THE IMPACT OF DATA PROTECTION RULES ON CORPORATE INFO SECURITY AND INCIDENT RESPONSE MANAGEMENT – The Energy sector

CEER Cybersecurity Workshop

Friday 21 june 2019

Massimo Attoresi

(European Data Protection Supervisor)

IT Policy officer – Data Protection Officer

The GDPR and the energy sector

- Regulation (EU) 2016/679 on the **protection of natural persons** with regard to the processing of personal data.....
- Energy sector and processing of personal data:
  - data provided by the customer for contract management and billing
  - data collected at the smart meter's level (readings);
  - data of the smart house (in case the energy operator is involved);
  - data provided by the customer or others for customer care and business improvement purposes;
  - data and infrastructure security;
  - ……
- Legal bases: law, legitimate interest, consent

Cybersecurity rules in the GDPR

- Art.32 - security of processing of personal data
  - The mandatory risk-based approach
  - The role of codes of conduct and certification mechanisms.
- Art. 33 - notification of a personal data breach to the supervisory authority
  - RISK for data subjects: notification to the SA within 72 hours
- Art. 34 – communication of a personal data breach to the data subject
  - HIGH RISK for data subjects: communication to the data subjects involved without undue delay

GDPR, corporate info security and incident management

- What are the new elements integrated?
  - **Difference of nature of risk to be assessed** and **notification obligations**
  - The role of codes of conduct and certification mechanisms.
- Overarching rule: art.25 on data protection by design and by default
  - Security of personal data by design and by default, too !
  - Protection of confidentiality, integrity and availability (and non-repudiation) of personal data as an early requirement and throughout the project lifecycle.
  - This approach benefits non-personal data, too: the whole project
- State of the art of protective measures
  - The experience of the BAT for the 10 minimum functional requirements of smart metering systems.

Then...what shall I change in my organisation?

- Do GDPR rules oblige me to have a parallel info security and incident management process?

  Which of the three replies would you consider?

  1. Yes. A complete new assessment of risks for personal data needs to be carried out and a different process to be set up for incident
  2. No, I need just to integrate the new notification and communication requirements in case of a personal data breach
  3. No. I need to consider also the risks for the individuals whose data are processed (further to those to corporate assets and other compliance obligation), and the new notification and communication requirements in case of a breach of personal data security.

- Looking for shared, processes integrating the many compliance obligations within the industry. The way forward?

  Personal views:

  - Industry and their representative to play a proactive, by proposing and sharing best practices and processes
  - Codes of conducts, integrating how to deal with compliance requirements, may play an important roles
  - Indeed Member States need to contribute resources to facilitate all this, especially when it comes to SMEs

Thank you!

For more information:

www.edps.europa.eu

edps@edps.europa.eu

@EU_EDPS

EDPS

European Data Protection Supervisor


Any questions ?