In designing collaborative information management processes or systems it is critical to know whether or not personal information will be exchanged between the different agencies. If so, those who host, and those who use such systems will need to comply with the regulatory frameworks that protects the usage of personal data. Within the EU, the processing of personal data is governed by the pan-European General Data Protection Regulation (GDPR). In order to implement the requirements of this piece of legislation, all of the actors involved in the system's architecture should map out the different data flows and define the roles and responsibilities of the different actors that send, receive and act on this data. These processes link strongly back to the need to implement a robust, evolving data protection impact assessment process. The new regime also gives further rights to data subjects which leads to the focus shifting towards them when planning how to handle, store and process personal data.

Guiding Questions

What personal data is used and stored? GPS tracks, images, names, …

When do I process personal data?

How is it anonymised? What if we use pseudonyms? Is there the potential for identification of individual subjects after the aggregation of data sets?

Who can access the data?

How long can they be stored?

How is accountability supported?

Further Information

The GDPR applies to all EU states when one is "processing" any kind of personal information.

The legal concept of "processing "is very broad: it refers to any kind of operation that is performed on personal data. This includes: collection, storage, alteration, consultation, transmission, or erasure of data. From the moment one comes across a single instance of personal data, then this means that they are processing it.

Personal data refers to any kind of information related to an identifiable natural person that

would allow this individual to be singled out. Pseudonymised data still qualifies as personal data, even though it does not reveal directly the civil identity of the person concerned. Examples of personal data are: an identification number, location data, IP addresses, a name or any factor specific to the physical, mental, economic or social identity of a person. Only anonymised information escapes the scope of the GDPR. But, there still remain questions, legally, as to whether anonymisation is technically feasible, particularly in relation to data aggregation, making individual acts of anonymity not enough to secure personal data in a collaborative information management system.

A first general principle that applies to the processing of personal data is lawfulness. This means that you need to invoke a specific legal basis to legitimise the processing of personal data. Consent is the most well-known example of a legal processing ground. This principle will be further elaborated in the guidance on Exceptions and lawful processing.

A second general principle that should be taken into account is purpose limitation. This principle means that the data can only be processed for the specific purpose they were collected for. If data is collected for one purpose, it cannot be used for another. Consequently, only the persons who need access to the data for these specified purposes should be able to do so. A concrete consequence of the purpose limitation principle is the need for role-based access controls.

A third important principle is the one of data minimisation, which means that the use of personal data should always be limited to what is strictly necessary for the purposes pursued. This principle excludes any excessive gathering of information and holds that data will only be stored for as long as necessary to complete the set tasks. The data minimisation principle also implies that data will only be stored for as long as necessary to complete the set tasks.

The specific rules concerning the treatment of sensitive data are specified at the national level while a number of so-called ‘special categories’ of personal data are subject to a stricter regime since they are of a very sensitive nature. Within the context of PPDR it is important to note that, for example, information relating to health, biometric data or information that reveals racial or ethnic origin qualify as sensitive data. When first responder agencies are, for example, exchanging health information concerning a victim through a collaborative information management system, they should be aware that the sensitive nature of this information might require additional precautionary measures.

Examples

Data minimisation & Retention policies: When the architecture of the collaborative information management system has a centralized set-up, which means that information is exchanged through a central server when it is transmitted to another agent, all of the information that is stored on this server should be deleted once the disaster situation is over.

Purpose limitation: Implementing role-based access controls is indispensable to comply with the purpose limitation principle. In this way actors can only access personal data for achieving the specific purpose that is in close relationship with their role. An example of this approach could be seen in the following scenario: a user of the collaborative information management system runs a search to find details of how emergency services dealt with the aftermath of a chemical leak. The aim of the search is to determine the extent of respiratory problems caused by the leak. The search shows information about all injuries sustained in the event. Only those relating to respiratory responses should be kept; all other information not relevant to the search should be discounted.

