39th International Conference of Data Protection and Privacy Commissioners Hong Kong

Closed Session: Government Information Sharing – the Estonian model

Proposed presentation by Viljar Peep

Key themes for presentation

This is a draft outline of the presentation being delivered by Viljar Peep.

1. Northern Europe seems to be a region having less privacy concern:
    a. Public sector datasets are widely cross-linked.
    b. "Collect once, use many times" model.
    c. Personal ID-numbers are not secret.
    d. Personal ID-numbers have been used across the public and private sector.
    e. Personal ID-numbers are recognisable (incl. date of birth), not randomly combined.
    f. Estonia: e-ID (digital authentication and signing) is mandatory and widely used. It saves around 2% of the GDP.
    g. Estonian online-services: companies' registration (99%), e-banking (99%), tax declaring (96%), local and national election (31%). Online health records, medical prescriptions…

2. Government's datasets – is it a super-database or a dispersed system?
    a. Many databases + one classificatory system + one security system + one blockchain-based data exchange layer (shared with Finland) + one system for uniformed descriptions of databases/services + eID as access key + data-embassies.
    b. Non-duplication-principle = referencing rather than storing.
    c. Fine-grade logging and auditing of accesses.
    d. Uniformed detailed descriptions of databases/services – used for approval proceedings by the national data protection authority and the national IT and cyber security authority.
    e. The data protection authority oversees all aspects of public sector information management. Coordinated activities with the IT and cyber security authority.

3. Personal ID schemes – how to create trust and confidence?
    a. Publicly available personal ID = no secrets to steal.
    b. Recognisable ID = memorability, no problems with namesakes (especially when publishing unpleasant information), exact searches.
    c. Unique personal ID in universal use = more transparency for individuals.

4. The government owes a secure e-ID to its citizens
    a. Issued like passports – the holder is the right person.
    b. The ID-card contains two certificates (authentication + signing). Mobile ID is voluntary.

    c. Two-factors-identification.
    d. Personal ID-numbers can be used for encryption of documents.
    e. No biometrics. No Near-Field-Connection.
    f. Available for the private sector services (widely used) and for good foreigners (e-residents).

5. Citizen’s trust and confidence is the key (Eurobarometer special surveys on privacy and cybersecurity):
    a. Privacy and transparency cultures are regionally diverse.
    b. Privacy concerns are lower when a society is more transparent.
    c. Privacy and cyber security concerns are lower when the Government builds up the basic digital infrastructure.
    d. Online banking as an example: more usability = more trust and confidence = more security awareness.
    e. Frequent use of digital services: less privacy concerns, more concerns on data quality.