As increasing amounts of personal information are being collected and processed in often opaque and increasingly complex ways, protection of personal data and privacy are seen as fundamental for the protection of human dignity. Legal frameworks such as the GDPR and the UK's Data Protection Act (2018) are being brought into force to ensure such protections.

In cases where data collection and processing is undertaken jointly by different stakeholders, it is important that the roles and responsibilities for this process are easily and clearly allocated in order to minimise the risk to the people and communities represented by the data. Otherwise, processing may lead to loss of confidentiality, social disadvantage, or accidental deprivation of rights and freedoms to exercise control over one's personal data.

- Be clear about the roles and the responsibilities for data protection
- Provide mechanisms for people to exercise control over their personal data.
- State clearly what kinds of data (and how much of it) needs to be shared and with who and why it is being shared.

Further information

One of the key principles of The EU Charter of Fundamental Rights is the right to protection of personal data (Article 8). The EU's General Data Protection Regulation (GDPR) has been recently introduced to ensure such protections in relation to the processing of personal data in today's Information Society and is based on the principles of lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability (Article 5). The overarching aim of the GDPR is to foster a free flow of information within the European Union. At the same time, it gives member states some opportunities to make provisions for how it applies in their country. As such, Member States do have a certain leeway to restrict and deviate from the European framework, for example, for matters on national security and immigration. In the UK, such matters are covered by the Data Protection Act 2018.

Within the specific context of disaster management, such GRPD provisions might mean more restrictions when exchanging information. These kinds of issues are often addressed in bi- or multilateral agreements that provide for a specific mutually recognised legal basis for the transnational exchange of information necessary to cope with a cross-border disaster situation. These agreements should make clear the roles and responsibilities allocated across partners in order to ensure the data protection of people and communities involved in the disaster. Such responsibilities include the obligation to notify when laws are broken, getting the required consent for processing, providing access to data, and deleting data

when the specific incident is declared closed. They also require that partners make explicit the decisions behind sharing and communicating. Failure to do so adequately, may lead to loss of confidentiality, social disadvantage, or accidental deprivation of rights and freedoms to exercise control over one's personal data.

While regulatory frameworks such as the GDPR have been welcomed by experts, professionals and policy-makers alike, the EDPS Ethics Advisory Group cautions that new technological developments, such as big data, bring about new forms of data collecting and processing which challenge classical understandings of data protection rights and principles. Such developments demand that we redefine our ethical understandings and encourage us to move from traditional articulations of European values towards an innovative and responsive digital ethics (2015, 2018).

Sources

Charter of Fundamental Rights of the European Union [Link]

EDPS (EU Data Protection Supervisor) (2018) 'Towards a digital ethics', Ethics Advisory Group Report [Link]

EDPS. (2015). European Data Protection Supervisor: Opinion 4/2015: Towards a new digital ethics. [Link]

General Data Protection Regulation (European Commission, 2016012/2014) [Link]

EU's Article 29 Working Party Opinion 1/2010 [Link]

UK's Data Protection Act 2018 [Link]