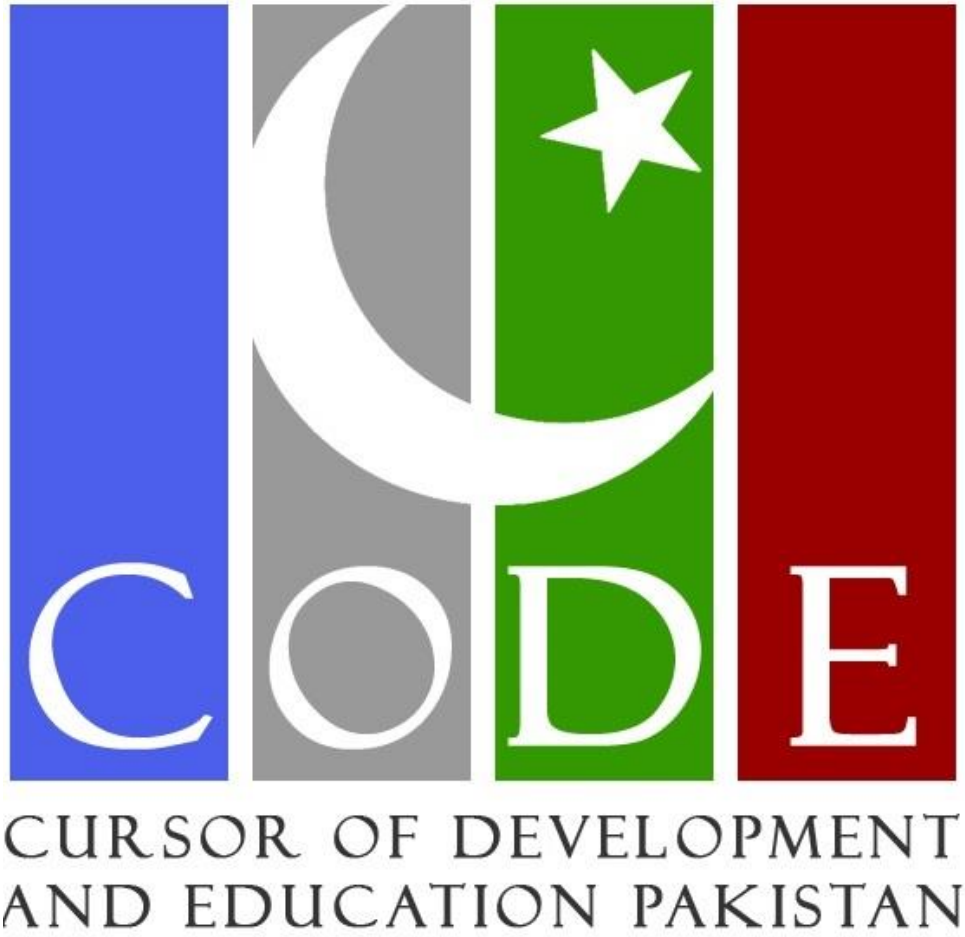
Data Sharing & Protection Protocols



CODE PAKISTAN

2023

Table of Contents

Introduction

Around the world, development and humanitarian practitioners increasingly collect, analyses and store large quantities of sensitive data, including individual beneficiary data. The need to coordinate humanitarian responses and ensure that no one is left behind makes sharing operational data essential to providing assistance to everyone who needs it. But it has also given rise to concerns about the safe handling of this data and the rights of individuals to have their data protected (do no harm). Therefore, Data Sharing Protocol (DSP) is to articulate the CODE Pakistan commitment to strong data protection policies and practices and to provide guidance on core principles that signatories commit to working toward. The DSP reflects existing humanitarian policies and established best practices for data use and outlines agreed expectations and minimum standards for the sharing of data between aid actors and the Government in Pakistan. CODE PAKISTAN believes that Data and information collection, sharing and management must adhere to data protection standards, principles of confidentiality and a defined purpose. It must be done in a manner that protects the individuals and groups providing information from harm, including through the use and respect of informed consent.

An Accountability to Affected People (AAP) and stakeholders' lens have been used to develop this protocol and to emphasize that stakeholders and departments being engaged are the owners of and decision-makers regarding their data. No decisions shall be taken for them without their consent.

