**Information Sharing Protocol**

|  |
| --- |
| Version française [ci-dessous](#_2bga9kgzde23). |

|  |
| --- |
| **Overview/Background:**   * An Information Sharing Protocol (ISP) serves as the foundation for a collective approach to responsible information and data exchange. While typically established at the system-wide level, ISPs may also be established at the cluster/sector and organization level as needed. * An ISP should include a context-specific data and information sensitivity classification, articulate common actions for data responsibility (including a process for data incident management), and specify how to handle breaches to the protocol.      * The template is based on the ISP template in the OCHA Data Responsibility Guidelines, which has been adapted and implemented in a range of complex humanitarian response settings since the release of the Guidelines in 2019. The template presented here also reflects best practice from a range of other resources reviewed during the development of the IASC Operational Guidance on Data Responsibility in Humanitarian Action.   **Instructions for Use**   * The template is designed to be adapted and tailored to specific contexts. It should be supplemented with additional directives and instructions as necessary (e.g. an additional section regarding data protection would be valuable in a Protection Sector ISP where highly sensitive personal data is being managed). The relevant text to be adapted by the user is highlighted in [green].      * At the system-wide level, the ISP should be developed through a collective exercise led by the **relevant interagency mechanism(s)** (both the **ICCM/ICCG/ISCG** and the **IMWG**) with support from **OCHA**. Once drafted, the ISP should be presented to the **HCT** for review and endorsement. All stakeholders involved in data management should be aware of the ISP and their respective obligations.      * At the cluster/sector level, the ISP should be developed through a collective exercise led by the **Cluster/Sector Lead and Co-Lead** in collaboration with their **partners**. Once drafted, the ISP should be endorsed by all cluster/sector partners and presented to the relevant inter-agency mechanism(s) for reference. * Feedback on this template can be sent to iasccorrespondence@un.org and centrehumdata@un.org. |

**INFORMATION SHARING PROTOCOL**

[NAME OF COUNTRY AND/OR SECTOR / CLUSTER]

[DATE]

# **OVERVIEW**

This Information Sharing Protocol (ISP) is designed to support *data responsibility -- the safe, ethical, and effective management of data -* within [NAME OF COUNTRY AND/OR SECTOR / CLUSTER]. It establishes a common set of principles[[1]](#footnote-1), an approach, and roles and responsibilities for data and information sharing across different humanitarian functions and activities. It provides a common framework for information and data exchange, informed by a shared definition of sensitivity and conditions for disclosure.

This ISP covers all data and information management activities in the [NAME OF COUNTRY AND/OR SECTOR / CLUSTER] humanitarian response. For the purpose of this protocole, ‘information’ refers to both raw data and the information products developed from it. This ISP applies to all humanitarian actors present in and supporting response activities in [NAME OF COUNTRY AND/OR SECTOR / CLUSTER], including United Nations entities, other international organizations, international and national non-governmental organizations (NGOs), third parties, and other relevant stakeholders.

The ISP has been developed through a collective exercise led by [NAME OF SECTOR / CLUSTER; ICCM/ICSG/ICCG and IMWG] in accordance with the Inter-Agency Standing Committee (IASC) Operational Guidance on Data Responsibility.[[2]](#footnote-2) The ISP has been endorsed by [RELEVANT HCT].

In this context, this ISP serves as the primary document governing data and information sharing in the [NAME OF COUNTRY AND/OR SECTOR / CLUSTER] response. It is designed to complement existing policies and guidelines and does not in any way affect or replace obligations contained in applicable legal and regulatory frameworks, cluster/sector- and AOR-specific protocols, or organizational policies.

The ISP will be reviewed and updated on a regular basis through a collaborative process overseen by the [relevant coordination mechanism in NAME OF COUNTRY AND/OR SECTOR, e.g. ICCM, ICCG, ISCG] and subject to review and endorsement by the HCT. Participation of cluster-/sector-level counterparts in response-wide mechanisms is key to consistent and harmonized decision-making at the response level. This includes monitoring and reporting on progress, challenges and opportunities for responsible data management.

**PURPOSE AND OBJECTIVES**

The purpose and objectives of responsible data and information sharing include:

* Conducting joint analysis (e.g. coordinated assessments) and avoiding duplication of data management efforts
* Better triangulation of information
* Ability to provide regular, credible situation analysis, response monitoring, reporting, and recommendations
* Improved inter-agency collaboration and strengthened operational coordination
* Improved protection and response to affected populations, including vulnerable groups such as survivors and individuals at heightened risk
* [Insert any other relevant objectives of this ISP]

# 

# **APPLICATION AND SCOPE**

This ISP applies to all humanitarian actors, including United Nations entities, other international organizations, international and national Non-Governmental Organizations (NGOs), and other stakeholders engaged in the delivery of humanitarian assistance in [NAME OF COUNTRY AND/OR SECTOR / CLUSTER].

The ISP applies to **information sharing** in the context of all forms of operational data management activities taking place in [NAME OF COUNTRY AND/OR SECTOR / CLUSTER]. ‘Information sharing’ is defined as the transfer of raw data or information products developed from it, either through digital means (e.g. email, file transfer services, or otherwise) or physical means (e.g. passing a laptop, usb stick or other storage device). Exposure of information (e.g. showing a screen with information on it, showing a report) is included in this definition and subject to the same restrictions as the actual transfer of data or information.

The ISP covers all operational data and information generated and used in the [NAME OF COUNTRY AND/OR SECTOR / CLUSTER] response. For the purposes of this ISP, raw data and the information products (e.g. infographics, charts and maps, situation reports, etc.) developed from it are referred to as ‘information’, which includes the following[[3]](#footnote-3):

* **Data about the context** in which a response is taking place (e.g., legal frameworks, political, social and economic conditions, infrastructure, etc.) and the humanitarian situation of focus (e.g., security incidents, protection risks, drivers and underlying causes/factors of the situation or crisis).
* **Data about the people affected by the situation** and their needs, the threats and vulnerabilities they face, and their capacities.
* **Data about humanitarian response actors and their activities** (e.g., as reported in 3W/4W/5W).

This ISP does not apply to the management of ‘corporate’ data such as data related to internal financial management, supply, human resources and personnel, and other administrative functions in humanitarian organizations. The management of such data should be governed by relevant organizational policies. This ISP does not supersede or amend existing internal policies relating to mandatory organizational policies.

