INFORMATION SHARING PROTOCOL
National level
June 2022

OVERVIEW

This Information Sharing Protocol (ISP) is designed to support *data responsibility – the safe, ethical, and effective management of data* – within Myanmar. It establishes a common set of principles[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 Myanmar humanitarian response. For the purpose of this protocol, 'information' refers to both raw data and the information products developed from it. This ISP applies to all humanitarian actors present and supporting response activities in Myanmar, 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 the ICCG in accordance with the Inter-Agency Standing Committee (IASC) Operational Guidance on Data Responsibility[2].

In this context, this ISP serves as the primary document governing data and information sharing in the Myanmar 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 ICCG. Participation of cluster-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

The purpose 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

[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.

[2] IASC Operational Guidance on Data Responsibility in Humanitarian Action (2021): https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action

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 Myanmar.

The ISP applies to information-sharing in the context of all forms of operational data management activities taking place in Myanmar. 'Information-sharing' is defined as the transfer of raw data or information products developed from it, either through digital means 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 Myanmar 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]:

- 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.

BACKGROUND AND CONTEXT

Section 8 of the Myanmar Privacy Law provides the following protections[4] regarding communications, telecommunications and private correspondence:

- No person shall have their communication with another person or communication equipment intercepted or disturbed in any way;
- No one shall demand or obtain personal telephonic and electronic communications data from telecommunication operators; and
- No one shall open, search, seize, or destroy another person's private correspondence, envelope, package or parcel.

---

[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 ICCG as necessary.

[4] https://www.dataguidance.com/notes/myanmar-data-protection-overview

Overall, Myanmar does not have sufficient laws and regulations to protect citizen's right to privacy. The newly amended (in February 2021) Electronic Transactions Law, which provides some limited personal data protection in Myanmar, states that person(s) responsible for managing and keeping personal information shall[5]:

- Systematically keep, protect and manage personal information based on its types, security levels, in accordance with the law;
- not allow the scrutiny, disclosure, distribution, dispatch, modification, destruction, copy or submission as evidence of personal information without the consent of such individual, to any individual or organization;
- not utilize personal information for managing issues that are not in compliance with stated and agreed-upon objectives; and
- systematically destroy or delete the personal information that is collected to be used for a certain period of time after such period has expired.

However, it is clear that these protections are insufficient, as in the months before the military takeover, telecom and internet service providers were ordered by the authorities to install intercept spyware that would allow authorities to monitor the communications of citizens and provide direct access to each operator's and ISP's systems without case-by-case approval[6].

Additionally, current legislation in Myanmar has specified multiple, broad exceptions, where the personal information protections no longer apply – these include[7]:

- Cybersecurity investigations; and
- Any investigation that is coordinating or collecting information on matters related to the stability of state sovereignty, public order and national security.

Notably, the terms "stability of state sovereignty", "public order" and "national security" have been left undefined in the amendment to the law. It was also noted that these amendments had "essentially been copied" from the draft Cyber Security Law which had received "widespread condemnation" from civil society and business associations.

With these amendments and the current political climate in mind, it is necessary to formulate protocols to safeguard the privacy of cluster members in Myanmar who might be targeted or discriminated against, based on either the nature or location of their interventions. Were the ICCG requested, under these new amendments, to furnish data on partners, clusters would now be legally obligated to provide this information to the de facto authorities.

[5] https://www.zicolaw.com/resources/alerts/finally-personal-data-protection-in-myanmar-a-closer-look-into-the-law-amending-the-electronic-transactions-law/#_ftn1

[6] https://www.reuters.com/world/asia-pacific/how-myanmars-military-moved-telecoms-sector-spy-citizens-2021-05-18/

[7] https://www.zicolaw.com/resources/alerts/finally-personal-data-protection-in-myanmar-a-closer-look-into-the-law-amending-the-electronic-transactions-law/#_ftn1

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. 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[8];
- 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), photos and other biometric data
- 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 ICCG will review and revise this classification every six months.

TWO-STAGE PROCESS TO CLASSIFYING SENSTIVE DATA

The ICCG envisions a two-step process to the classification of sensitive data. The first step takes place at cluster level, where each cluster populates the table below as a guideline for their partners. Data is classified according to four broad categories.

Clusters are to fill out the table below and present their initial classification and categories to their partners for feedback. Clusters should also orient them on the reasoning behind their classifications.

