Data Sharing Agreement

Overview/Background:

- A data sharing agreement establishes the terms and conditions that govern the sharing of specific personal and sensitive non-personal data between two or more parties.
- This type of agreement is essential to upholding legal, policy and normative requirements related to the sharing of personal and sensitive non-personal data, as well as to establish the roles and responsibilities of the Parties in the data sharing vis-à-vis data subjects.
- Organizational policies and applicable legislation may require a data sharing agreement for personal data. Always consult colleagues responsible for personal data protection in your organization, and refer to policies and legislation as these take precedence over this template. If no other guidance or template is available, refer to this template to develop a data sharing agreement.
- This template is intended to guide users in the development of a data sharing agreement. The template includes several key clauses that should be included in such agreements. The examples provided in the clauses below may be adapted to the context of the data sharing.

While these points typically cover the necessary precautions for the protection of personal and other sensitive data, it is critical that humanitarians carefully consider before data sharing. Sharing personal and other sensitive data can create or exacerbate risk of harm, exploitation or other negative effects for data subjects.

Feedback on this template can be sent to centrehumdata@un.org and iasccorrespondence@un.org.

Preparation

Before drafting the Agreement, consider the following:

1. Determine whether any personal data is shared under this agreement. The sharing of personal data will be governed by applicable data protection legislation or policies. Please consult colleagues responsible for personal data protection in your organization, and refer to policies and legislation as these take precedence over this template.

2. Determine which data responsibility framework applies. This will depend on the data being shared (see point below), the parties involved, the location where the data is processed and the location of the organization's headquarters, as well as their role in the data sharing.
    a. If personal data is being shared, determine which data protection legislation applies. If international organizations with privileges and immunities are among the parties, national and regional legislation will not apply to them. All of the points below should be informed by provisions in applicable data protection legislation/frameworks.

3. It may be recommended to conduct a Data Impact Assessment (DIA) before sharing data with humanitarian partners.[1] A DIA helps determine the expected impacts of a data management activity and identify recommendations to mitigate the potential negative impacts of the envisaged data sharing. These recommendations should be implemented before sharing data.
    a. Some data protection legislations require that a data transfer impact assessment is conducted before sharing personal data.

[1] More information on Data Impact Assessments is available here: https://centre.humdata.org/wp-content/uploads/2020/07/guidance_note_data_impact_assessments.pdf

Data Sharing Agreement

Between

[*INSERT NAME of 1st party*]

and

[*INSERT NAME of 2nd party*]

on [*INSERT DATE*]

This Data Sharing Agreement is entered into by [*INSERT NAME of 1st party*] hereinafter referred to as "[X]", and [*INSERT NAME of 2nd party*], hereinafter referred to as the "[X]".

This agreement covers the sharing of [*INSERT DESCRIPTION OF DATA*].

1. **DEFINITIONS**
   Parties should agree on a set of definitions, including the roles of the parties, that will be referred to throughout the agreement.[2]
   a. *(Recipient - Sender).*
   b. *In the case of personal data, this relationship will be that of Data Controller and Data Processor (or Data Controller - Data Controller, Joint Controllership). This is about establishing responsibilities vis-à-vis the data subjects.*
      [add clause]

2. **[for personal data only] GOVERNING LAW**
   Reflect applicable data protection framework.
   [add clause]

3. **PURPOSE**
   Specify purpose(s) for sharing data. Any subsequent processing of data must be compatible with the established purpose.
   [add clause, for example: to conduct analysis and derive insight to inform the design of humanitarian interventions; or to support the generation of a needs overview for response context Y, or to select individuals for the distribution of assistance based on their vulnerabilities, etc.]

4. **SCOPE**
   In line with and strictly limited to what is required for meeting the specific purpose, define the scope of the data to be shared. Wherever the intended use of the data allows, personal data should be anonymized before sharing.

Dataset(s) name(s)	Description

[2] The IASC Operational Guidance on Data Responsibility in Humanitarian Action and the ICRC Handbook on Data Protection in Humanitarian Action and applicable national laws contain a set of standard definitions to use.