# **DATA AND INFORMATION SENSITIVITY**

The Data and Information Sensitivity Classification indicates the level of sensitivity of different types of data and information for a given context. Data sensitivity is the classification of data based on the likelihood and severity of potential harm that may materialize as a result of its exposure in a particular context.[[4]](#footnote-4) If disclosed or accessed without proper authorization, sensitive data and information are likely to cause:

* harm (negative implications of a data processing initiative on the rights of a data subject, or a group of data subjects, including but not limited to physical and psychological harm, discrimination and denial of access to services);
* a negative impact on the capacity of an individual organization or the broader humanitarian community to carry out its activities, or on public perceptions of an individual organization or the response;[[5]](#footnote-5)
* an erosion of trust within the humanitarian community or between humanitarian actors and key stakeholders in the broader response context (e.g. if sensitive data is disclosed without the source’s consent, this may impact the relationship with the organization and the data flow on a regular basis).

Some types of data are categorically considered sensitive. These include:

* Personal data (e.g. name, phone number, home address, national identity number, date of birth)
* Disaggregated (household-level) assessment data
* Unprocessed Individual survey results (microdata)

# 

Under this ISP, data and information should be shared in-line with the parameters presented in the table below. This Sensitivity Classification should be developed through a collective exercise in which different stakeholders -- including the affected population -- align on what constitutes sensitive data in their context. While this table presents the default classification for various data and information types, the classification and associated dissemination method may vary based on the specific circumstances of a given case (e.g. cases in which the identity of a humanitarian actor should not be disclosed, or data relating to particularly vulnerable groups). Ultimately, data responsibility requires the buy-in and participation of all functions across each organization, cluster/sector, and the humanitarian system at large. As the sensitivity of data and information may change over time as the response context evolves, the ICCM will review and revise this classification every six months.

|  |
| --- |
| **Instructions for the Data and Sensitivity Classification**  **1**. List the types of data and information that are being collected in your exercise. Examples  of types of such data and information are listed in the table below.  **2**. Please consult the table below and carefully read the information and data sensitivity  classification which help inform the level of sensitivity of the data or information at hand.  **3**. According to the classification in the table, determine the level of sensitivity for each type  of data and information and insert them in the corresponding column of the table. |

|  |  |  |
| --- | --- | --- |
| **Data and Information Sensitivity Classification for** [NAME OF COUNTRY AND/OR SECTOR / CLUSTER] | | |
| **Sensitivity Level** | **Data and Information Types**  *Fill in the relevant data and information types and indicate the appropriate treatment (e.g. level of aggregation, required disclosure control methods, etc.) for each level of sensitivity. Examples are included for reference.* | **Classification and Dissemination Methods**  *Fill in the appropriate dissemination method(s) for each level of sensitivity and corresponding classification. Examples are included for reference.* |
| **Low or No Sensitivity**  Information or data that, if disclosed or accessed without proper authorization, **are unlikely to cause any harm or negative impacts** to affected people and/or humanitarian actors. | - HNO and underlying national-level aggregate survey results  - CODs  - Access restrictions (district level)  - 3W/4W data (at national and district level) | **Classification: Public**  Data or information may be publicly disclosed.  Methods for sharing public data:   * ReliefWeb * HRInfo * HDX * Other response-specific public sites |
| **Moderate Sensitivity**  Information or data that, if disclosed or accessed without proper authorization, **are likely to cause minor harm or negative impacts and/or be disadvantageous** for affected people and/or humanitarian actors. | - Aggregated survey results (e.g. aggregated to the district level)  - 3W/4W data\* (for x, y and z clusters, this data at XX level is restricted) | **Classification: Restricted**  Data or information can be shared within a wider humanitarian community, based on a clearly specified purpose and related standards for data protection.  Methods for sharing restricted data:   * HDX [via HDX Connect] * Intra-sector mailing lists |
| **High Sensitivity**  Information or data that, if disclosed or accessed without proper authorization, **are likely to cause serious harm or negative impacts** to affected people and/or humanitarian actors and/or damage to a response. | - Aggregated survey results (e.g. aggregated to the household level and with additional disaggregation based on different indicators)  - Beneficiary lists  - Aid-Worker Contact Details / Lists | **Classification: Confidential**  Data or information can be disclosed within an organization or small community of organizations directly involved in delivering humanitarian assistance**,** based on a clearly specified purpose and related standards for data protection.  Methods for sharing confidential data:   * Internal intra-sector sharing only * Inter-sector sharing on case by case basis * HDX Connect |
| **Severe Sensitivity**  Information or data that, if disclosed or accessed without proper authorization, **are likely to cause severe harm or negative impacts and/or damage** to affected people and/or humanitarian actors and/or impede the conduct of the work of a response. | - Raw survey data, e.g. individual survey responses at HH-level data  - Personal data of beneficiaries (i.e. Beneficiary lists)[[6]](#footnote-6), | **Classification: Strictly Confidential**  Highly limited, bilateral disclosure only. Determined and approved on a case-by-case basis, with assurance of upholding the highest standards of data protections.  Methods for sharing strictly confidential data:   * Bilateral disclosure between organizations based on formal requests and, in some cases, bilateral data sharing agreements |

# 

# Whenever possible, [NAME OF SECTOR / CLUSTER; ICCM or / ICSG] members, cluster leads and members, and individual organizations should strive to share data in a timely manner through the appropriate channels, based on the classification and recommended dissemination methods in the table above.

# 

# **ACTIONS FOR DATA RESPONSIBILITY**

Data responsibility requires the implementation of principled actions at all levels of a humanitarian response. These include for example actions to ensure data protection and data security, as well as strategies to mitigate risks while maximizing benefits in all steps of operational data management as defined below. See the *IASC Operational Guidance on Data Responsibility in Humanitarian Action*[[7]](#footnote-7) for a complete overview of the actions.

[SPECIFY A SELECTION OF PRIORITY ACTIONS FOR YOUR CONTEXT HERE AS APPROPRIATE]

**DATA INCIDENT MANAGEMENT**

Data incident management helps reduce the risk of incidents occurring, supports the development of a knowledge base, and fosters more coordinated approaches to incident management over time. Data incidents are events involving the management of data that have caused harm or have the potential to cause harm to crisis affected populations, organizations, and other individuals or groups. Data incidents include:

* Unwarranted or unauthorized disclosure of data
* Loss, destruction, damage, or corruption of data

Organizational processes should provide for clear accountability mechanisms and escalation paths for cases where a data breach or other incident occurs. Data incidents should be addressed as soon as possible and be recorded in order to prevent them from reoccurring. A standard approach for data incident management in humanitarian response is outlined in this guidance note[[8]](#footnote-8).

While data incident management should be handled primarily at the organizational level, it is important to track incidents across the response in a common registry that captures key details about the nature, severity, and resolution of different incidents.[[9]](#footnote-9) Under this ISP, the ICCM and the individual Clusters are tasked with supporting this activity.

