SAURON

Data Protection and Critical Infrastructures in the EU

The impact of the General Data Protection Regulation and the Network and Information Systems Directive on Critical Infrastructure Protection

Laurens Naudts, Plixavra Vogiatzoglou, Anton Vedder

(KU Leuven, imec – CiTiP)

Novel approaches in Risk and Security Management for Critical Infrastructures

Vienna 19th and 20th September 2017

KU LEUVEN
CENTRE FOR IT & IP LAW

Outline

Sauron

A. The EU Legal Landscape

B. EU Data Protection Framework
   I. Main Definitions
   II. Main Obligations

C. Critical Infrastructures: Challenges
   I. Accountability
   II. Data Protection by Default and Design
   III. Data Protection versus Security
   IV. Breach Notification
   V. Data Sharing

The EU Legal Landscape

The CID, NISD and GDPR

The EU Legal Landscape

	Critical Infrastructures Directive	Security of Networks and Information Systems Directive	General Data Protection Regulation
Date of Adoption/Application	8 December 2008	6 July 2016 (10 May 2018)	27 April 2016 (25 May 2018)
Objectives	• Identification & Designation ECIs • Improve CI protection • Operator Security Plan • Security Liaison Officer	• Ensure common security level across EU • National CS Strategy • National single point of contact • Incident Response Team (& Network) • Cooperation Group • Security and Breach Notification Requirements	• Protection of Personal Data Processing • Data Protection Officer • Controller/Processor Agreements • Data Protection by Design (T&O Measures, PIA) • Breach Notification • Etc.…
Scope of Application	• Member States • European Critical Infrastructure Operators (Energy (gas, electricity, oil) and transport)	• Member States • Operators of Essential Services (energy, transport, banking, financial market, health, etc.) • Digital Service Providers (online search engines, online market place, cloud computing)	• Member States • Data Controllers • Data Processors

Overlap: processing of personal data pursuant to NIS Directive, e.g. security related personal data processing activities, e.g. intrusion detection or data sharing, by operators of essential services. (See also: Recital 72 and Art. 2 Nis Directive)

The General Data Protection Regulation

Main Definitions and Obligations

EU Data Protection Framework – Main definitions

Personal data: data related, directly or indirectly, to an identified or identifiable natural person (data subject)

Data Processing: (any) operation(s) on data/data sets

Material Scope of Application

Data Controller: entity which determines the purposes and means of data processing

- Alone or jointly with others
- Control over decisions
  - Specification of purpose (the 'why')
  - Determination of the 'means', e.g. technical and organizational measures (the 'how')
  - E.g.: critical infrastructure operators, essential service providers, research consortia, etc.

Data Processor: entity which processes personal data on behalf of the controller

Main obligations I.

Data Controller: demonstrate compliance data principles (accountability, Art. 5 GDPR)

a) Fair, lawful and transparent data processing:
- Legal ground:
  - Performance of contract
  - Performance of task of public interest or exercise of official authority
  - Legitimate interest of controller or third party

b) Purpose Limitation

c) Data Minimization

d) Data Accuracy

e) Storage Limitation

f) Integrity and Confidentiality
- Appropriate security of personal data, e.g. unauthorized access, accidental loss.

Main obligations II.

Data Processor:

a) Acts only within limits of instructions set by controller

b) Implementation of appropriate technical and organisational measures to ensure data protection

➔In the case of 'data outsourcing' the controller remains liable for damage caused by *any* GDPR infringement:

- *"A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller." (Art. 82 §2 GDPR).*

The General Data Protection Regulation

Challenges for critical infrastructure (security)

Accountability: The ability to provide reasons in order to explain and justify actions, decisions and policies for a forum of persons or organisations.

- **Demonstrate compliance with GDPR principles (Art. 5 §2 GDPR)**
  - Internal documentation of data policies and procedures
  - Designation of Data Protection Officer
  - Data protection impact assessment
  - Data Protection by Design
- Ensure transparent data processing (Art. 13, 14 GDPR)
- Safeguard data subjects' (subjective) rights
  - Access (Art. 15 GDPR), Rectification (Art. 16 GDPR), Erasure (Art. 17 GDPR), Restriction (Art. 18 GDPR) Portability (Art. 20 GDPR), Object (Art. 21 GDPR), Automated Decision-Making (Art. 22 GDPR)
- Cooperation with DPAs
- Breach notification

Internal

External

Data Protection by Default and Design (Art. 25 GDPR):

- **Data Controllers:** ensure the integration of data protection principles through internal measures and policies, both technical and organizational.
- **Product/Service Providers:** ensure the integration of data protection principles when developing and designing services, products and applications, with due regard to the state of the art.

Data Oriented Strategies	Process Oriented Strategies
MINIMISE	INFORM
HIDE	CONTROL
SEPARATE	ENFORCE
AGGREGATE	DEMONSTRATE

Source: ENISA

I. Privacy and Data Protection ⇔ Security

- GDPR: fair and lawful data processing
- NIS Directive: security of network and information systems
- Both require: technical and organisational measures to enhance interests covered.

II. Privacy Enhancing Technologies (Art. 25 GDPR) ⇔ Security Enhancing technologies (e.g. Annex II CID, Art. 14 & 16 NIS)

- Different mechanisms available to ensure security, but diverging desirability concerning their adoption
- Balancing data protection measures versus security
  - Intrusion detection: Confidentiality versus Integrity (e.g. encryption versus deep packet inspection)
    - However: advancements in searchable and homomorphic encryption

BREACH NOTIFICATION

GDPR (art. 33)	NIS Directive (ES) (Art. 14)	NIS Directive (DSP) (Art. 16)
Personal Data Breach (unless unlikely to result in a risk to the rights and freedoms of natural persons)	(Security) Incident with **Significant Impact** (number of users affected, duration, geographic spread)	**Substantial Impact** on the provision of covered service (number of users affected, duration of the incident, geographic spread, extent of disruption and extent of impact on economic/societal activities)
Within 72 hours or, if unfeasible, without undue delay.	Without undue delay	Without undue delay
Information on nature of the breach (data subjects, records, concerned), name contact point, likely consequences of personal data breach and measures to mitigate adverse effects)	Information facilitating determination cross-border impact.	
	Notification does not make notifying party subject to increased liability.	Notification does not make notifying party subject to increased liability.
To Data Protection Authorities **and** to data subject without undue delay	To competent authority on security of NIS or CSIRT	
	MUST also apply GDPR (1st column) if personal data included	MUST also apply GDPR (1st column) if personal data included

Information sharing: Exchange and sharing of security related information, e.g. security incidents, amongst private actors, including critical infrastructures, and public authorities

- Mandatory: notification requirements under GDPR and NIS Directive, CSIRT Network, etc.
- Voluntary: platforms eg. Critical Infrastructure Warning Information Network (CIWIN), European Reference Network for Critical Infrastructure Protection(ERNCIP), NIS Public-Private Platform (NISP),, etc..

Important: Data sharing remains subject to GDPR (see also Recital 72 and Art. 2 Nis Directive)

Information sharing remains primarily a matter of trust.

Proposal Regulation on Free Flow of Non-Personal Data (COM(2017) 495 final)

Regulation Aim: *Establish clear framework accompanied by cooperation between and with Member States, as well as by self-regulation, in order to enhance legal certainty and increase trust levels.*

- Principle of free movement of non-personal data
  - *Data stored by natural or legal person in EU*
  - *E.g. general prohibition of data localisation requirements, unless if justified by public security*
- Data availability for regulatory control by competent authorities
- Encouragement of codes of conduct
- Single point of contact
- Free Flow of Data Committee

KU LEUVEN
CENTRE FOR IT & IP LAW

Sauron

SAURON

Thank you for your attention!

Questions?