European cybersecurity and data protection regulation: Challenges and opportunities

dr. Irene KAMARA

Assistant Professor, Tilburg Institute for Law, Technology, and Society

Dansk Standard Cyberdag, 29 September 2022

Tilburg Institute for Law, Technology, and Society

About me

- Assistant professor and Research Coordinator at Tilburg Law School in the Netherlands, affiliate researcher at Vrije Universiteit Brussel (Law & Criminology)
- PhD in Law on standardisation as a private regulation instrument to support EU data protection law
- Teaching cybersecurity and cybercrime law, data protection, privacy and anti-discrimination at law bachelor and master students, and data scientists.
- Lawyer
- Member of NEN TC Cybersecurity and Privacy (381027)
- ENISA Experts List for assisting in the implementation of its Annual Work Programme

Data Protection Certification Mechanisms

Study on Articles 42 and 43 of the Regulation (EU) 2016/679

Final report

Guidance and gaps analysis for European standardisation

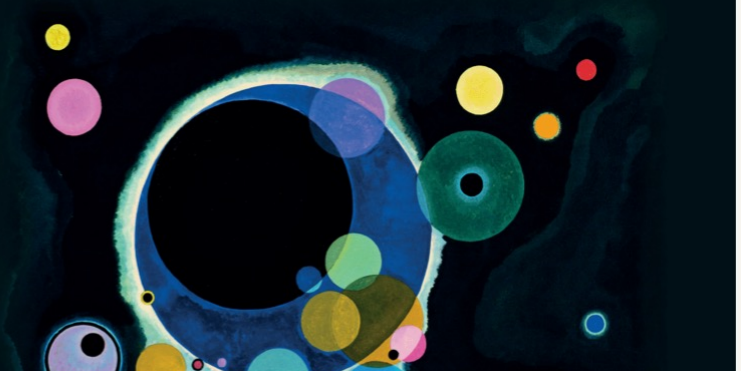
Privacy standards in the information security context

Ronald Leenes
WITH
Irene Kamara

Data Protection Standardisation

The role and limits of technical standards in the European Union data protection law

IRENE KAMARA



Recommendations on European Data Protection Certification

Law School

LTMS

The Cybersecurity Certification Landscape in the Netherlands after the Union Cybersecurity Act

Final Report

Irene Kamara, Ronald Leenes, Kees Stuurman, Jasper van den Boom

Outline

- Key concepts
- EU law
- Role of standards to support EU data protection law, cybersecurity, and electronic privacy
- Priorities & challenges

Privacy

- *Article 7*
- **Respect for private and family life**
- Everyone has the right to respect for his or her private and family life, home and communications.

Personal data protection

- Article 8 Charter of Fundamental Rights EU
- **Protection of personal data**
- 1. Everyone has the right to the protection of personal data concerning him or her.
- 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
- 3. Compliance with these rules shall be subject to control by an independent authority.

What is personal data?

- Art. 4(1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

What is personal data?