# **BREACHES TO THE PROTOCOL AND DISPUTE RESOLUTION**

Should there be a breach of this Protocol by any of the participating members, members will work to resolve such issues bilaterally. If a resolution cannot be reached, the Chair of the [relevant coordination mechanism in NAME OF COUNTRY AND/OR SECTOR, e.g. ICCM, ICCG, ISCG] should organize a dedicated meeting with the parties concerned to determine the appropriate course of action.

In case of differences in interpretation of this ISP or other related disputes, the [relevant coordination mechanism in NAME OF COUNTRY AND/OR SECTOR, e.g. ICCM, ICCG, ISCG] will be responsible for finding an amenable resolution. If such a resolution cannot be found, the chair of the [relevant coordination mechanism in NAME OF COUNTRY AND/OR SECTOR, e.g. ICCM, ICCG, ISCG] will refer the dispute to the Humanitarian Country Team (HCT).

**Annex A: Principles for Data Responsibility in Humanitarian Action**

The following Principles for Data Responsibility in Humanitarian Action (hereafter ‘the Principles’) are designed to inform safe, ethical and effective operational data management within organizations, clusters/sectors, and the broader humanitarian system in a given response context. They should serve as a normative guide for actors implementing the recommended actions for data responsibility outlined in this Operational Guidance. The Principles do not represent a compliance standard.

These Principles are based on a review of existing principles for data management (including data protection) across the humanitarian and development sectors.[[10]](#footnote-10) The review revealed gaps in guidance for operational data management at the system-wide and cluster/sector level, as well as gaps in guidance for the management of non-personal data at all levels of humanitarian response. The Principles help to fill these gaps and to ensure safe, ethical and effective data management. In this way, they reinforce humanitarians' overarching commitment to **Do No Harm** while **maximizing the benefits** of data in humanitarian action.[[11]](#footnote-11) The Principles also reaffirm the centrality of affected people and their rights and well-being in humanitarian action.

The management of **personal** **data** should be informed by the *Personal Data Protection Principle*,[[12]](#footnote-12) while the management of **non-personal data** should be informed by the other Principles. The Principles are presented in alphabetical order, and no hierarchy is intended.

Wherever these Principles conflict with one another in their interpretation or application, they should be balanced against each other based on the particular dynamics of the response context.[[13]](#footnote-13) In the event that the Principles conflict with either internal policies or applicable legal obligations, the latter take precedent.

**Principles for Data Responsibility in Humanitarian Action**

**Accountability**

In accordance with relevant applicable rules, humanitarian organizations have an obligation to account and accept responsibility for their data management activities. Humanitarian organizations are accountable to people affected by crisis, to internal governance structures, to national and international humanitarian partners, and, if applicable, to national governments and regulatory bodies. To achieve their accountability commitments, humanitarian organizations should put in place all measures required to uphold and monitor adherence to these Principles. This includes establishing adequate policies and mechanisms and ensuring the availability of sufficient competencies and capacities, including but not limited to personnel, resource and infrastructure capacity.[[14]](#footnote-14)

**Confidentiality**

Humanitarian organizations should implement appropriate organizational safeguards and procedures to keep sensitive data confidential at all times. Measures should be in line with general confidentiality standards as well as standards specific to the humanitarian sector[[15]](#footnote-15) and applicable organizational policies and legal requirements, while taking into account the context and associated risks.

**Coordination and Collaboration**

Coordinated and collaborative data management entails the meaningful inclusion of humanitarian partners, national and local authorities, people affected by crisis, and other stakeholders in data management activities, all where appropriate and without compromising the humanitarian principles[[16]](#footnote-16) or these Principles. Coordination and collaboration should also aim to ensure that appropriate connections are established between humanitarian operational data management activities and longer-term development-oriented data processes and data investments. Local and national capacity should be strengthened wherever possible, and not be undermined.

**Data Security**

Humanitarian organizations should implement appropriate organizational and technical safeguards, procedures and systems to prevent, mitigate, report and respond to security breaches. These measures should be sufficient to protect against external breaches as well as unauthorized or inappropriate internal access or manipulation, accidental disclosure, damage, alteration, loss, and other risks related to data management. Measures should be adjusted based on the sensitivity of the data managed and updated as data security best practice develops, both for digital data and analogue data.

**Defined Purpose, Necessity and Proportionality**

Humanitarian data management and its related activities should have a clearly defined purpose. The design of processes and systems for data management should contribute to improved humanitarian outcomes, be consistent with relevant mandates and relevant rights and freedoms, and carefully balance those where needed. In line with the concept of data minimization, the management of data in humanitarian response should be relevant, limited and proportionate – in terms of required investment as well as identified risk – to the specified purpose(s).

**Fairness and Legitimacy**

Humanitarian organizations should manage data in a fair and legitimate manner, in accordance with their mandates, the context of the response, governing instruments, and global norms and standards, including the Humanitarian Principles. Legitimate grounds for data management include, for example: the best interests of people affected by crisis, consistent with the organization’s mandate; public interest in furtherance of the organization’s mandate; the vital interests of communities and individuals not able to make a determination about data management themselves; and any other legitimate ground specifically identified by the organization’s regulatory framework or applicable laws.

**Human Rights-Based Approach**

Data management should be designed and implemented in ways that respect, protect and promote the fulfilment of human rights, including the fundamental freedoms and principles of equality and non-discrimination as defined in human rights frameworks, as well as the more specific right to privacy and other data-related rights, and data-specific rights promulgated in applicable data protection legislation and other applicable regulation.

**People-Centered and Inclusive**

Affected populations should be afforded an opportunity to be included, represented, and empowered to exercise agency throughout data management whenever the operational context permits. Special efforts should be made to support the participation and engagement of people who are not well represented and may be marginalized in the data management activity at hand (e.g., due to age, gender and other diversity factors such as disability, ethnicity, religion, sexual orientation or other characteristics), or are otherwise ‘invisible’, consistent with commitments to leave no one behind. A people-centered and inclusive approach is particularly important in the development of context-specific norms and standards for data management.

**Personal Data Protection**

Humanitarian organizations have an obligation to adhere to (i) applicable national and regional data protection laws, or (ii) if they enjoy privileges and immunities such that national and regional laws do not apply to them, to their own data protection policies.[[17]](#footnote-17) These laws and policies contain the list of legitimate bases for the processing of personal data, including but not limited to consent.[[18]](#footnote-18) When designing data management systems, humanitarian organizations should meet the standards of privacy and data protection by design and by default. Humanitarian organizations should take personal data protection into consideration when developing open data frameworks. In line with their commitment to inclusivity and respect for human rights, they should ensure the rights of data subjects to be informed about the processing of their personal data, and to be able to access, correct, delete, or object to the processing of their personal data.

