ANNEX A

DEFINITIONS

Data: Re-interpretable representation of information in a formalized manner suitable for communication, interpretation, or processing.[20]

Data impact assessment: A data impact assessment is a generic term to refer to a variety of tools that are used to determine the positive and negative consequences of a data management activity. These include commonly used – and sometimes legally required – tools such as Data Protection Impact Assessments and Privacy Impact Assessments.[21]

Data incidents: Event involving data management, such as the loss, destruction, alteration, acquisition, or disclosure of data and information, caused by accidental or intentional, unlawful or otherwise unauthorized purposes that have caused harm or have the potential to cause harm.[22]

Data management: The data management cycle consists of the following steps: planning, collecting and receiving, storing, cleaning, transfer, analysis, communicating and disseminating, feedback and evaluation, and retention and destruction.

Data management registry: A data management registry provides a summary of the key datasets being generated and managed by different actors in a context.[23]

Data processing: Any operation or set of operations that is performed on data or on sets of data, irrespective of the technology and processes used, including by automated means, by or on behalf of the Secretariat, including but not limited to collecting, registering, recording, structuring, storing, adapting, altering, cleaning, filing, retrieving, consulting, using, disseminating, disclosing, transferring, sharing, copying, making available, erasing and destroying.[24]

Data protection: The systematic application of a set of institutional, technical and physical safeguards that preserve the right to privacy with respect to the processing of personal data.[25]

Data responsibility: The safe, ethical and effective management of personal and non-personal data for operational response, in accordance with established frameworks for personal data protection.

Data security: A set of physical, technological and procedural measures that safeguard the confidentiality, integrity and availability of data and prevent its accidental or intentional, unlawful or otherwise unauthorized loss, destruction, alteration, acquisition, or disclosure.[26]

Data sensitivity: 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.[27]

Data sharing agreement: Agreement that establishes the terms and conditions that govern the sharing of personal data or sensitive non-personal data. It is primarily used for data sharing between two parties and typically established at the country level.[28]

[20] UN, **Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity, 2020-22** (2020).

[21] IASC, **Operational Guidance on Data Responsibility in Humanitarian Action** (2021).

[22] UN OCHA Centre for Humanitarian Data, **Guidance Note: Data Incident Management** (2019).

[23] IASC, **Operational Guidance on Data Responsibility in Humanitarian Action** (2021).

[24] UN Secretariat, **Secretary-General's bulletin on Data protection and privacy policy for the Secretariat of the United Nations**, ST/SGB/2024/3 (2024).

[25] Definition developed by the UN Privacy Policy Group (2017).

[26] UN OCHA Centre for Humanitarian Data, **Glossary**.

[27] UN OCHA Centre for Humanitarian Data, **Glossary**.

[28] IASC, **Operational Guidance on Data Responsibility in Humanitarian Action** (2021).