In any collaborative information management system, data controllers must be assigned who will be liable in case something goes wrong. This responsibility could be spread over or divided between multiple different parties. Within the context of the GDPR, a distinction is made between data controllers and data processors in order to allocate the responsibilities that flow from its provisions. A data controller determines the purpose and the means of the processing of the personal data (Art. 4(7) GDPR). A data processor, on the other hand, processes the personal data on behalf of the controller (Art. 4(8) GDPR). In general, a data controller will have to adhere to some additional obligations compared to a data processor. The allocation of responsibilities will have to be agreed upon beforehand by the parties who participate in the system. The concept of data controller is mentioned throughout the GDPR due to the complexities of the role. The recent changes in the law have placed more stringent duties on the data controller and, among other duties, they need to facilitate the rights of the data subjects and ensure that procedures are put in place to allow data subjects to, for example, rectify errors and assert their right to data portability. It is important that a data controller is aware of the advice of supervisory authorities and complies with all duties they have in relation to reporting the issues that arise.

Guiding Questions

How are data controllers and data processors' roles to be established in a collaborative information management system ? For example, who is responsible for notifying all parties concerned in case of a data breach?

Who is responsible for log keeping of the processing activities?

Have processes been put in place that allow data subjects to assert their new rights under the GDPR?

Have all special categories of data (e.g. sensitive/the data of minors) been assessed and procedures put in place to fulfil specific legal duties relating to these?

Further Information

It is most likely that the parties brought together in a collaborative information management system will work as so-called 'joint' data controllers (Art. 26 GDPR). If all of the parties involved share a common objective and there is no hierarchy between them, they jointly determine the purpose and the means of the processing operations. Part of this is

determined by the governance structure. Consequently they should all bear the same degree of responsibilities. This assessment remains valid even if the parties involved would use these data to pursue their own individual purposes. When the agencies involved set up the system-architecture, they determine the essential elements of the means to be used and they will qualify as joint controllers even though they do not necessarily share an identical purpose. This is important to note, since in spite of the obvious common goal of information-sharing to manage a crisis situation, the decision-making capacity often remains at the level of each single agency.

Data controllers bear the end responsibility for the compliance with the data protection regulations. Internally, the first responder agencies connected to the system-infrastructure should draw up an agreement that defines their precise relationship and responsibilities. However, from an external point of view data subjects will be able to enforce their rights vis-à-vis any of the agencies involved (Art. 26(3) GDPR).

Both data controllers and data processors should make records of their processing activities in order to demonstrate their compliance with the GDPR. This means that all of the connected entities will need to maintain logs concerning the data they sent and received through the CIS (Art. 28 and 30 GDPR).

Given the fact that all of the connected entities are data controllers, they should all notify a data breach to their national Data Protection Authority (DPA) without any delay and at least within 72 hours after they become aware of the leak (Art. 33 GDPR). In case the leaked data poses a high risk to the rights and freedoms of data subjects (for example health data), the connected entities should also inform the data subject whose data have been compromised.

Lastly, data controllers also have the final responsibility to conduct data protection impact assessments under certain conditions (Art. 35 GDPR).

Examples

Different first responder agencies that are signing up to a collaborative information management system should draw up joint controller agreements among themselves to determine their respective responsibilities. While internally liabilities might be distributed, such agreements should designate one of the partners as a central point of contact that will serve as a liaison partner vis-à-vis data subjects that want to exercise their rights.

Resources

Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”. [Link]

Van Alsenoy, B. Regulation Data Protection: The allocation of responsibility and risk among actors involved in personal data processing, Phd Thesis KU Leuven, 43-76 [Link].

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]

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