This document should not be considered as static but will necessarily evolve to reflect new issues that arise in data collection and sharing over time, as well as new circumstances in the country that frame the development work and humanitarian response and CODE engagement with government departments and ministries and donors.

Objective

The objective of this DSP is to clearly articulate the rationale for data sharing in the development context and to establish basic principles and best-practice arrangements that signatories can commit to applying in their work.

Scope of the Protocol

The DSP covers all relevant phases of the data management process and multiple types of data, including but not limited to: the location of critical infrastructure, government departments data, humanitarian access data, needs assessment data, movement data and locations of affected people, community perception data, distribution data, data produced from collective analysis of Focus Group Discussions (FGDs), key informant interviews, Consultation, meetings, trainings and feedback and complaint mechanism (including referral) data.

The types of data covered in the DSP include:

Category of humanitarian data	Examples of data covered by the Protocol
Data about the context in which a development intervention is occurring	○ Government secondary data ○ Administrative Boundaries ○ Locations of schools, health facilities and other infrastructure

	○ Humanitarian access data ○ Development data ○ Political and socio-economic data
Data about the people engaged in the development intervention	○ Needs assessment data ○ Population figures ○ Movement data ○ Locations of people engaged
Data about the response by aid organizations and people seeking to help those who need assistance	○ Community perception data ○ Cash and aid distribution locations ○ Humanitarian financing data ○ Financial tracking data ○ Beneficiary feedback and complaint data

The principles outlined in the protocol cover all relevant phases within the data management process:

Classification of data

CODE Pakistan the international best practices for data safety and classifies data as per international data protection laws. These laws typically distinguish between categories of data, depending on how strictly the information must be protected. These categories are defined as follows:

Personal Data: Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Non-Personal Sensitive Data: Non-personal data which is classified as sensitive based on the likelihood and severity of potential harm that may materialize as a result of its exposure in a particular context. While most humanitarian organizations acknowledge the sensitivity of personal data such as names, biometric data, or ID numbers and anonymize datasets accordingly, it is often still possible to re-identify individual respondents or organizations by combining answers to different questions, even after such 'anonymization' is applied.

Thus, the classification of data should always take into account two dimensions:

1) the type of data (personal data and non-personal sensitive data), and
2) the aggregation level of the data (individual, household, village, district, province level, etc.)

Personal data of targeted populations should always be classified as confidential by default even if disclosure is unlikely to cause any harm. The classification table below provides general guidance on determining the sensitivity level and corresponding classification of different types of data covered by this protocol, and examples of appropriate dissemination methods.

Information and Data Sensitivity Classification					
Sensitivity	**Definition**	**Combination of type of data and aggregation level**	**Example**	**Classification**	**Example Dissemination Methods**
Low or No	Information or data that, if disclosed or accessed is unlikely to cause harm or negative impacts to affected people and/or humanitarian actors.	Low impact: When disclosing data aggregated at district, provincial or national levels, a minimal chance exists of affected people and/or humanitarian actors being negatively affected.	Anonymized data sets published for the purpose of research, benefit of the humanitarian community or response.	Public	Web HR Info Other response-specific public sites
Moderate	Information or data that, if disclosed or accessed without proper authorization, is likely to cause minor harm or negative impacts and/or be disadvantageous for affected people and/or humanitarian actors.	**Moderate impact**: Disclosure of non-authorized non-personal data at Village-level could lead to moderate harm or negative impacts.	Assessment data at the village level on the numbers of households affected, with a single contact number.	**Restricted**	Intra-cluster/sector mailing lists *[encrypting the file and using encrypted email, with passwords shared separately through a different secure channel]*
High	Information or data that, if disclosed or accessed without proper authorization, is likely to cause serious harm or	**High impact**: If the precise names and locations of individuals OR sensitive personal	Non-anonymized household or individual level assessment data including names, contact, numbers,	**Confidential**	Internal intra-cluster/ sector sharing only *[encrypting the file and using encrypted email,*