[insert dataset(s) name(s) and/or specific data points]	[include: a description of the data itself, e.g. # of households, specific geographic area, variables included / excluded]

5. [for personal data only] LEGAL BASIS

For each specified purpose, determine the legal basis for data sharing. The possible legal bases are prescribed in the data protection framework applicable to the parties. The choice of legal basis depends on the objective circumstances of the sharing, particularly on establishing whether the data subject has a free choice to accept or refuse the data processing without suffering a serious detriment (eg. losing access to humanitarian assistance and protection).[3] [add clause]

6. DATA CONFIDENTIALITY AND SECURITY

Establish the required measures to ensure data confidentiality and security throughout the sharing process. This includes minimum technical and procedural requirements for data security, such as encrypted means of data sharing and storage:
[add clause, e.g. including the following examples:

- *Personal and other sensitive data should be shared via secure channels that provide end-to-end encryption, with passwords always shared separately and through a different channel than the message through which the Data is shared.*
- *Personal and other sensitive data should be stored / hosted by both parties in a secure, encrypted storage modality.*
- *Access to personal and other sensitive data should be subject to clear access management and oversight procedures, and should only be available to personnel that require access to fulfill the specified purpose of data sharing.]*

7. ONWARD DATA SHARING

Determine the parameters for onward sharing, including the following examples:

- *Parties should agree whether onward sharing of the data is authorized for specific third parties, and/or establish a process for authorizing onward sharing of personal and other sensitive data with other third parties. Parties should agree on the conditions for sharing or publication of information products and anonymized datasets derived from personal data.*
- *The Recipient should not copy, retain or release personal and other sensitive data, whether in its original form, altered, aggregated or otherwise changed, to a third party without prior approval from the sender.*
- *Sharing of information products based on personal data and other sensitive data received should be subject to prior approval from the sender*
- *[add clause, for example: any third party granted access to the shared data should be subject to approval from the other party, and such sharing should be subject to the same safeguards as set out in this agreement.]*

[3] See further Chapter 3 of the ICRC Handbook on Data Protection in Humanitarian Action; for GDPR context see also Guidelines 05/2020 on consent under Regulation 2016/679: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

8. DATA INCIDENT MANAGEMENT

Establish a data incident management protocol with required actions in case of a data incident.[4] If such an incident occurs, each party must take appropriate and adequate steps, including to (i) notify the other party that an incident has occurred, (ii) classify incident and (iii) treat the incident by rectifying the vulnerability and mitigating any potential harm, including, if necessary, notifying the data subjects about the breach.

[add clause]

9. [for personal data only] DATA SUBJECTS' RIGHTS AND REMEDIES

Establish the responsibilities of Parties to the agreement via-s-vis data subjects. The responsibilities of the Parties will depend on their roles as Data Controller or Data Processor .

[add clause, including the following:

a. *For example, a Data Processor will need to be provided with detailed instructions by the Data Controller on:*
    i. *How to inform the data subjects about the data processing;*
    ii. *How to respond to requests by data subjects or escalate them for data controller's attention;*
    iii. *How to refer complaints by data subjects for the data controller's attention.*
b. *Where the Parties are separate or joint data controllers, the agreement may establish how they coordinate the requests by data subjects and the minimum information notice that shall be provided to the data subjects.]*

10. DATA RETENTION AND DESTRUCTION

Parties to the agreement should abide by a clear data retention period and the destruction protocol. The responsibility for establishing the retention period, the purposes and legal basis of retention lies with the data sender/controller.

[add clause]

11. DISPUTE RESOLUTION

Determine what should happen if the agreed terms for the shared data are breached, and how any disputes between parties should be resolved. This is likely to be covered in applicable data protection legislation or, in the case of sharing with international organizations, in applicable public international law.

[add clause]

12. ENTRY INTO FORCE

Determine when the agreement will enter into force. This is typically upon signature by the duly authorized representatives of the parties.

This agreement applies from the moment of signature by the duly authorized representatives of [insert sender name] and [insert recipient name].

---

[4] A data incident is a data management related event that has caused harm or has the potential to cause harm to crisis affected populations, organizations, and other individuals or groups. Data incidents may include physical breaches of infrastructure, unauthorized disclosure of data, and the use of 'anonymised' beneficiary data for non-humanitarian purposes, among others. For more information, see here: https://centre.humdata.org/wp-content/uploads/2019/08/guidanceNote2_dataincidentmanagement.pdf

13. SIGNATURES

Ensure the document is signed appropriately by duly authorized representatives of both parties.

1st party FOCAL POINT NAME	2nd party FOCAL POINT NAME
FOCAL POINT SIGNATURE	FOCAL POINT SIGNATURE
DATE	DATE