Cybersecurity for Europe

Insights Webinar: Developments in European Regulations

Monday, 17 May 2021

Fostering Rights Through Technology

Alessandro Mantelero
Associate Professor of Law | Polytechnic University of Turin

Research partially funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830929

< I >

Data protection and cybersecurity

Cyber Security for Europe

Sector-specific studies on EU data protection and cybersecurity provisions

- ✓ Different legal domains (private/administrative law vs. criminal law)
- ✓ Detrimental effects:
  - Obligations and procedures, often deeply interrelated in the daily business activities, are considered as separate
  - Sector-specific analysis fails to reveal the common approach of EU regulation
  - An obstacle to the development of an integrated model for legal compliance

< II >

Challenges, objectives, and outcome

Challenges and objectives

- ✓ Bridging the gap and business perspective
- ✓ CyberSec4Europe H2020 Project
- ✓ Comparative and coordinated analysis of the main regulatory instruments (GDPR, NIS directive, PSD2 Directive and eIDAS Regulation)
- ✓ Limitation: At this stage of implementation, it is not possible to provide a fully integrated picture of the various obligations in these fields

- ✓ Key objectives:
  - To identify common patterns of obligations deriving from the different legal instruments
  - To highlight the relations between these obligations (including technology-based organisational and security measures)

Outcome and impact:

- ✓ A basis for a future integrated compliance model
- ✓ A steppingstone for rule makers towards a more comprehensive technical and legal harmonisation in the national implementation of the EU framework

< III >

Data protection and cybersecurity

GDPR and other legal instruments

- ✓ The GDPR provides a general framework
  - Main binding principles (data use and data security)
  - Principles-based approach and further elaboration by other regulations (technology-based and context-specific provisions)

The GDPR refers to the implementation of *appropriate technical and organisational measures*

- ✓ Appropriateness: a contextual notion
- ✓ Sector-specific instruments (NIS, PSD2, and eIDAS) frame appropriateness in terms of risks and available responses

A. Mantelero, G. Vaciago, M.S. Esposito, N. Monte. 2020. **The common EU approach to personal data and cybersecurity regulation.** *International Journal of Law and Information Technology*, 28(4): 297–328, https://doi.org/10.1093/ijlit/eaaa021

Table 1: (continued)

Rules and principles	GDPR	Technical and organizational measures
Data protection by design and by default	Recital 78 Article 25	**Organizational measures** • Adoption of specific security requirements and procedures from the early stages of the development lifecycle • Procedures to integrate data protection safeguards into processing activities **Technical measures** • Special technologies to support privacy and data protection (PETs) (ie tools that encourage data minimization, anonymization or limitation of use, amongst other things)
Regular assessment of the effectiveness of the security measures adopted	Article 32.1.d	**Organizational measures** • Records of technical and organizational security measures taken **Technical measures** • Vulnerability and penetration testing (eg vulnerability scanning, ethical hacking)
Notifications, reporting obligations, and mitigation measures (data breaches)	Recitals 85, 86, 87 Articles 33, 34	**Organizational measures** • Procedures to immediately detect whether a personal data breach has taken place • Incident response plan **Technical measures** • Data flow and log analysers • Tokenization, encryption, etc.
Business Continuity, Disaster Recovery, and resilience	Article 32.1.b, 32.1.c	**Organizational measures** • Business continuity plan • Data restore procedures • Adoption of an effective cyber-resilience approach • Disaster recovery plan **Technical measures** • Backup techniques • Business continuity technologies (eg redundancy techniques)

- ✓ Not a patchwork, but a coordinated model, including its technological implementation

- ✓ Five central pillars:
  - Risk-based approach
  - By-design approach
  - Reporting obligations
  - Resilience
  - Certification schemes

Alessandro Mantelero

alessandro.mantelero@polito.it

@mantelero