While data responsibility is linked to data protection and data security, these terms are different. 'Data protection' refers to 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 and uphold the rights of data subjects. 'Data security', which is applicable to both personal and non-personal data, refers to physical, technical and procedural measures that aim to safeguard the confidentiality, availability, and integrity of data.

The graphic below depicts the relationship between these key concepts and the humanitarian principles.
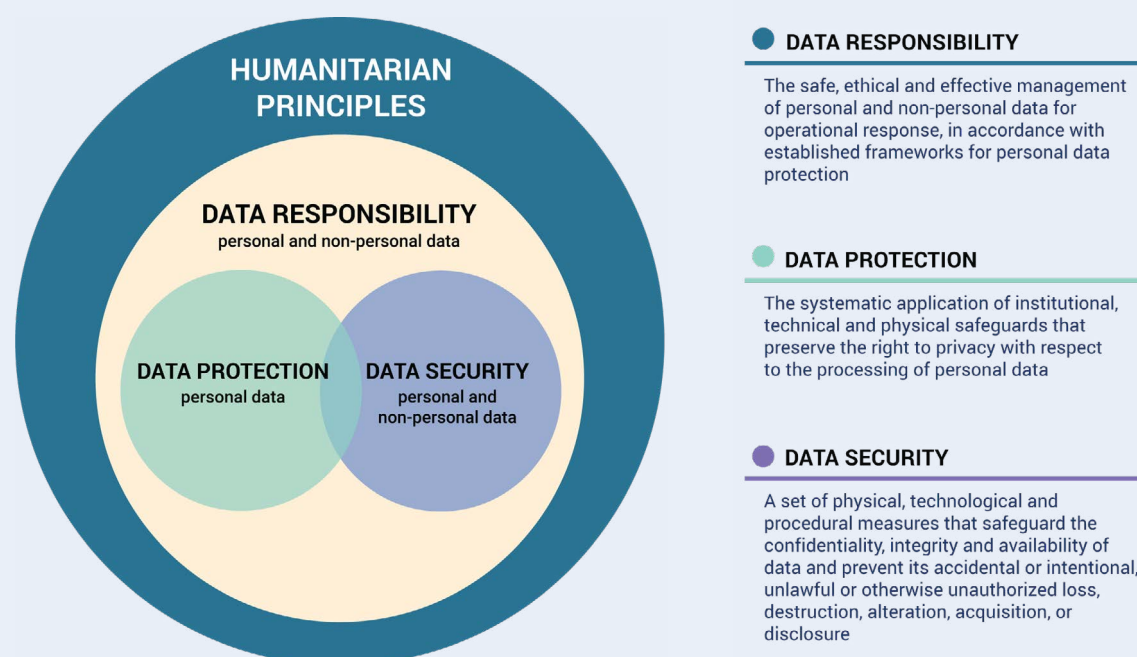
Relationship between Humanitarian Principles, Data Security, Data Protection and Data Responsibility.

Operational data management: The ensemble of data management activities for operational response, including the design of activities and their subsequent execution, including the collection or receipt, storage, quality assurance, analysis, sharing, use, retention and destruction of data and information by humanitarian actors. Data management occurs as part of humanitarian action throughout the planning and response cycle across clusters/sectors and includes activities such as situational analysis, needs assessments, population data management, registration and enrollment, case management, communicating with affected populations, protection monitoring, and response monitoring and evaluation.

The term 'data processing' is used to refer to any operation or set of operations that is performed on personal data or 'non-personal data in a sensitive context', as per the UN Secretariat Data Protection and Privacy Policy.

Personal data: Information, in any form, that relates to an identified or identifiable natural person ('data subject').