**Quality**

Data quality should be maintained such that users and key stakeholders are able to trust operational data management and its resulting products. Data quality entails that data is relevant, accurate, timely, complete, up-to-date and interpretable, in line with the intended use and as appropriate within the given context. Where feasible and appropriate, and without compromising these Principles, organizations should strive to collect and analyze data by age, sex and disability disaggregation, as well as by other diversity characteristics as relevant to the defined purpose(s) of an activity.   
  
**Retention and Destruction**  
Sensitive data should only be retained for as long as it is necessary to the specified purpose for which it is being managed or as required by applicable law or donor audit regulations. When its retention is required, safe and secure storage should be ensured to safeguard sensitive data from being misused or irresponsibly exposed. All other data may be retained indefinitely, provided that its level of sensitivity is reassessed at appropriate moments, that access rights can be established, and – for anonymized or aggregate data – that a re-identification assessment is conducted. Regardless of the sensitivity level, a retention schema should indicate when data should be destroyed and how to do so in a way that renders data retrieval impossible. Specific durations for retention should be defined where possible and, where this is not the case, specific periods for review of necessity should be set.  
  
**Transparency**  
Data management in humanitarian response should be carried out in ways that offer meaningful transparency toward stakeholders, notably affected populations. This should include provision of information about the data management activity and its outputs, as well as data sharing in ways that promote genuine understanding of the data management activity, its purpose, intended use and sharing, as well as any associated limitations and risks.

**Annex B: Other Information Sharing Protocols and Related Guidance in** [NAME OF COUNTRY AND/OR SECTOR]

At the time of writing, the following [relevant coordination mechanism in NAME OF COUNTRY AND/OR SECTOR, e.g. ICCM, ICCG, ISCG] had **country-specific** information sharing protocols or related documents in place:

**Annex C: Information Sharing with Third Parties (OPTIONAL)**

**Background**

Beyond the information sharing activities within the humanitarian community in [NAME OF COUNTRY AND/OR SECTOR / CLUSTER] as covered in this ISP, humanitarian actors may be asked to share information with different third parties. Information sharing by organizations subject to this ISP with such third parties who are not subject to the ISP (including donors, authorities, service providers, and others) should be guided by this Annex.

This Annex covers operational data and information generated and used by humanitarian actors in [NAME OF COUNTRY AND/OR SECTOR / CLUSTER]. Raw data and the information products (e.g. infographics, charts and maps, situation reports, etc.) developed from it are referred to collectively as ‘information’.

Information sharing with third parties is predicated on the principle of transparency and understanding that sharing of humanitarian information – including on needs assessments, analysis and response – is key to decision-making in a coordinated and effective response. In such information sharing, the humanity, neutrality, impartiality and independence of humanitarian organizations and their operations in [NAME OF COUNTRY AND/OR SECTOR / CLUSTER] must be ensured, and a level of data responsibility that is similar or equal to that provided by this ISP must be upheld.

In many instances, humanitarian organizations will have formal arrangements (e.g. contracts, MoUs, etc.) in place with different third parties that already specify clear terms for data sharing. Where possible, these terms should align with the overall approach to responsible data management outlined in this ISP while adhering to relevant institutional policies and related requirements. Where formal arrangements are being developed, the following considerations can help inform the design of such arrangements. Where such formal arrangements are *not* in place, the following considerations should inform the different steps of data sharing between humanitarian actors and third parties.

**Requests for Information**

Data and information sharing should only be done based on a specific request by third parties, and take into account the sensitivity of the information, the burden of requests on the sharing organization, the criticality of access needs, and longer term impact of sharing and interference in programming and operations. To meet this requirement, third party requests for information should adhere to the following criteria:

* **Written, formal and specific**

Requests for information should be (a) made in writing, (b) specify clearly which data is requested, (c) the format desired, and (d) the other elements specified below.

* **Define a specified purpose**

The purpose for which information is requested should be clear and explicit from the request.

* **Proportionate and necessary**

The information requested should be proportionate and necessary to fulfil the specified purpose.

* **Restricted in scope and duration**

Third parties should only request the information required to meet the specified purpose for which it is being requested, and should indicate a timeline for destruction of the data.

* **Coordinated and consistent**

Third parties should ensure that requests for information of a similar type are consistently formulated to all partners concerned. Where relevant, third parties should direct requests for information from joint or coordinated data management exercises to the appropriate cluster lead or inter-agency body.

**Responses and Information Sharing**

All requests for information should be logged by the organization receiving the request. If the third party request meets the criteria specified above and if an individual organization’s policy allows for data sharing as requested, organizations subject to this ISP may share the requested information with the following safeguards in-place:

* **Secure information transfer as informed by the sensitivity classification**

Identify the channel through which information will be shared based on the sensitivity of the information as indicated by the latest version of the sensitivity classification included in this ISP.

* **Appropriate anonymisation and other preparation of information**

Prior to sharing the requested information, the responsible organization will ensure the appropriate precautions are taken, including the removal of names and other unique identifiers, and the application of methods such as Statistical Disclosure Control as needed.

* **Confidentiality requirements**

Organizations will set appropriate restrictions regarding onward sharing and publication of the information upon sharing. This should include an obligation to notify the sharing organization in case information is intentionally or accidentally shared with other parties than those agreed.

* **Consultation and alignment**

In cases where individual organizations are unsure whether a given request for information should be granted, they may consult the Inter-Cluster Coordination Mechanism and the Humanitarian Country Team for guidance.

