Interactive Workshop on Data Protection Impact Assessment:

A Hands-On Tour of the GDPR's Most Practical Tool

Case 1: Smart Surveillance in Train Stations

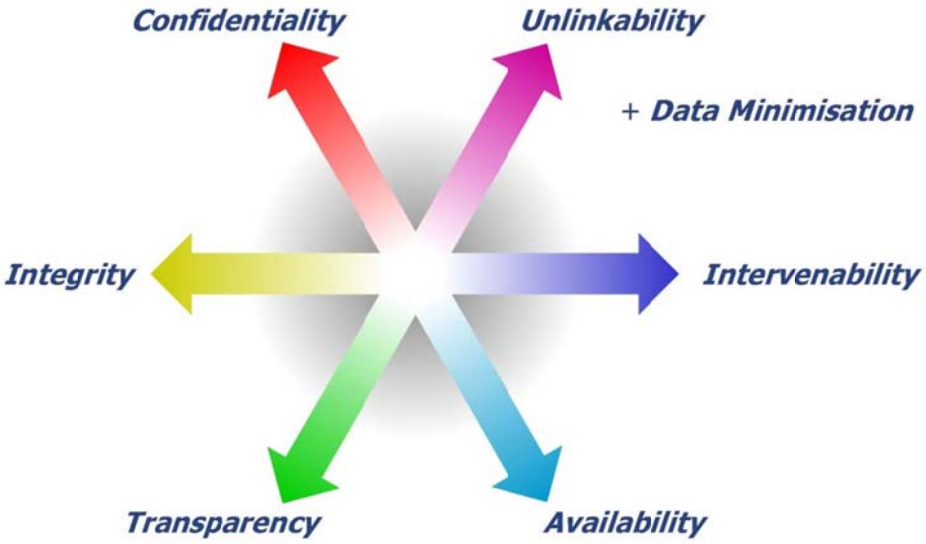
After successful pilots, the national police force of an EU Member State has proposed setting up cameras with automated biometric recognition and behavioral analysis capabilities in all of the country's train stations. The system will have access to the images and biometric data from the national identity-card database, as well as police databases of terrorist and criminal suspects, political extremists and religious fanatics, and persons of interest or concern. It is supposed to be able to identify individuals with a very high degree of accuracy. The data will be stored for up to 1 year.

Besides identifying individuals, the system performs behavioral analysis to identify a range of suspicious behaviors (e.g., looking about a lot, avoiding security personnel, leaving luggage behind). It also identifies dangerous behavior or behavior indicating suicidal tendencies, especially of vulnerable individuals (e.g. drunken gait, straying close to platforms).

When the system picks up suspicious (or dangerous) behavior or individuals, it sends automated messages to the station security personnel, city anti-terror units, and / or the station health and safety personnel (for drunks, etc.), whereupon these initiate enhanced monitoring or other interventions (e.g. arrest).

Standard Data Protection Model

Protection Goals



Data minimisation: Data minimisation substantiates and operationalises the principle of necessity, which requires of any process as a whole as well as any of its steps not to collect, process and use more personal data than necessary for the achievement of the purpose of the processing. Data minimisation is to be taken into account proactively as an element of data protection-friendly design. Starting with the design of information technology by the manufacturer and its configuration and adaptation to the operating conditions, to its use in the core and auxiliary processes of the operation, for instance in the maintenance of the systems used; from the collection of personal data, through its processing and use, to its erasure or complete anonymization; throughout the entire life cycle of the data.

(1) *Availability:* personal data must be available and can be used properly in the intended process. Thus, the data must be accessible to authorised parties and the methods intended for their processing

must be applied. This presupposes that the methods can deal with the available data formats. Availability comprises the ability to find specific data (e.g. by means of address directories, reference or file numbers), the ability of the employed technical systems to make data accessible to individuals in an adequate manner, and the possibility to interpret the content of the data (semantic ascertainability).

(2) *Integrity:* on the one hand, information technology processes and systems must continuously comply with the specifications that have been determined for the execution of their intended functions. On the other hand, integrity means that the data to be processed remain intact, complete, and up-to-date. Deviations from these properties must be excluded or at least ascertainable so that this can either be taken into consideration or the data can be corrected. If the protection goal integrity is understood as a form of accuracy within the meaning of Article 5 (1) (d) GDPR, this leads to the claim that there is sufficient congruency between the legal-normative requirement and common practice, both in terms of technical detail as well as in the broad context of the procedure and its overall purpose.

(3) *Confidentiality:* no person is allowed to access personal data without authorisation. A person is not only unauthorised when it is a third party external to the controller, regardless of whether they act with or without a criminal intent, but also employees of technical service providers who do not need access to personal data for the provision of the service, or persons in organisational units who are unrelated to the respective procedure or data subject.

(4) *Unlinkability:* data shall be processed and analysed only for the purpose for which they were collected. Data sets can in principle be processed for further purposes and can be combined with other, potentially publicly available data. Larger and more meaningful data sets also increase the potential for abuse, i.e. to use the data unlawfully, for purposes beyond the legal basis. Such further processing is lawful only in strictly defined circumstances. The GDPR only allows them to be used for archival purposes which are in the public interest, for scientific or historical research purposes or for statistical purposes, and explicitly calls for safeguards for the rights and freedoms of the data subjects. These safeguards are to be achieved through technical and organisational measures. In addition to measures of data minimisation and pseudonymization, other measures that allow the further processing to be separated from the source processing are also suitable, ensuring separation both on the organisational and on the system side. The data base can, for example, be adapted to the new purpose by pseudonymization or reduction of data volume.

5) *Transparency:* the data subject as well as the system operators and the competent supervisory authorities must be able to understand, to a varying extent, which data are collected and processed for a particular purpose, which systems and processes are used for this purpose, where the data flow for which purpose, and who is legally responsible for the data and systems in the various phases of data processing. Transparency is necessary for the monitoring and control of data, processes, and systems from their origin to their erasure and is a prerequisite for lawful data processing. Informed consent, where it is necessary, can be given by data subjects only if these criteria are met. Transparency of the entire data processing operation and of the parties involved can help ensure that data subjects and supervisory authorities can identify deficiencies and, if necessary, demand appropriate procedural changes.

(6) *Intervenability:* data subjects are effectively granted their rights to notification, information, rectification, blocking and erasure at any time, and that the controller is obliged to implement the appropriate measures. For this purpose, controllers must be able to intervene in the processing of data throughout the process; from the collection to the erasure of the data.