Personal data

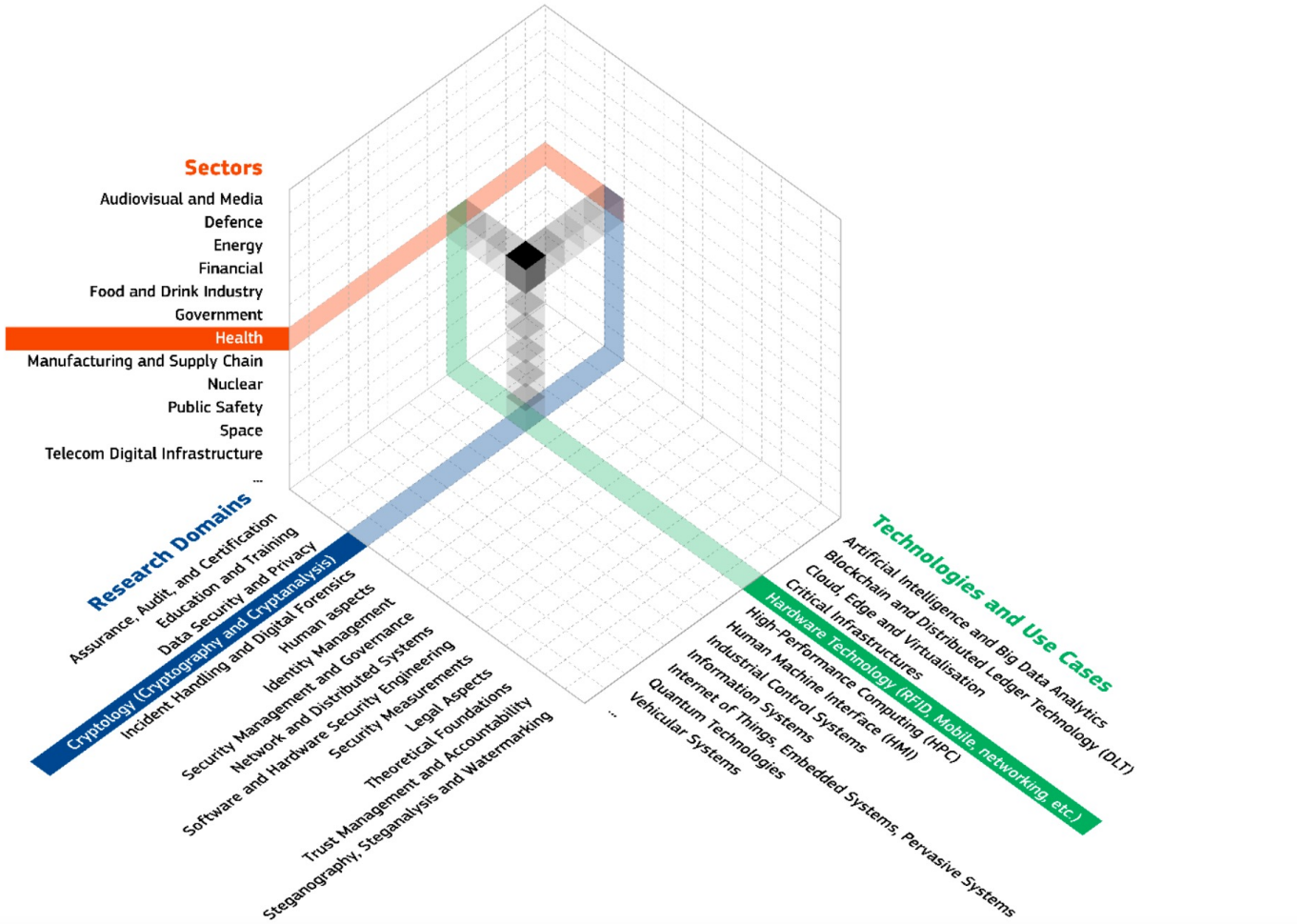
- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone);
- an Internet Protocol (IP) address;
- a cookie ID;
- the advertising identifier of your phone;
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

Non-personal data

- a company registration number;
- an email address such as info@company.com;
- anonymised data.