# **PROTOCOLE DE PARTAGE DES INFORMATIONS**

|  |
| --- |
| **Contexte:**   * Un protocole de partage des informations (PPI) établit la base fondatrice pour une approche collective de l'échange responsable de données et d'informations. Bien qu'ils soient généralement établis au niveau du système, les PPI peuvent également être établis au niveau des clusters/secteurs et des organisations, au besoin. * Un Protocole de partage des informations (PPI) doit inclure une classification de la sensibilité des données et informations pour le contexte spécifique, les actions communes pour promouvoir la Responsabilité des données, des clauses quant au respect de la protection des données personnelles au besoin, et aussi inclure des instructions quant au traitement des incidents et à la résolution des violations. * Ce modèle est basé sur le modèle de PPI qui figure dans les ‘OCHA Data Responsibility Guidelines’, et qui a été adapté et mis en œuvre dans une série de contextes d'intervention humanitaires complexes depuis la publication des Guidelines en 2019. Le modèle présenté ici reflète également les meilleures pratiques d'une série d'autres ressources examinées lors de l'élaboration des Directives opérationnelles de l’IASC sur la responsabilité des données dans l'action humanitaire.   **Mode d’emploi**   * Le modèle est conçu pour être adapté et personnalisé à des contextes spécifiques. Il doit être complété par des directives et des instructions supplémentaires si nécessaire (par exemple, une section supplémentaire concernant la protection des données serait utile dans un PPI qui relève du secteur de la protection où des données personnelles très sensibles sont gérées). Le texte pertinent à adapter par l'utilisateur est surligné en [vert]. * Au niveau du système, Le PPI doit être développé de manière collective et sous la direction **de(s) mécanisme(s) inter-agence(s) compétent(s)** (le **ICCM/ICCG/ISCG** et le **IMWG**) avec le soutien de OCHA. Le PPI doit être présenté à l’EHP pour revue et approbation. Tous les acteurs impliqués dans la gestion des données doivent être au courant du PPI et des obligations qu’il contient. * Au niveau des clusters/secteurs, le PPI doit être développé de manière collective et sous le direction **de(s) agence(s) Lead et Co-Lead des clusters/secteurs** en collaboration avec leurs **partenaires**. Le PPI doit être approuvé par tous les partenaires des clusters/secteurs et présenté au mécanisme inter-agence compétent pour référence. * Tout commentaire sur ce modèle peut être envoyé à iasccorrespondence@un.org et centrehumdata@un.org. |

**PROTOCOLE DE PARTAGE DES INFORMATIONS**

**[Pays / réponse]**

**[date]**

# **CONTEXTE**

Ce Protocole de Partage des Informations (PPI) a pour but de soutenir la *responsabilité des données - la gestion des données sécurisée, éthique et efficace -* dans le cadre de la réponse humanitaire dans/au [nom du pays/réponse].Il établit les principes directeurs et les procédures à suivre, ainsi que rôles et responsabilités, pour le partage des données et des informations à travers un nombre de fonctions et activités humanitaires, sur la base d’une conception commune de la sensibilité des données et des conditions de diffusion.

Ce PPI couvre toutes les activités de gestion des données et des informations relatives à la réponse humanitaire dans/au [nom du pays/réponse]. Aux fins du présent protocole, on entend par “informations” les données brutes et les produits d’informations qui en sont développés. Ce PPI s’applique à tous les acteurs humanitaires qui sont présents dans/au [nom du pays/réponse] et y soutiennent la réponse humanitaire, y compris les Nations Unies, les organisations internationales, les organisations nongouvernementales (ONG) internationales et nationales, les tiers et tout autre acteur compétent.

Le PPI a été développé par [ ... ] conformément aux directives du IASC sur la responsabilité de données dans l’action humanitaire[[19]](#footnote-19). Il a été approuvé par [mécanisme de coordination en place au/en pays, p. ex. l’ICCM, l’ICCG, l’ISCG] et présenté à l'équipe humanitaire du pays (HCT) pour information. Dans ce contexte, ce PPI doit être considéré comme le document principal qui guide l’échange des données et des informations dans le cadre de la réponse humanitaire dans/au [nom du pays/réponse]. Il complète les politiques et directives en vigueur et ne se substitue pas et ne porte en rien atteinte aux autres obligations prévues dans des cadres juridiques et réglementaires, dans des protocoles spécifiques aux groupes sectoriels et aux domaines de responsabilité, et aux politiques organisationnelles pertinentes. Ce PPI sera révisé et mis à jour régulièrement/annuellement/au besoin à travers un processus collaboratif géré par le mécanisme de coordination intersectorielle et sujet à l’approbation par [mécanisme de coordination en place au/en pays, p. ex. l’ICCM, l’ICCG, l’ISCG]

# **BUTS ET OBJECTIFS DU PPI**

Les buts et objectifs d’un partage responsable des données et d’information sont les suivants:

* Mener des analyses conjointes (p.ex. évaluations coordonnées), tout en évitant la duplication d’efforts et en garantissant l’interopérabilité des données.
* Améliorer la programmation des efforts de prévention et d’intervention, en permettant de cibler les lacunes et de déterminer les actions prioritaires.
* Augmenter la capacité de conduire des analyses/études, de monitorer la réponse humanitaire, renforcer le suivi et donner des recommandations de manière régulière et crédibiliser les actions.
* Améliorer la collaboration interagence et renforcer la coordination opérationnelle.
* Assurerune meilleure protection de et réponse efficace aux populations affectées, y compris les groupes vulnérables tels que les survivants et les individus à haut risque.
* […]

# **CHAMP D’APPLICATION**

Ce PPI s’applique à **tous les acteurs humanitaires** qui sont présents dans/au [nom du pays/réponse] et y et soutiennent la réponse humanitaire, y compris [ ... ].

Le présent protocole s’applique au **partage des informations** dans le cadre des activités relatives à la gestion des données opérationnelles qui ont lieu dans/au [nom du pays/réponse]. Aux fins du présent protocole, on entend par ‘partage des informations’ le transfert des données brutes ou des produits d’information développés à partir de ceux-ci, soit par moyens numériques (p.ex. courriel, services de transferts de dossiers ou tout autrement) ou par moyens physiques (p.ex. passer des ordinateurs portables, de clé USB ou d’autre dispositif de conservation/stockage). Toute exposition d’information (p.ex. montrer un écran affichant de l’information, présenter un rapport) est inclue dans cette définition et ainsi soumise aux mêmes restrictions que le transfert effectif des données et des informations.

Le présent protocole s’applique à **toutes les données et informations** générées et utilisées dans la réponse humanitaire dans/au [nom du pays/réponse]. Aux fins du présent protocole, on entend par “information” les données brutes et les produits d’information développés à partir de ceux-ci (p.ex. infographies, tableaux/graphiques/organigrammes et cartes, rapports de situation, etc.), y compris:

* **Données et informations sur le contexte** dans lequel se produit une crise humanitaire.
* **Données et informations sur les personnes affectées par une crise** et leurs besoins, les risques et vulnérabilités auxquels elles sont exposées, et leurs capacités.
* **Données et informations sur la réponse,** y inclus les acteurs humanitaires et leurs activités.

Ce PPI ne s’applique pas à la gestion des données d’organisation interne - y compris les données relatives à la gestion des finances, des ressources humaines, et au personnel. La gestion de telles données doit être réglée par les politiques applicables.