[8] 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

Data and Information Sensitivity Classification for MYANMAR [Cluster name]		
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 and FODs - Access restrictions (township level) - 3/4/5W data (at national and township level) - Some organization names	**Classification: Public** Data or information may be publicly disclosed. Methods for sharing public data: • ReliefWeb • HRInfo • HDX • MIMU
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 township level) - 3/4/5W data (this data at the village-tract level and below is restricted) - Names of some organizations who do not want to be publicly-known	**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: • Intra-sector mailing lists

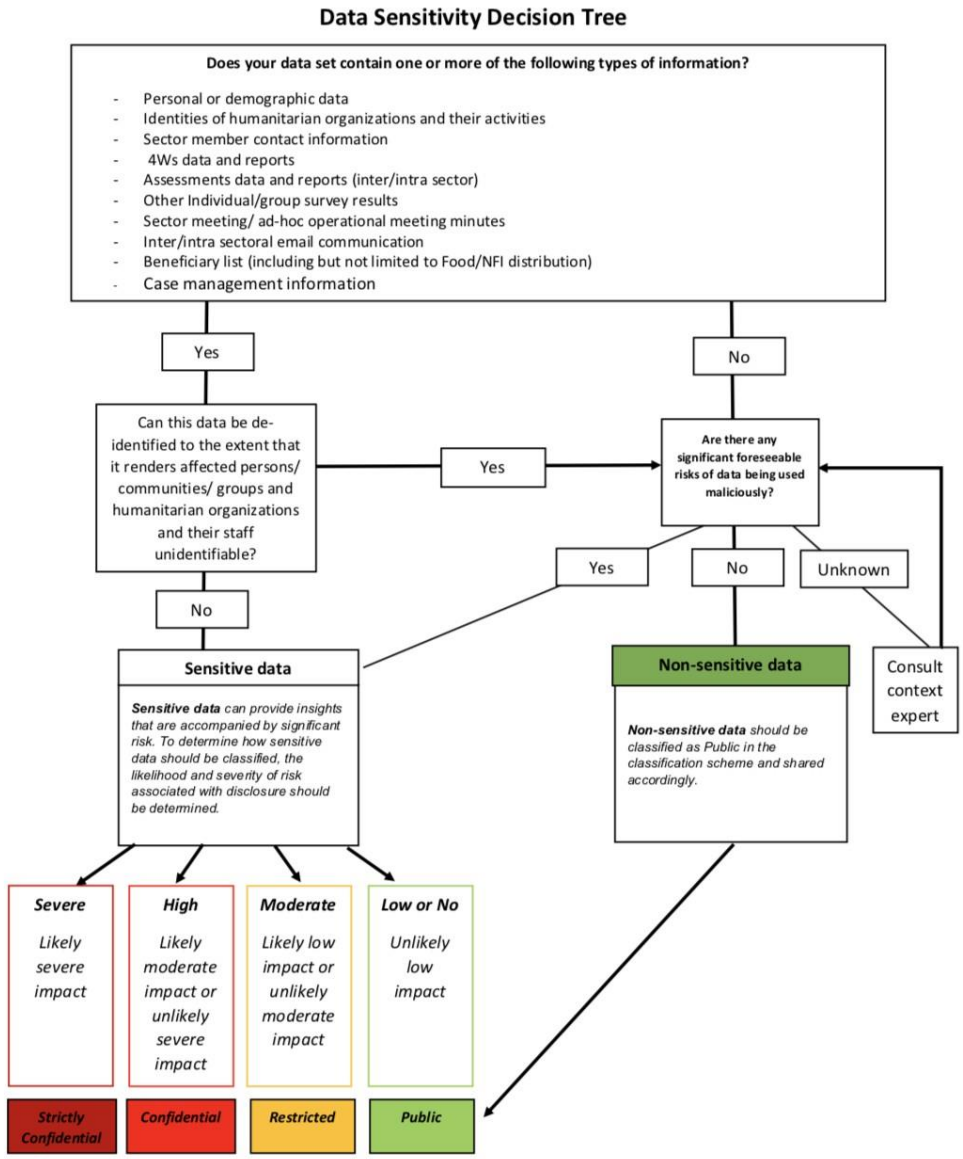
High Sensitivity Information or data that, if disclosed or accessed without proper authorization, **are likely to cause serious harm or negative impacts** to affected people and/or humanitarian actors and/or damage to a response.	- Aggregated survey results (e.g. aggregated to the household level and with additional disaggregation based on different indicators) - 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
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)[9,]	**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

Examples of decisions that clusters should make at this stage would be the threshold for when key data becomes sensitive. It is conceivable that 5W data may be considered restricted at administrative level 4 (village tract) and below. But what can be made public are township-level aggregates. Continuing the example, the statement “in Hpapun township, a total of 1,000 beneficiaries were reached across 43 locations with hygiene kits” would be public information. An example of what would be considered restricted is “the 230 beneficiaries who have been reached in Aik Gyi ward in Bogale are returnees.”

[9] 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.

Once guidelines have been established by the clusters, each organization will then undertake a classification of their data as the same piece of information i.e. an organization's name might be considered publicly available by one organization but restricted by another.

A useful tool that each organization may use to classify their data is the decision tree below:



Data that is shared with the cluster will then be stored with the cluster securely within their own servers. No centralized repository is planned at this moment.

