To facilitate collaboration, it is necessary to clarify each organisation's rights, responsibilities, tasks, expectations, and decision-making powers in relation to collaborative information management. For example, while one organisation may host a collaborative information management system – hence becoming the managing authority and data controller, responsible for things such as system maintenance, data security – in a collaborative setting, some of these responsibilities may be shared across organisations.

Guiding Questions

What does it mean to take responsibility for data in collaborative situations?

Who is responsible for notifying all parties concerned in case of a data breach?

Are any data sharing agreements and joint data controller arrangements revisited on an on-going basis to determine how they should be updated to reflect any changes in relationships?

Further Information

The exchange of information in the disaster relief sector has become very complex. There are many actors and many new actors, yet processes of exchanging information have not changed substantially and are often *ad hoc* and negotiated on a case-by-case basis. Often, there is more information than necessary while at the same time the relevant information that a particular stakeholder requires might not be available. Many parties argue that these processes of information sharing and exchange need to be better coordinated. The challenge lies in 'creating an information infrastructure that is sufficiently flexible to manage the dynamic exchange of information among the participating entities in an inter-organisational system, but sufficiently ordered to ensure that the relevant information gets to the responsible parties in valid format and in time to support effective action' (Bjerge et al 2016: 3)

Within ecologies of mobile technology and data sharing, the data controller, according to the General Data Protection Regulation (GDPR), Article 4 (7), is defined as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The challenge for defining the controller or joint controllers lies in identifying all the responsible entities that could be engaged in disaster management. While in some cases, the controller could be easy to identify, in others, it could be a variety of authorities which could possibly become joint

controllers or co-controllers (Jasmontaite and Dimitrova 2016).

Examples

Ferrãos and Sallent (2015:237) describe how the use of private Access Point Names (APN) is common between Mobile Network Operators (MNO) and the dedicated or private infrastructure pf PPDR service providers hosting PPDR communications services. The connection between the commercial MNO and the PPDR operator is based on dedicated resources, such as leased lines. This prevents risks related to security threats or traffic congestions. End-to-end security services like encryption remain within the responsibility of the PPDR organisation.

In their report of how a Hastily Formed Network (HFN) was designed to support the response to the European Refugee crisis led by humanitarian agencies, Maitland and Bahrania (2017:12) explain how "the network design for this implementation required collection of significant amounts of traffic data for telemetry or network management." This posed challenges of data protection. To comply with the EU Data Protection Directive, "the providers of cloud-based network management act in the role of "data processors," with NetHope [the NGO] as the 'data controller'. To ensure privacy of individual users, the network analytics and management were designed for automatic analyses. … the network design [also] did not require user registration or other mechanisms to tie a device identifier back to an identifiable person. As described by the NetHope network manager, this configuration ensured that even if Greek authorities pursued proper channels to access network traffic analyses, only general patterns of networks usage, and not an individual's network traffic or communications, would be accessible."

Resources

Bjerge, B., Clark, N., Fisker, P., and Raju, E. (2016). Technology and Information Sharing in Disaster Relief. PLOS ONE, 11(9): 1–20 [DOI]

Ferrãos, R., & Sallent, O. (2015). *Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology*. Wiley.

Jasmontaite, L., and Dimitrova, D. (2017). Online Disaster Management: Applicability of the European Data Protection Framework and Its Key Principles. Journal of Contingencies and Crisis Management, 25(1): 23–30 [DOI]

Maitland, Carleen and Bharania, Rakesh, Balancing Security and Other Requirements in Hastily Formed Networks: The Case of the Syrian Refugee Response (March 31, 2017). [DOI]