# **SENSIBILITÉ DES DONNÉES ET DES INFORMATIONS**

Aux fins du présent protocole, on entend par “données et informations sensibles” des données ou informations qui, en cas de divulgation ou accès sans autorisation correcte, sont susceptibles d’engendrer les conséquences suivantes:

* Risques (effets négatifs résultants du traitement des données sur les droits des personnes ou groupes concernées, incluant sans s'y limiter les souffrances physiques ou psychologiques, la discrimination ou le refus d’accès à des services);
* Impact négatif sur la capacité d’une organisation ou de la communauté humanitaire d’effectuer ses activités, ou sur la perception publique d’une organisation ou de la réponse[[20]](#footnote-20);
* Erosion de la confiance au sein de la communauté humanitaire ou entre des acteurs humanitaires et des parties prenantes dans le contexte de la réponse (p.ex. La divulgation de données sensibles sans le consentement de la source peut avoir un effet sur la relation avec l’organisation et sur le flux des données de façon régulière).

Certains types de données sont catégoriquement considérées comme sensibles, tels que:

* Les données à caractère personnel (p.ex. noms, numéros de téléphone, numéros d'identité nationale, date de naissance, ...),
* Les données d'évaluation désagrégées (au niveau du ménage),
* Les résultats d’enquêtes non traités (microdonnées).

Aux termes de ce PPI, les données et les informations doivent être **partagées conformément aux paramètres présentés dans le tableau ci-dessous**. Ce tableau doit être développé en collaboration avec les différentes parties prenantes, y inclus la population affectée par la crise humanitaire. Il présente la classification et les modes de diffusion de certains types de données et d’informations. Compte tenu de la nature très spécifique de la sensibilité de l’information qui varie d’un contexte à un autre, il n’est pas possible de proposer une liste standard de types de données ou des informations qui seraient considérées comme « sensibles » pour tous les contextes. En raison du caractère évolutif de la sensibilité des données et des informations en vertu du contexte de la réponse humanitaire, [mécanisme responsable] révisera cette classification [tous les six mois/annuellement/veuillez indiquer le délai de révision].

|  |  |  |
| --- | --- | --- |
| **Classification de la sensibilité des données et des informations** dans/au [nom du pays/réponse] | | |
| **Niveau de sensibilité** | **Types de données et d’informations** | **Classification et méthodes de diffusion** |
| **Sensibilité: Faible**  Informations ou données dont la divulgation ou l’accès non-autorisé ne sont pas susceptibles d’engendrer du préjudice ou un impact négatif sur les populations affectées et/ou les acteurs humanitaires. | - | **Classification: Publique**  Les données ou informations peuvent être partagées publiquement.  **Méthodes de diffusion:**  - ReliefWeb  - HRInfo  - HDX  - Autres sites spécifiques à la réponse en question |
| **Sensibilité: Modérée**  Informations ou données dont la divulgation ou l’accès non-autorisé sont susceptibles d’engendrer du préjudice ou un impact négatif mineurs sur les populations affectées et/ou les acteurs humanitaires. |  | **Classification: Limitée**  Les données ou informations peuvent être partagées dans une communauté humanitaire plus large, sur la base d'un objectif clairement défini et de normes associées en matière de protection des données.  **Méthodes de diffusion:**  - HDX [via HDX Connect]  - Listes de diffusion intra-sectorielles |
| **Sensibilité: Élevée**  Informations ou données dont la divulgation ou l’accès non-autorisé sont susceptibles d’engendrer du préjudice ou un impact négatif important sur les populations affectées et/ou les acteurs humanitaires et/ou du dommage à la réponse humanitaire. |  | **Classification: Confidentielle**  Les données ou informations peuvent être divulguées au sein d'une organisation ou d'une petite communauté d'organisations directement impliquées dans la fourniture de l'aide humanitaire, sur la base d'un objectif clairement défini et de normes associées en matière de protection des données.  **Méthodes de diffusion:**  - Partage interne intrasectoriel  - Partage intersectoral déterminé au cas par cas  - HDX Connect |
| **Sensibilité: Sévère**  Informations ou données dont la divulgation ou l’accès non-autorisé sont susceptibles d’engendrer du préjudice ou un impact négatif sévères sur les populations affectées et/ou les acteurs humanitaires et d’entraver le bon déroulement de la réponse. |  | **Classification: Strictement confidentiel**  Divulgation strictement limitée et bilatérale. Déterminée et approuvée au cas par cas, avec l’assurance de respecter les normes les plus strictes en matière de protection des données.  **Méthodes de diffusion:**  - Divulgation bilatérale entre organisations, fondée sur des demandes formalisées, et, dans certains cas, sur un accord bilatéral de partage des données |

Dans la mesure du possible, les membres du [mécanisme de coordination en place au/en pays, p. ex. l’ICCM, l’ICCG, l’ISCG] et les membres du groupe sectoriel, ainsi que les organisations individuelles doivent aspirer à partager les données en temps utile à travers des voies approuvées, sur la base de la classification et paramètres de partage dans le tableau ci-dessus.

# **ACTIONS POUR RESPONSABILITÉ DES DONNÉES**

La responsabilité des données nécessite la mise en œuvre d’actions raisonnées à tous les niveaux de la réponse humanitaire. Ceux-ci incluent par exemple des actions pour garantir la protection des données et la sécurité des données, ainsi que des stratégies pour atténuer les risques tout en maximisant les bénéfices à chaque étape de la gestion des données.[[21]](#footnote-21)

* Les secteurs/clusters respecteront les directives de l'IASC[[22]](#footnote-22) sur la gestion, le partage et la confidentialité des informations et fonctionneront sur le principe que les informations / données humanitaires doivent être rendues accessibles à tous les acteurs humanitaires, à moins que le partage des données ne menace l'espace humanitaire et la sécurité de l'organisation, personnel et partenaires.[[23]](#footnote-23)
* Les coordonnateurs des secteurs et les gestionnaires de l’information acceptent de stocker les informations et les données partagées par les membres du cluster de manière sécurisée.

# **GESTION DES INCIDENTS DE DONNÉES**

Les incidents de données sont des événements impliquant la gestion des données ayant causé du préjudice à des populations affectées par une crise, des organisations, et tout autre individu et groupe. Les incidents de données incluent:

* Divulgation indue ou non-autorisée de données
* Perte, destruction, dommage, ou corruption de données

Les processus organisationnels doivent prévoir la mise en œuvre de mécanismes de responsabilisation claires et des voies d’escalade lors d’une violation de données ou tout autre incident. Par ailleurs, tout incident de données doit être remédié dès que possible/au plus vite et doit être enregistré afin de prévenir qu’un tel incident se reproduise dans le futur. La démarche habituelle pour la gestion d’un incident de données au sein d’une réponse humanitaire est détaillée dans cette note de guidage[[24]](#footnote-24).