PSEUDONYMIZATION

An additional layer of protection may be afforded through pseudonymization – that is, having sensitive information being replaced with non-sensitive information – this will be particularly useful to partners who do not want to disclose their presence publicly. Below are some of the proposed actions that will allow partners working in sensitive areas to be able to report their achievements and plans with confidence.

1. **Pseudonymization of partner names**. For instance, Partner A would be tokenized as “org_9983” – this token, containing only the word “org_” and a randomly-assigned number between 1 and 10,000, would be stored securely in a translation table within OCHA’s servers, where it would be subject to much more stringent data protection regulations such as the EU General Data Protection Regulation (GDPR) and there would no legal basis for parties and actors in Myanmar to requisition it. If the partner would like for its data to be even more secure, knowledge of the token could be restricted to Partner A and the organization with the translation table. Partner A could then submit all documents it wanted to share under the pseudonym “org_9983”. There will be one, shared inter-cluster translation table to ensure that there is no duplication of partners and codes between clusters. Access to the translation table will be restricted to cluster IMOs.

2. For additional operational security, **interception risks should also be considered**. Parties in Myanmar have the capability to target and intercept information – unencrypted communications between the cluster and the partner might result in the leak of sensitive information even if it has already been pseudonymized. To avoid this, the submission of emails containing sensitive information through a secure mail service such as Proton Mail should be considered. Additional measures that should be considered are (i) password protecting any attachments sent via email that contain sensitive information and (ii) the use of secure SFTP portals for sharing sensitive information including large datasets and files.

   It is currently unclear if UN-system emails are privileged and secure or if these accounts are also regularly monitored, but it would be the safest for both sides – the partner and the cluster – to set up secure mail accounts in order to share sensitive information. Secure emails, however, do not hide IP addresses, subject lines or recipients so care must also be taken to ensure that no identifying information is placed there.

3. **Protection of location data**. It is certainly conceivable that detailed geographic data could be used by various groups to target and discriminate against vulnerable persons i.e. an armed group wants to identify which villages are hosting IDPs. There are several levels of data security that can be enacted – firstly, in public reports, no data that identifies a specific location at admin level 4 or below may be used, though specific township names may be used.

   Secondly, the pseudonymization of locations data should also be considered, as villages, wards, camps and industrial zones could also be used to pinpoint specific vulnerable groups, with translation tables, once again, stored and managed by OCHA.

4. Partners who agree to this process will have **only their tokens appear in all public reports**. They may also additionally choose to not to appear in any lists of partners; should their information be “highly confidential”. Clusters will have to first seek the partner’s consent before sharing who they are with other partners in the cluster, if another partner would want to speak to organizations working in a specific township.

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*[10] for a complete overview of the actions.

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[11].

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.[12] Under this ISP, the ICCG 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 between themselves. If a resolution cannot be reached, the Chair of the ICCG 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 ICCG will be responsible for finding an amenable resolution. If such a resolution cannot be found, the chair of the ICCG will refer the dispute to the Humanitarian Country Team (HCT).

RIGHTS OF PARTNERS WHO SUBMIT DATA TO THE ICCG

The main purposes of collecting data are reporting and coordination, as such, apart from each cluster's external and upwards accountabilities (to global clusters, to the UNCT), it is

---

[10] IASC Operational Guidance on Data Responsibility in Humanitarian Action: https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action

[11] 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/

[12] See IASC OG for more detailed actions related to data incident management.

also important to specify the obligations that the ICCG has towards partners, regarding the data they have submitted to us[13]:

Right to Information – partners will be informed by the ICCG how exactly their data has been used, including being provided an accounting of all processing performed on it. Partners should be aware, at every step of the processing and reporting process, how their data is being used and with whom it is being shared.

Right to Products – partners will have access to all products created with their data.

Right to Access – partners will be able to request access to the data they have submitted; partners will also be given the opportunity to verify the data they have submitted. They may access the data in raw or processed form. It should be noted that pseudonymized data may be shared with cluster partners, like any other 5W data.

Right to Correction – partners will be able to ensure that the ICCG corrects any inaccurate data relating to them, including being able to provide supplementary information. The ICCG may seek from the partner proof that the information is incorrect.

Right to Erasure – partners will be able to have the ICCG erase from its databases, any data related to the partner by withdrawing consent for processing. Additionally, if the ICCG does not uphold its obligations, partners may request their data to be erased as well.

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]

Confidentiality

Humanitarian organizations should implement appropriate organizational safeguards and procedures to keep sensitive data confidential at all times. Measures should be in line with

[13] Adapted from: ICRC, *Handbook on Data Protection in Humanitarian Action,* ICRC: Geneva, accessed from: https://reliefweb.int/sites/reliefweb.int/files/resources/4305_002_DataProtection2020_web.pdf

[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.

general confidentiality standards as well as standards specific to the humanitarian sector[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] 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

[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.

[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.

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-Centred 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-centred 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] These laws and policies contain the list of legitimate bases for the processing of personal data, including but not limited to consent.[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-

[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.

[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).

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.