

Non-personal data: Any information that does not relate to an identified or identifiable natural person. Non-personal data can be categorized in terms of its original nature: data that has never related to a data subject (i.e., that has always been non-personal data), such as data about the context in which a response is taking place and data about humanitarian organization and their activities; or data that was initially personal data but later rendered anonymous, such as data about the people affected by the humanitarian situation and their needs, the threats and vulnerabilities they face, and their capacities. Non-personal data includes demographically identifiable information (DII), i.e., data that enables the identification of groups of individuals by demographically defining factors, such as ethnicity, gender, age, occupation, religion, or location.

Sensitive Data: Data that, if disclosed or accessed without proper authorization, is likely to cause:

- harm (such as sanctions, discrimination) to any person, including the source of the information or other identifiable persons or groups, or;
- a negative impact on an organization's capacity to carry out its activities or on public perceptions of that organization.¹¹

Sensitive data includes personal data as well as 'non-personal data in a sensitive context'. Non-personal data in a sensitive context is information, in any form, that, while not relating to an identified or identifiable natural person, may, by reason of its sensitive context, put certain individuals and groups at risk of harm, including vulnerable or marginalized individuals and groups of individuals, such as children. The same types of data may have different levels of sensitivity in different contexts and sensitivity may change over time.

¹¹ Based on the definition in the ICRC-led Advisory Group on "Professional Standards", **Professional Standards for Protection Work, 3rd edition** (2018), Chapter 6: Managing Data and Information for Protection Outcomes.