Privacy by Design or Design for Privacy? Privacy by design is a relatively new approach and it has several meanings and origins (Cavoukian, 2001; Langheinrich, 2001 – see Buscher et al 2014 for references). Firstly, privacy by design is about heightening sensitivity to privacy issues during design. Secondly, it can be about enforcing compliance with privacy regulations through hard wiring constraints on practices into design with privacy enhancing technologies (PETs). Existing examples include privacy policy inspection, access control restriction, and pseudonymisation tools that allow people to maintain a degree of anonymity (Pearson, 2009). Both approaches need to be supplemented with methods that support translation into the design and appropriation of technologies. Such methodologies may include privacy and ethical impact assessments, that is, structured investigations into the privacy and ethical implications of design decisions (Clarke, 2009; Wright, 2010), and legal risk analysis. All should “begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project” (Wright & De Hert, 2012).

Privacy by design approaches can be of limited utility in view of the dynamic nature of emergency management and the need for role improvisation and emergent interoperability in systems of systems approaches. Privacy cannot easily usefully be ensured or ‘enforced’ apriori by design in this context. Buscher et al (2014) propose a third approach of human-practice focused privacy by design. This is based on a shift from conceptions of privacy as a value that has to be traded in in return for security, or a right that has to be respected through regulation, to an understanding of privacy as a contextual, situated and embodied

practice of boundary management that is augmented and constrained by technologies, cultural conventions and the law. By taking this perspective, alternative socio-technical design avenues are opened up, for example via specification of non-functional requirements such as architectural qualities of transparency and inspectability. For example, privacy protection in emergency response systems of systems may be supported by imposing temporal and geographical constraints on data sharing, 'seamful design' (Chalmers, 2003) and approaches that support 'accountable' or 'palpable' computing (Dourish, 2001, Kyng, 2007).

When, in times of crises, boundaries between different systems (telecoms databases, transport management systems, police records, social networking systems, insurance databases) are made permeable, allowing automated data collection, data mining, analysis and profiling, conventional privacy protection that involves limiting access at the point of data collection, including using legal, cryptographic and statistical techniques is likely to be prohibitively rigid and restrictive. Accountable datamining, an approach developed in response to the fact that the Internet provides a huge source of data that can render conventional access-limiting methods ineffective and impractical, is an example of innovative privacy solutions that may be useful in a human practice focused approach. Referring to the US use of data mining around Passenger Records, (Weitzner, Abelson, Berners-Lee, Feigenbaum, Hendler & Sussman, 2008:85) argue that: 'Laws that limit access to information do not protect privacy here because so much of the data is publicly available. To date, neither law nor technology has developed a way to address this privacy loophole.' New socio-technical mechanisms are required and Weitzner and his colleagues suggest:

- Transparency: mechanisms where the history of data manipulations and inferences is maintained and can be examined by authorized parties (who may be the general public)
- Accountability: one can check whether policies that govern data processing were in fact adhered to (Weitzner, Abelson, Berners-Lee, Hanson, Hendler, Kagal, McGuiness, Sussman & Waterman, 2006)

In the context of emergency response exceptional breaches of data protection regulations may be necessary and legitimate. Personal data may, for example, be used for purposes other than those specified at the time of collection. To support trust in systems that support interoperability in times of crisis (but not under normal circumstances), the design of tools that make the use of personal data accountable both at the time of use and retrospectively, seems promising.

Büscher et al (2014) also suggest that in view of the substantive ethical and legal

challenges, a human practice focused co-design approach is particularly useful for crisis ICT design, because it brings in located accountabilities (Suchman, 2002) and enables collective, iterative development of understanding of challenges and search for socio-technical solutions.

Resources

Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation.

Article 29 Data Protection Working Party, Opinion 04/2007 on the concept of personal data.

Büscher, M., Perng, S-Y., Liegl, M. (2014) Privacy, Security, Liberty: ICT in Crises. International Journal of Information Systems for Crisis Response and Management (IJISCRAM) 6(4): 76-92. Preprint version available here.

CJEU, C-582/14, Patrick Breyer v Bundesrepublik Deutschland.

CJEU, C-293/12, Digital Rights Ireland Ltd.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Link]

Petersen, K. Easton, C. and Buscher, M. (2018) On anonymity in disasters: socio-technical practices in emergency management. *Ephemera: Theory and Politics in Organization.*

GDPR Overview of the General Data Protection Regulation (2017). Information Commissioner's Office [Link]