	negative impacts to affected people, humanitarian actors and/or damage to a response.	data at village level were disclosed, this would likely lead to physical harm, persecution, imprisonment or death of an individual.	locations		*with passwords shared separately through a different channel, or using an encrypted file transfer service]* Inter-cluster/sector sharing on case by case basis *[encrypting the file and using encrypted email or using an encrypted file transfer service, with passwords shared separately through a different secure channel]*
Severe	Information or data that, if disclosed or accessed without proper authorization, is likely to cause severe harm or negative impacts and/or damage to affected people and/or humanitarian actors and/or impede response activities.	**Severe impact**: If the precise names and locations of individuals AND their sensitive personal data were disclosed, this would likely lead to physical harm, harassment, imprisonment, or death of an individual.	Full assessment data sets including locations, GPS, personal information, and sensitive personal data	**Strictly Confidential**	Bilateral disclosure between organizations based on formal requests and, in some cases, bilateral data sharing agreements *[encrypting the file and using encrypted email or using an encrypted file transfer service,*

					with passwords shared separately through a different secure channel]

Guiding principles for data and information sharing and management
CODE Pakistan is practicing data safety and security protocols and the following principles have been adapted from the international best practices and standards and serve as a benchmark for the processing of non-personal data.

FAIR AND LEGITIMATE PROCESSING OF DATA:
Development interventions data should be processed in a fair manner, in accordance with the mandates and governing instruments, and on the basis of:

(i) the clear, freely given and informed consent of a data subject has been obtained;
(ii) in the public interest, understood in this context as consistent with the organization's humanitarian mandate
(iii) in the vital interests or best interest of a data subject who is not able to make a determination about data management him/herself, or;
(iv) any other legal basis specifically identified by the organization's regulatory framework or applicable laws, so long as these do not conflict with (i) through (iii)

PURPOSE SPECIFICATION: Data should be processed for specified purposes that are narrowly defined, consistent with organizational mandates and take into account the balancing of relevant rights, freedoms and interests. Personal data or non-personal sensitive data should not be shared with third parties without an express purpose and without data safety policies being in place.

NECESSITY, RELEVANCE AND ADEQUACY OF DATA PROCESSING: The processing of data should be relevant, limited and adequate to what is necessary for data processing.

RETENTION: Data should only be retained as long as necessary to fulfil the purpose for which it was collected. Personal data and other sensitive data should only be retained for as long as it is necessary for the specified purpose for which it is being managed or as required by applicable law or regulations.

ACCURACY: Data should be accurate and, when necessary, up to date to meet the specified purposes. There should be capacity to have specific data on crisis-affected individuals removed from databases at the individual's request or when it is no longer accurate.

CONFIDENTIALITY: Data should be processed with due regard to confidentiality and not shared with third parties without consent.

SECURITY: Appropriate organizational, administrative, physical and technical safeguards and

procedures should be implemented to protect the security of data, including against or from unauthorized or accidental access, purposeful misuse, damage, loss or other risks presented by data processing. Training should be provided to staff who manage such information so that they are aware of their obligations.

TRANSPARENCY: Processing of personal data should be carried out with transparency to data subjects, as appropriate and whenever possible. This should include, for example, the provision of information about the processing of humanitarian data, as well as information on how to request access, verification, rectification, and/or deletion of that humanitarian data, insofar as the specified purpose for which humanitarian data is processed is not undermined.

ACCOUNTABILITY: Civil Society organizations should have adequate policies and mechanisms in place to adhere to these Principles.

DATA OWNERSHIP: Development intervention stakeholders including beneficiaries are the primary owners of their data. Organizations should have policies requiring staff to inform crisis-affected people of that fact, and of their right to keep their personal data private.

GLOBAL OBLIGATIONS: Processing of data must comply with relevant global data standards and protocols.

Informed consent

CODE Pakistan manages personal and non-personal sensitive data in accordance with mandates, the context of the response, governing instruments and global norms and standards including global best practices. Data is processed on the basis of one of the following legal bases, in order of priority:

a. the explicit, freely given and informed consent of a data subject has been obtained;
b. in the public interest, understood in this context as consistent with the organization's humanitarian mandate
c. in the vital interests or best interest of a data subject who is not able to make a determination about data management him/herself, or;
d. any other legal basis specifically identified by the organization's regulatory framework or applicable laws, so long as these do not conflict with (a through (c).

