The recently adopted General Data Protection Regulation (GDPR) stipulates that an assessment of the relevant privacy consequences should be carried out by the data controller before putting a new technology in place (art. 35 GDPR). This evaluation is compulsory if the data processing poses a high risk to the rights of natural persons. This assessment is not a one-time event and should be reiterated throughout the whole development and deployment process of the technology. A strong emphasis should be laid on data minimisation, risk minimisation and secure storage and processing of information. Crucial in this respect is that the DPIA is not a mere box-ticking legal compliance check, but rather an overall evaluation process that should also encompass ethical and social impacts. In this respect it would be advisable to integrate the DPIA with, for example, ethical impact assessment processes. It is best practice to use the DPIA to shape and revisit data sharing arrangements and how procedures within an organisation support ethical data sharing and uphold the rights of data subjects.

Guiding Questions

Have you conducted a data protection impact assessment prior to the deployment of the technology?

What information security measures have you adopted to address data protection concerns?

How regularly do you reassess the privacy compliant character of the technology?

Have you taken an approach that embeds privacy protection at all levels of the technological development?

Further Information

Article 35 requires to carry out a DPIA in situations where data processing involves:

a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing;
b. processing on a large scale of sensitive categories of data (e.g., revealing racial or ethnic origin, genetic data, biometric data or health); or
c. a systematic monitoring of a publicly accessible area on a large scale.

Since a collaborative information management system aims to facilitate interaction and optimize coordination of civil protection assistance in disasters of various scale, it can be anticipated that special categories of data (e.g., health condition about an affected

individual) will be processed within the system by PPDR stakeholders ranging from public authorities to private entities and NGOs. The scale of data, including personal data, processed via the collaborative information management system will depend on the type of an event, the amount of affected individuals, and on the number of first responders involved in the response action. Therefore it is difficult to anticipate the exact scale of data processing operations on the system, but a situation, in which massive amounts of data, including personal data that entail special categories of data, will be processed, cannot be dismissed. To avoid any adverse impact of the ambiguity of the system set up, a DPIA should be used as a tool that would allow system operators to identify weaknesses and take the necessary precautions. Since it will be difficult to identify a single controller of the system that could be responsible for a DPIA, all of the companies developing the collaborative information management system architecture would have to get involved in the DPIA exercise.

A DPIA should at least comprise the following elements:

a. A systematic description of the processing operations and their respective purposes;
b. an assessment of the necessity and the proportionality of the processing operations in relation to these purposes;
c. an assessment of the privacy and data protection risks; and
d. measures addressing those risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and demonstrate compliance with the GDPR.

While there are no specific methodologies available nor prescribed for conducting a DPIA, it is highly recommended to build on internationally acknowledged existing risk-assessment frameworks such as those developed by the ISO or ENISA (see the resources section).

Examples

These are a number of example questions that provide guidance in structuring the DPIA exercise:

1. Who are data controllers and who are data processors?
2. What information processed can be considered to be “personal data”?
3. What is the relevant legal basis for the processing of personal data?
4. What personal data can be collected and for exactly what purposes?
5. For which purpose and for how long personal data should be stored (retained)?

6. For which purpose and for how long should personal data be stored (retained) by entities that participated in a common effort?
7. How and under what conditions could individuals exercise their rights (e.g. information, access and objection) as a data subject?
8. How to ensure security and confidentiality of personal data processing?
9. What risks are there in relation to potential threats to personal data?

Resources

Commission pour la Protection de la Vie Privée (BE), Projet de recommandation d'initiative concernant l'analyse d'impact relative à la protection des données et la consultation préalable, CO-AR-2016-4 .

Gellert R., "We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection", European Data Protection Law Review, 4/2016, Vol. 2, pp. 481-492 .

ISO 31000 (Risk management) en ISO 27005 (Information security risk management).

ENISA, Position on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications .