Data Protection and Privacy for the Smart Grid

Panel Session: SPARKS

Marie Holzleitner

EU FP7 Programme Contract No. 608224

2 new pieces of EU Legislation for Data Security and Breach Reporting

1) The General Data Protection Regulation 2016 (GDPR) and
2) The Network and Information Security Directive 2016 (NIS- or Cybersecurity Directive)

EU FP7 Programme Contract No. 608224

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Focus:

NIS Directive: focused on network security to improve security of the Internet and private networks and information systems

GDPR: safeguard personal data

Requirement:

NIS Directive: requires operators to appropriately secure their networks to protect the provision of the service

GDPR: requires controllers to adopt measures that secure personal data

EU FP7 Programme Contract No. 608224

General Data Protection Regulation

- Notice requirements remain and are expanded.
- Automated individual decision-making, including profiling (Article 22) is made reviewable.
- Privacy by Design and by Default (Article 25).

  → Privacy settings must be set at a high level by default.
- Data Protection Impact Assessments (Art. 35).
- Risk assessment and mitigation is required.

- Data Protection Officers (Art. 37–39) are to ensure compliance within organizations.
- Data Protection Officers have to be appointed:
  - for all public authorities, except for courts acting in their judicial capacity
  - if the core activities of the controller or the processor consist of
    - processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale or
    - processing on a large scale of special categories of data or processing personal data relating to criminal convictions and offences

EU FP7 Programme Contract No. 608224

Rights of the data subjects (consumers)

- the right to be informed
- the right to access their own personal data,
- the right to rectify any wrong or incomplete information,
- the right, in some cases, to object to the processing on legitimate grounds,
- the right not to be subject to an automated decision
- the right to judicial remedy and to receive compensation from the data controller for any damage suffered

Source: S3C; Guideline: Privacy and Data Protection

EU FP7 Programme Contract No. 608224

Data controllers' (service provider) obligations

- ensure the data subjects' rights are correctly observed
- ensure observance of the data minimisation principle
- ensure observance of criteria for making data-processing legitimate
- safeguard confidentially of processing
- safeguard security of processing
- notify processing of personal data to the national data protection authority (DPA)
- the right to the erasure of data

Source: S3C; Guideline: Privacy and Data Protection

EU FP7 Programme Contract No. 608224

THANK YOU FOR THE DISCUSSION

Mag. Marie-Theres Holzleitner

Energieinstitut an der Johannes Kepler Universität Linz

Altenberger Straße 69

4040 Linz, AUSTRIA

Tel: +43 723 2468 5675

Fax: + 43 723 2468 5651

e-mail: holzleitner@energieinstitut-linz.at

EU FP7 Programme Contract No. 608224