When requested, consent is to be given unambiguously through accessible and appropriate methods, enabling a freely given, specific and informed indication of the data subject's wishes, either by a written, oral or other statement, or by a clear affirmative action by the data subject signifying their agreement to have their personal data processed. The data controller is obliged to keep record of when and how the data subject provided explicit consent for any collection and subsequent use of their data. Informed consent should always be obtained in ways that are culturally and linguistically appropriate and relevant (verbal or written), and the collection of information should not take place until field staff have been trained to ensure that principles of informed consent are understood and respected. Where consent has not been requested, or has not been recorded, the information must not be transmitted to a third party. In such circumstances, it would be necessary to revisit the participant, in order to request and obtain consent before transmitting the information.

Consent covers all data processing activities carried out for the same purpose. The data subject should receive explanations in clear terms and in the language she/he prefers (verbal or written), as to the following:

- the identity and contact details of the data controller;
- the specific purpose for processing of his/her personal data and an explanation of the potential risks and benefits;
- the fact that the data controller may process his/her personal data for purposes other than those initially specified at the time of collection, if compatible with a specific purpose mentioned above; circumstances in which it might not be possible to treat his/her personal data confidentially;
- the data subject's rights and limitations on his/her rights to access, correct and delete her/his

personal data and object to processing, either at the time of collection or later;
- an indication of the security measures implemented by the data controller regarding data processing;
- a process and a communication channel for the subject to inform the data controller that he/she wants personal information kept private;
- that the data controller may need to transfer data to another country; and
- an indication of the data controller's policy on record retention (how long records are kept and any steps taken to ensure that records are accurate and kept up to date), whether a data subject's personal data can be shared with other organizations, with the Government in the country of data collection or another country, or be publicly disclosed and to approve that their personal data be used as explained.

Sensitive and non - sensitive referrals

A referral is the process of directing a data subject (beneficiary) to another service provider because s/he requires help that is beyond the expertise or scope of work of the current service provider. A referral can be made to a variety of services, for example health, psychosocial support, protection services, nutrition, education, shelter, material or financial assistance, physical rehabilitation, community center and/or a social service agency. Similarly, with the consent of the beneficiary, referrals can be made to humanitarian, development or government entities.

Whether the case being referred between service providers is sensitive or non-sensitive, all referrals should include basic steps:

- Identification of org/orgs who are able to meet this need
- Engagement with identified service provider to confirm that the intended beneficiary meets the eligibility criteria of the identified services provider
- A detailed explanation of the referral process to the intended beneficiary. Information provided should include details regarding which services are available, where the service provider is located, and how the service provider can be accessed. A clear option for the beneficiary to decline referral should also be provided
- If the beneficiary consents to the referral, documented consent of the beneficiary should be obtained
- A referral form should be filled in. Electronic copies of the referral form should be provided to the referring agency, the beneficiary, and the receiving agency
- All referral forms and case files should be stored in secure locations to ensure safe data processing

Specific concerns with information related to the reporting human rights abuses and/or Protection concerns

The very act of collecting, processing and transmitting information on abuses can endanger individuals or groups, especially if they are singled out in the process. Special considerations must be given to minimize risks which may arise from the transmission of information to a potentially dangerous authority.

Having identified potential risks, procedural mechanisms need to be put in place to minimize adverse outcomes. These might include methods of transmitting information that conceal the sources of information or identity of victims, or deferring interviews with sources and witnesses until they are no longer within reach of those who might seek to persecute them. If it is estimated that the risks are too high, and if the protection actor lacks adequate mechanisms to manage them, it must consider forgoing the intended collection of protection information and directing victims and witnesses to other protection actors who are better equipped to handle the information.

Further consent is required whenever personal information is handed over to another protection actor, or to the authorities, especially when the information is likely to be used for purposes other than those for which it was originally collected. Exceptions apply when the protection of vital interests of the person concerned, or of others, are at stake, or when consent cannot be obtained and transmission is clearly in the best interest of the person concerned. This can happen, for example, when tracing missing persons, who simply cannot be reached for their consent. Others, such as children or patients undergoing psychiatric treatment, may not be in a position to anticipate or understand the risks entailed in providing information. Decisions should then be made based on an assessment of their best interests, in consultation with relatives, caregivers or others close to them. Having obtained the necessary informed consent does not remove the actor's responsibility to assess the risk, for an individual or a given group, of collecting, storing or processing sensitive information. If the risk is seen as too high, information should not be used or transmitted, even if informed consent was obtained.