En principe, les incidents de données doivent être gérés au niveau organisationnel. Cependant, il faut monitorer les incidents au niveau de la réponse humanitaire à l’aide d’un registre commun qui reflète les détails principaux concernant la nature, sévérité et résolution des différents incidents.[[25]](#footnote-25) Aux termes de ce PPI, [mécanisme de coordination en place au/en pays, p. ex. l’ICCM, l’ICCG, l’ISCG] est chargé de soutenir cette activité.

# **VIOLATIONS DU PROTOCOLE ET RÉSOLUTION DES LITIGES**

En cas de violation du présent protocole par l’un des membres participants, les membres vont se concerter pour résoudre le problème bilatéralement. Si aucune résolution ne peut être trouvée, le responsable du, [mécanisme de coordination en place au/en pays, p. ex. l’ICCM, l’ICCG, l’ISCG] tiendra une réunion dédiée à déterminer la marche à suivre.

En cas de divergence dans l'interprétation de ce PPI ou d'autres litiges, [mécanisme de coordination en place au/en pays, p. ex. l’ICCM, l’ICCG, l’ISCG] sera chargé de trouver une solution à l'amiable. Si une telle résolution ne peut pas être trouvée, le responsable du [mécanisme de coordination en place au/en pays, p. ex. l’ICCM, l’ICCG, l’ISCG] renverra le différend au HCT.

# **ANNEXE A: Partage des Informations avec des Tiers**

**Contexte**

En plus des activités de partage des informations au sein de la communauté humanitaire couvertes par ce PPI, il se peut que les acteurs humanitaires soient sollicités pour partager des informations avec des tiers. Tout partage d’informations par des organisations qui sont soumises à ce PPI avec des tiers qui ne sont pas soumis à ce PPI (y inclus de donateurs, autorités, prestataires de services, et autres) devrait être guidé par cette annexe.

Cette annexe couvre les données et informations opérationnelles générées et utilisées par les acteurs humanitaires dans/au [nom du pays/réponse]. Dans cette annexe, on entend par “informations” les données brutes et les produits d’informations qui en sont dérivés (p.ex. infographies, tableaux/graphiques/organigrammes et cartes, rapports de situation, etc.).

Le partage des informations avec des tiers est fondé sur le principe de transparence et sur la compréhension du fait que le partage de données humanitaires - notamment sur l'évaluation des besoins, l'analyse et la réponse - est essentiel à la prise de décisions coordonnée et efficace dans le cadre d'une réponse spécifique. Lors d’un tel partage des informations, l’humanité, la neutralité, l’impartialité et l’indépendance des organisations humanitaires et de leurs opérations dans/au [nom du pays/réponse] doivent être assurées, et un niveau de responsabilité des données semblable ou égal à celui prévu dans le présent PPI doit être maintenu.

Dans la plupart des cas, les organisations humanitaires auront des accords officiels (p.ex. contrats, protocole d’entente, etc.) en place avec différents tiers qui détaillent les conditions spécifiques pour le partage de données. Dans la mesure du possible, ces termes doivent s’aligner sur l’approche globale de la responsabilité des données décrite dans ce PPI, tout en respectant les politiques institutionnelles pertinentes et les exigences connexes. Lorsque des accords officiels sont en cours d'élaboration, les considérations suivantes peuvent aider à la conception de ces accords. Lorsque de tels accords ne sont pas en place, les considérations suivantes doivent guider les différentes étapes du partage des données entre les acteurs humanitaires et les tiers.

**Demandes d’informations**

Le partage de données et d’informations ne doit se faire que sur la base d’une demande spécifique par un tiers et doit prendre en compte la sensibilité des information, de la charge des demandes pour l'organisation qui les partage, la criticité des besoins d’accès, et l’impact à long terme du partage et de l’ingérence dans la programmation et les opérations.

Afin de satisfaire ce critère, les demandes d’informations par des tiers doivent respecter les critères suivants:

* **Les demandes doivent être écrites, formalisées et spécifiques**

Les demandes pour partage des informations doivent être (a) soumises par écrit, (b) préciser clairement quelles données sont demandées, (c) le format souhaité, et (d) satisfaire les autres critères ci-dessous.

* **Les informations sont demandées pour des finalités déterminées et explicites**

La finalité pour laquelle les informations sont demandées doit être claire et explicite dès la demande.

* **L’information est proportionnée et nécessaire**

Les informations demandées doivent être proportionnées et nécessaires pour atteindre la finalité spécifiée.

* **Les demandes sont limitées en portée et en durée**

Tout tiers ne doit demander que les informations nécessaires à la réalisation de la finalité spécifiée pour laquelle elles sont demandées, et doit indiquer un calendrier de destruction des données.

* **Coordonnée et cohérent**

Les tiers doivent s’assurer que les demandes sont formulées de manière cohérente pour tous les partenaires concernés. Le cas échéant, les tiers doivent diriger les demandes d'information concernant les exercices de gestion de données coordonnés au cluster lead pertinent.

**Réponse et Partage des Informations**

Au sein d’une réponse humanitaire, toute demande d'information doit être enregistrée par l’organisation qui reçoit la demande. Lorsqu’une demande par un tiers satisfait les critères mentionnés ci-dessus et lorsque la politique d’une organisation individuelle permet de partager les données tel que demandé, les organisations soumises à ce PPI peuvent partager les informations demandées, en s’assurant de prendre les précautions suivantes:

* **Transfert d’informations sécurisé tel que spécifié dans la classification par niveau de sensibilité**

Veuillez identifier le moyen pour partager l’information tel qu’indiqué dans la classification du niveau de sensibilité de ce PPI.

* **Niveau d’anonymisation et autres moyens de traitement appropriés**

Avant de partager les informations demandées, l'organisation responsable doit s’assurer que les mesures de précaution appropriées ont été prises, y compris la suppression de noms et d’autres identificateurs directs, et que des méthodes de traitement (p.ex. contrôle de la divulgation de données statistiques) appropriées ont été appliquées au besoin.

* **Règles de confidentialité**

Lors du partage, les organisations doivent mettre en place des restrictions appropriées concernant les transferts ultérieurs et la publication de l’information, y compris une obligation d’avertir l’organisation qui a partagé l’information dans le cas où toute information est partagée intentionnellement ou par accident avec des parties autres que celles convenues.

* **Consultations et alignement**

Lorsqu’une organisation hésite à approuver une demande d’information, l’ICCG/ISCG ou l’EHP peuvent être consultés pour instructions.

