PP11. IMPROVING DATA PROTECTION INSIDE COMMUNITY POLICE PROGRAMS

[Tags: Community policing, Legislation, Privacy and Data Protection]

Law enforcement agencies should have clear instructions and effective procedures on privacy and data protection, including procedures for data retention, accessibility and data subject right management.

Thus, community police programs should handle personal data in accordance with the main principles of data protection:

- ✓ Lawful processing;
- ✓ Purpose limitation;
- ✓ Data minimisation;
- ✓ Storage limitation;
- ✓ Data accuracy;
- ✓ Integrity and confidentiality;
- ✓ Transparency;
- ✓ Enablement;
- ✓ Accountability.

The community-policing program must enable data subjects to exercise their rights, such as the right to correct personal data.

It is important to communicate to both the police officers and citizens the data protection procedures, as well as the relevant parts of data protection impact assessments that do not compromise the security of the system.

Examples:

- There should be a reference to the users right to access information, to rectify or erase personal data, e.g. in a menu point "User Info" or a link to an information site within any functionality or application processing personal data.
- One of the central guidelines to be followed is the principle of data avoidance or "Datensparsamkeit". Originating in German privacy legislation (§ 3a Bundesdatenschutzgesetz - BDSG Federal Act on Data Protection) and mentioned in Art. 43 (2) lit d GDPR, data avoidance refers to the idea of limiting the collection of personal information to the minimum absolutely required for data processing regarding a specific purpose.

Mode of implementation:

- Informed consent and transparency are two fundamental conditions upon which the data protection framework is built;
- As a general rule, personal data may therefore only be processed if the data subject has unambiguously consented. Exceptions to the requirement of informed consent can however be justified if processing of personal data is necessary for the performance of a contract to which the data subject is party, for compliance with a legal obligation, for the performance of a government task, to protect the vital interests of the data subject, or to protect the legitimate interests of the controller, except where such interests are overridden by the interests of the data subject;
- Informing the citizen as to what purpose the personal data is being collected. Specification of the purpose is a pre-requisite for applying other

data quality requirements, including the adequacy, relevance, proportionality and accuracy of the data collected and the requirements regarding the period of data retention.

Resources:

- Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, 27 February 2014.
- Hope, Dunstan Allison: "Protecting Human Rights in a Digital Age", 2011.
- Njeri, Mutheki Tropister, "Citizens on Patrol: Mobile technology in enhancing community policing", May 2013.
- Potere, Michael: "Who will watch the watchmen? Citizens recording police conduct", Northwestern University Law Review Vol. 106, No. 1, 2012.