Managing sensitive information

- CODE PAKISTAN specify how to manage sensitive information and the circumstances under which information may be referred. As far as possible, CODE PAKISTAN seeks the consent of the individuals concerned for the use of such information. Any referral of information is done in a way that does not put the source of information or the person/people referred to at risk of physical danger or any form of intimidation or abuse.

- Information on specific abuses and violations of rights is only collected if its intended use is made explicit and the detail required is defined in relation to the intended use. Such protection information should be collected by organizations with a protection mandate or those with the necessary capacity, skills, systems and protocols in place. Collecting this information is subject to informed consent and, in all cases, the individual's consent is necessary for the information to be shared with third parties. The default understanding is that if the person has NOT given consent, sharing with a third-party is prohibited. The possible reaction of the Government or other relevant authorities to the collection and use of information about abuses should be assessed.

Complaints about actors or intervention:

Complaints often include sensitive information requiring specific handling procedures. Sensitivities are not isolated and can span multiple layers of the development architecture, but most importantly include affected people. In managing this data, there are inherent risks such as accidental or unauthorized loss or disclosure, which may entail negative effects on the complainant including, but not limited to retaliation and threats to the safety of the individual. This becomes particularly critical when the complaint mentions a specific agency and/or name of a specific staff member in their community and/or the complaint involves government counterparts. Safeguarding the sharing of information between humanitarian actors is paramount.

All complaints should be treated with appropriate levels of confidentiality including the necessary data protection mechanisms (password protection, no sharing of databases, no sharing of non-anonymized data) in accordance with the organization's confidentiality guidelines. Staff handling complaints and feedback must be trained on how to route complaints to appropriate organizational and inter-agency focal points, observing principles of confidentiality.

Monitoring and evaluation of protocol

The status of the adoption and application of the DSP within the development interventions shall be reported on a regular basis. It is recommended that the CODE PAKISTAN management undertake an annual review of the effectiveness of the DSP and levels of implementation among the stakeholders engaged in the intervention.

Annex 1 – Information Sharing with A Third Party for Development Interventions

Principles for the secure use of personal data

a) CODE PAKISTAN shall collect personal data only for specific, explicit and legitimate purposes and shall further process it in a way that is compatible with those purposes. If a secondary purpose arises that is not compatible with the originally stated purpose, then beneficiary consent must be obtained for this secondary purpose.
b) CODE PAKISTAN should strictly adhere DSP for the Secure Use of Beneficiary Data in their own organization and for use by third parties for each programme intervention they initiate or implement.
c) CODE PAKISTAN analyses and document the flow of a beneficiary's data for each development intervention transaction within their own organization and between their organization and others, and develop risk mitigation strategies to address any risks arising from these flows.
d) CODE PAKISTAN ensures that the purpose of sharing beneficiary data with third parties prior to a programme starting. Contracts with third parties should contain and agreed upon data sharing policies and procedures, clearly establishing what the data can be used for.
e) Third parties should not be allowed to use the personal data for purposes other than those specified in the contract, as needed to deliver the programme or to which the beneficiary has given prior consent.
f) In the data collection stage, beneficiaries should be informed of the nature of the data collection, with whom it will be shared, who is responsible for the secure use of his/her data and be provided with the opportunity to question the use made of the data, and be informed that they can withdraw from the programme should they not wish their personal data to be used for the purposes described.
g) Organizations should implement appropriate technical/operational security standards for the transfer of beneficiary data to prevent unauthorized access, disclosure or loss. In particular, external threats should be identified and actions taken to mitigate risks.
h) Organizations should ensure third parties respect the confidentiality of personal data transferred to them through a written agreement by the third party that the personal data will be kept confidential at all times.
i) If the third party uses digital systems, ensure their digital storage systems are encrypted and password protected, and if hard copies of records are retained that include beneficiary data, make sure these records are kept securely.
j) Organization must ensure that beneficiary data is not held by third parties for longer than is required in the contract into fulfil the specific purposes for which they were collected unless retention is specifically for repeat distributions.
k) When organizations operate together in a consortium, it should be agreed and documented within that consortium which organization is responsible for leading on beneficiary data protection and sharing. A lead partner also should be designated in a consortium to ensure that adequate protections are built into programme design so that each agency operates by common standards that ensure the integrity, protection and use of personal data that benefits the beneficiary.
l) Organization may not use the third party's service if the risks associated with data sharing of vulnerable groups or communities are high.