# 

# **ANNEXE B: Autres Protocoles de Partage des Informations et directives [nom du pays/réponse]**

Au moment de la rédaction, les groupes sectoriels suivants ont établi des protocoles de partage des informations et documents relatifs spécifiques au pays:

*(Veuillez inclure des références et liens vers les PPI et documents mentionnés)*

1. See Annex A of this protocol for the Principles for Data Responsibility in Humanitarian Action as endorsed in February 2021 as part of the IASC Operational Guidance on Data Responsibility. [↑](#footnote-ref-1)
2. IASC Operational Guidance on Data Responsibility in Humanitarian Action (2021): <https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action> [↑](#footnote-ref-2)
3. Other categories and types of data and information may be added to this Information Sharing Protocol through a formal revision process led by the ICCM as necessary. [↑](#footnote-ref-3)
4. ibid. [↑](#footnote-ref-4)
5. International Committee of the Red Cross, “Professional Standards for Protection Work Carried out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence,” 2018. Available here: <https://shop.icrc.org/professional-standards-for-protection-work-carried-out-by-humanitarian-and-human-rights-actors-in-armed-conflict-and-other-situations-of-violence-2512.html?___store=default> [↑](#footnote-ref-5)
6. Personally identifiable data like beneficiary lists should be shared within bilateral agreements based on organizational policies framed in accordance with the minimum standards prescribed by the UN General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files,* as adopted by Resolution A/Res/45/95 of 14 December 1990, available at: <http://www.refworld.org/docid/3ddcafaac.html> and other international instruments concerning the protection of personal data and individuals’ privacy. [↑](#footnote-ref-6)
7. IASC Operational Guidance on Data Responsibility in Humanitarian Action: <https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action> [↑](#footnote-ref-7)
8. OCHA Centre for Humanitarian Data and Yale University (2019). Guidance Note on Data Incident Management. Available here: <https://centre.humdata.org/guidance-note-data-incident-management/> [↑](#footnote-ref-8)
9. See IASC OG for more detailed actions related to data incident management. [↑](#footnote-ref-9)
10. This includes the humanitarian principles and widely accepted standards articulated for example in Sphere, the Core Humanitarian Standard and the Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief, the United Nations Data Strategy, and the UN Personal Data Protection and Privacy Principles. In addition, it includes more topical or thematic guidance specific to different aspects of data management, including the Professional Standards for Protection Work, the Protection Information Management (PIM) Framework, and the ICRC Handbook on Data Protection in Humanitarian Action, among others. Finally, the Principles draw on existing IASC guidance, including IASC Operational Guidance on Responsibilities of Cluster/Sector Leads & OCHA In Information Management, and IASC Operational Guidance for Coordinated Assessments in Humanitarian Crises. A complete list of the documents analyzed by the Sub-Group on Data Responsibility is available in Annex C. [↑](#footnote-ref-10)
11. Broadly acknowledged across the humanitarian sector, the concept of Do No Harm finds its roots in medical practice, from which it was developed into an axiom of humanitarian response in Mary B. Anderson, *Do No Harm: How Aid Can Support Peace - Or War*, (1999). For the purposes of this document the term is used as follows: ’Doing no harm’ entails that data management in humanitarian response should not cause or exacerbate risk for affected people and communities, host communities, humanitarian personnel or other stakeholders, through actions or omissions. Harm is defined as ‘Negative implications of a data management activity on the rights of a data subject, or a group of data subjects, including but not limited to physical and psychological harm, discrimination and denial of access to services.’ ‘Maximizing the benefits’ of humanitarian data management entails that data is shared when a purpose requires it, in an appropriate and safe way, upholding the necessary data protection requirements. It also entails that data is managed in ways that increase the likelihood of positive impact for affected people. [↑](#footnote-ref-11)
12. This includes the UN Personal Data Protection and Privacy Principles. [↑](#footnote-ref-12)
13. See Annex B for *Examples of Principles in Practice*. [↑](#footnote-ref-13)
14. This includes upholding the IASC, Commitments on Accountability to Affected People and Protection from Sexual Exploitation and Abuse (2017), available at: <https://interagencystandingcommittee.org/accountability-affected-populations-including-protection-sexual-exploitation-and-abuse/documents-56>. [↑](#footnote-ref-14)
15. The ICRC Handbook on Data Protection in Humanitarian Action (2020) and the IASC Policy on Protection in Humanitarian Action (2016) offer guidance on confidentiality. These standards should be interpreted in line with existing organizational policies and guidelines. [↑](#footnote-ref-15)
16. For more information on the humanitarian principles, see OCHA on Message: Humanitarian Principles, available at:

    [https://reliefweb.int/sites/reliefweb.int/files/resources/oom-humanitarianprinciples- eng-june12.pdf](https://reliefweb.int/sites/reliefweb.int/files/resources/oom-humanitarianprinciples-%20eng-june12.pdf). [↑](#footnote-ref-16)
17. In respect to UN-system organizations, the HLCM has adopted the Personal Data Protection and Privacy Principles, which should serve as a foundational framework for the processing of personal data by UN entities. For organizations that do not enjoy privileges and immunities, reference should be made to applicable data protection legislation as well as sets of principles and other guidance such organizations are subject to. [↑](#footnote-ref-17)
18. For more information on processing of personal data and the use of ‘consent’ as a legitimate basis in humanitarian response, see the ICRC Handbook on Data Protection in Humanitarian Action (2nd edition, 2020). [↑](#footnote-ref-18)
19. IASC Operational Guidance on Data Responsibility in Humanitarian Action, 2021, <https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action-0> [↑](#footnote-ref-19)
20. International Committee of the Red Cross, “Professional Standards for Protection Work Carried out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence,” 2018. Available here: <https://shop.icrc.org/professional-standards-for-protection-work-carried-out-by-humanitarian-and-human-rights-actors-in-armed-conflict-and-other-situations-of-violence-2512.html?___store=default> [↑](#footnote-ref-20)
21. Veuillez retrouver un aperçu des actions dans le IASC Operational Guidance on Data Responsibility in Humanitarian Action, 2021, <https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action-0> [↑](#footnote-ref-21)
22. IASC Operational Guidance on Responsibilities of Cluster/Cluster Leads and OCHA in Information Management. [↑](#footnote-ref-22)
23. IASC Operational Guidance on Data Responsibility in Humanitarian Action, 2021, available here: <https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action-0> [↑](#footnote-ref-23)
24. OCHA Centre for Humanitarian Data and Yale University (2019). Guidance Note on Data Incident Management. Available here: <https://centre.humdata.org/guidance-note-data-incident-management/> [↑](#footnote-ref-24)
25. IASC Operational Guidance on Data Responsibility in Humanitarian Action, 2021, <https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action-0> [↑](#footnote-ref-25)