Regulatory framework in the e-society

Rights and responsibilities in a borderless society

Tallinn 10 April 2019

Katrin Nyman Metcalf
Programme Director Research and Legal Issues,
eGovernance Academy

Katrin.Nyman-Metcalf@ega.ee
Legal obstacles to e-government?

- The difference between applying law and creating law
Building Blocks of the Digital Society

IT

Symbols
Perceptions

Education
Awareness

LAW

Organisation
Trust!
Data Protection

- The development of information society must not undermine **people’s sense of security** or the protection of their fundamental rights.
- Data protection is a key issue in a modern information society - **Human right to privacy** (Article 7-8 EU Charter, Article 8 ECHR, etc.)
- The law should focus on **content** of data **rather than form**
From Directive 95/46 to Regulation 2016/679, adopted April 2016, in effect from May 2018

Importance also outside of EU

Difference between Directive and Regulation:

- Regulations are directly applicable in Member States, the same rules will apply everywhere
- Directives are implemented by national law and some differences can exists, the aim rather than the details are binding
Global impact of EU rules

• Processing of personal data of EU controllers/processors or those providing services to EU subjects shall be carried out in accordance with EU law, regardless of whether processing takes place within the EU. The legal form – branch, subsidiary with legal personality - is not the determining factor.

• Adequacy decisions – if standards are sufficient, even if system is different, takes into account various aspects
Principles (Article 5 GDPR)

- Personal data shall be:
  - (a) processed lawfully, fairly and in a transparent manner;
  - (b) collected for specified, explicit and legitimate purposes (purpose limitation);
  - (c) adequate, relevant and limited to what is necessary;
  - (d) accurate, up to date;
  - (e) kept in a form which permits identification of data subjects for no longer than is necessary;
  - (f) processed with integrity and confidentiality.
Lawful processing (Article 6 GDPR)

- Processing is lawful only if and to the extent that at least one of these applies:
  - consent - for specific purposes
  - necessary for the performance of a contract
  - compliance with a legal obligation
  - necessary in order to protect vital interests of the data subject or of another natural person
  - necessary for the performance of a task in the public interest or exercise of official authority
  - other legitimate interests if not overridden by fundamental rights and freedoms
Consent

- Consent should be given by a clear affirmative act showing *freely given, specific, informed and unambiguous* indication of agreement.

- Examples: written statement, including by electronic means, oral statement (statement or clear affirmative action). May include ticking a box on a website, choosing technical settings, etc. -must clearly indicate acceptance. Silence, pre-ticked boxes or inactivity should not constitute consent.
Databases: what needs regulation?

• Definition of databases: an organised collection of information, regardless if ICT or not. Practical issues, access, data protection - differs depending on form but legal protection should be the same.

• Who is owner of the data? Rights of users of information.

• Data services are the priority, not data collection.

• Responsible body (Ministry or other) for the integrated system - each database has a responsible administrator.

• Registration of databases including verification of technical systems.

• Cross-institutional interoperability.

• Database set up (and terminated) through law or a legal act based on law.
Interactivity: Digital ID and Signature
Since 2002
Digital Identity: Legal aspects

• What is the role of a signature - of identification - from a legal viewpoint?
  • *When this is properly understood, the role can be recreated electronically*

• How can this be created electronically? What are the key elements that need to be created?
  • Ensure that the person is who he/she claims
  • Possibility to identify one individual and one individual only
  • Durability of identification

• Verification of digital identity: *What you know – what you have – what/who you are*
The legal framework

1. There should *not* be a lot of specialised legislation on e-governance (but a proper analysis of all laws is needed)

2. Data protection is essential (also for the perception of e-governance), focus on content and not form

3. e-identification must be established and regulated by law

©ega.ee