PP12. USING AND IMPLEMENTING "PRIVACY BY DESIGN" PRINCIPLES IN COMMUNITY POLICING PROGRAMS

[Tags: Community policing, Privacy & Data Protection, Human rights]

Community policing programs should comply with the privacy by design principle and should have clear instructions and effective procedures on privacy.

Information regarding the privacy procedures as well as the relevant part of privacy audits that do not compromise the security of the system should be made publicly available.

Examples:

- Privacy by default is included in Art. 23 (2) GDPR and likewise ensures a privacy-compliant technology design. However, the GDPR has not only given Privacy by Design a direct legal effect by articulating it in article 25 but also unfolded some of its main principles, such as data minimisation and data security. Article 25, titled "Data protection by design and by default", provides that the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing.
- Moreover, Article 25 (2) GDPR provides that the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Mode of implementation:

- Products are set by default to privacy-friendly settings (e.g., use of cookies is illicit without the consent of the persons concerned). The aim is data reduction, or at least data minimisation;
- As both a data protection standard and a legal principle, Privacy by Design requires the designers of IT systems or business operations to integrate in the design the necessary measures to meet the following well-established privacy and personal data protection requirements:
    - ✓ lawful processing of personal data: by enabling the collection of the informed consent of the data subjects through a clear affirmative action and only after providing them with the details of the processing of their personal data;
    - ✓ purpose limitation: by informing the data subjects in a clear, precise, and accessible manner about the specific purpose(s), context, and scope of the data processing and by discouraging the processing of personal data for purposes incompatible with the system functions;
    - ✓ data minimisation: by processing the minimum, relevant, and necessary personal information to achieve the system functions;

- ✓ storage limitation: by storing the personal data of the data subjects only for the minimum amount of time necessary for achieving its functions;
- ✓ data accuracy: by enabling the data subjects to correct and update their personal data stored by the system and to erase the data that are no longer accurate in light of its functions;
- ✓ integrity and confidentiality: by providing the personal data processed with a high level of security against any breach such as unauthorised or unlawful access, disclosure or processing, accidental loss, destruction, alteration, or damage;
- ✓ transparency: by communicating to the data subjects in an accessible language and format the information about the processing of their personal data, specifically the identity of the data controllers, the purpose(s) of the processing, the legal basis of the processing, and the recipient(s) of the personal data;
- ✓ enablement: by enabling the data subjects to exercise their right to access, rectify, erase, and block personal data; right to object to the processing of personal data; right to be notified in the case of a data breach resulting in violating their human rights; and right to withdraw consent; and
- ✓ accountability: by conducting a privacy impact assessment identifying the privacy risks involved in the processing of personal data by the ICT system and identifying the design features and other measures necessary for addressing these risks.

Resources:

- 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), L 119/1, 4.5.2016 (GDPR).
- Ann Cavoukian & Mark Dixon, Privacy and Security by Design: An Enterprise Architecture Approach (Information and Privacy Commissioner Ontario, Canada: September 2013).
- Edith Ramirez, Remarks, Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission (Hong Kong, Privacy by Design Conference 13 June 2012).
- Handbook on European Data Protection Law (European Union Agency for Fundamental Rights & 2014 Council of Europe, 2014) at 36.
- Peter Schaar. "Privacy by Design" (2010) 3 Identity in the Information Society 267.
- GDPR, art. 35(1). The supervisory authorities have the duty to prepare a public list of the types of data processing operations that will require data protection impact assessment. See GDPR, art. 35(4).
- Ira S. Rubenstein & Nathaniel Good, "Privacy by design: A counterfactual Analysis of Google and Facebook Privacy Incidents" (2013) 28 Berkeley Technology Law Journal 1333.
- Inga Kroener and David Wright, "A Strategy for Operationalizing Privacy by Design" (2014) 30 The Information Society 355.
- Dirk van Rooy & Jacques Bus, "Trust and Privacy in the Future Internet—a Research Perspective" (2010) 3 Identity in the Information Society 397.

- Alessandro Acquisti, Curtis Taylor & Liad Wagman, "The Economics of Privacy" (2016) 54:2 Journal of Economic Literature 442.
- Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation, Doc. 00569/13/EN, WP 203 (2 April 2013).