PP13. LAW ENFORCEMENT AGENCIES SHOULD DESIGNATE A PRIVACY OFFICER

[Tags: Community policing, Accountability, Privacy & Data Protection]

Accountability is the principle that requires data controllers to implement the necessary internal measures and procedures to effectively apply, and demonstrate their compliance with, the data protection principles such as the principles of lawfulness of processing, purpose limitation, storage limitation, data minimisation, transparency, integrity and confidentiality, and data accuracy.

Complying with the accountability principle involves measures and procedures that may vary in light of the risks involved in the processing and the nature of the data processed. However, the GDPR specifies 3 accountability requirements: the first is data protection impact assessment, the second is prior consultation, and finally the third accountability requirement is the designation of a data protection officer.

Example:

- In accordance with data protection law, a data protection officer should be appointed if:
  - ✓ data processing is carried out by a public authority, except courts;
  - ✓ the main activity of the data controller or processor is processing operations that regularly involve extensive and systematic monitoring of the data subjects;
  - ✓ or the main activity of the data controller or processor is the processing of special categories of data, such as personal information relating to criminal records and other types of sensitive data listed in articles 9-10 of the GDPR, on a large scale.

Mode of implementation:

- The data protection officer will carry out a number of duties to ensure the compliance with the data protection principles including the duty:
  - ✓ to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
  - ✓ to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
  - ✓ to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
  - ✓ to cooperate with the supervisory authority;
  - ✓ to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.
- In carrying out these duties, the data protection officer must give due regard to the risks associated with the operations of personal data

processing and, at the same time, take into consideration the specifics of the processing: its nature, scope, context and purpose.

Resources:

- Alexander Dix, "EU Data Protection Reform: Opportunities and Concerns" (2013) 48:5 Intereconomics 268.
- Ann Cavoukian, Scott Taylor & Martin E. Abrams, "Privacy by Design: Essential for Organizational Accountability and Strong Business Practices" (2010) 33 Identity in the Information Society 405.
- Daniel J. Solove, Marc Rotenberg, Paul M. Schwartz, "Privacy, Information, and Technology" (New York, Aspen, 2006).
- Dirk van Rooy & Jacques Bus, "Trust and Privacy in the Future Internet—a Research Perspective" (2010) 3 Identity in the Information Society 397.