Source: European Commission

Cybersecurity

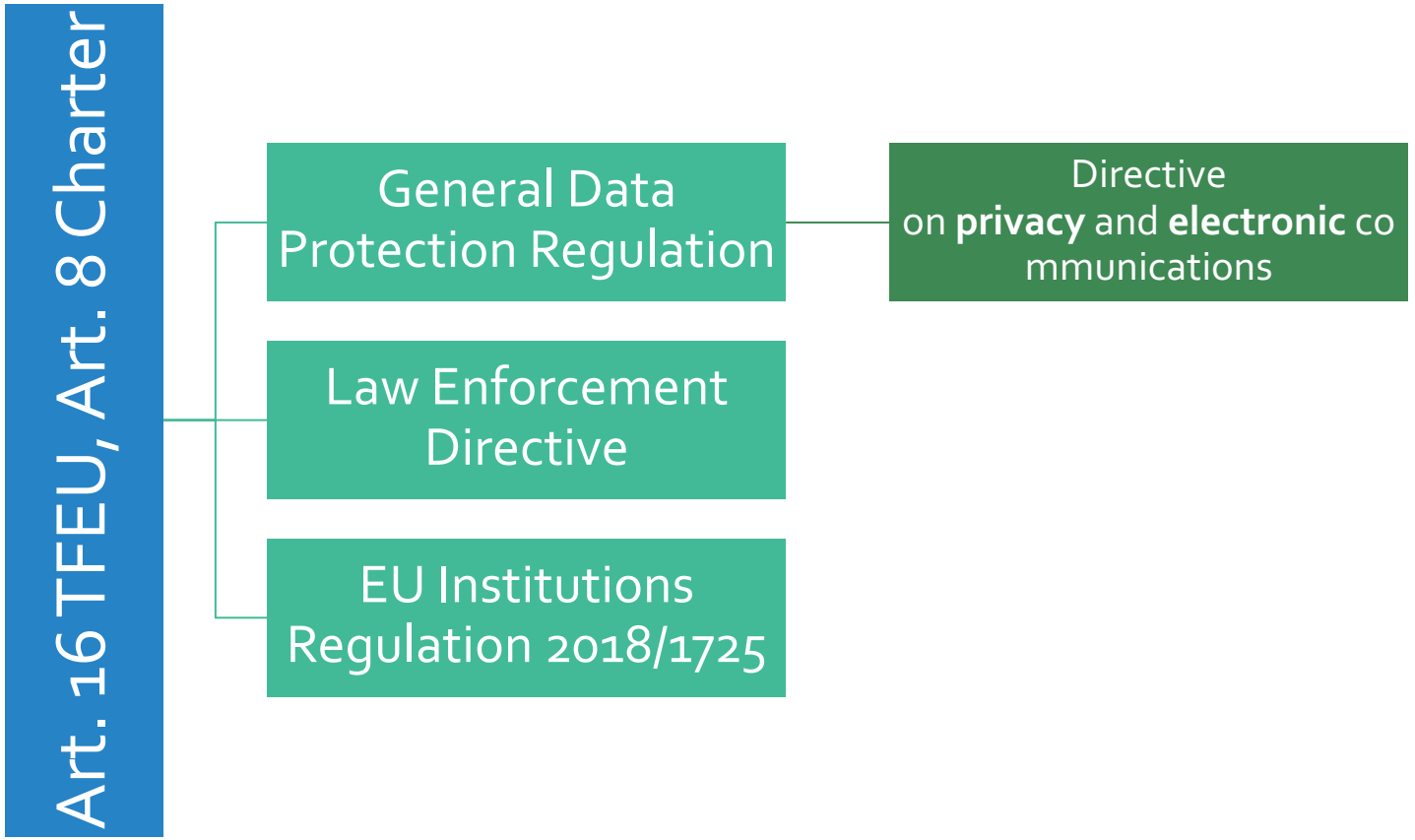


Source: EC Joint Research Centre, Taxonomy for Cybersecurity, 2019

Overview of main EU cybersecurity laws

Cybersecurity Act	• Regulation • 2019/881
Network & Information Security Directive	• Directive 2016/1148 • Revised in 2022, final text pending publication
EU Cybercrime Directive	• on attacks against information systems • 2013/40
EU Cyber resilience Act	• Published proposal for horizontal Regulation providing cybersecurity requirements 2022/0272 (COD)

Overview of personal data protection EU law



Why standards to support EU data protection & cybersecurity law?

- Growing number of references to the concept of technical standards in the text of EU law
- Informal guidance by supervisory authorities →standards as a solution to assist organisations with legal compliance
- Very broad scope of application of the law: companies need support
  - Cross-border business
  - Small Medium Entreprises (SMEs)
- Reliance on technology –> value sensitive design
  - Data protection by design
  - Security by design

Role of European standards in EU data protection & cybersecurity law

Clarity & interpretation	**Implementation and compliance**	**Technology-triggered**
Definition of concepts	Uniform application across companies, Member States, sectors	Translation of legal requirements to technical auditable requirements and controls
Interpretation of principles and provisions	Assisting enforcement, providing a benchmark for supervisory authorities	Technical measures for compliance, state of the art
	Accountability for those with a duty to comply	Enforcement by means of technology

Irene Kamara, 2021

Standardisation Strategy 2022

- data standards enhancing data interoperability, data sharing and data re-use in support of the Common European Data Spaces.

- new technology challenges and horizontal considerations: artificial intelligence, data protection or cybersecurity

Rolling Plan for ICT Standardisation 2021

Key priority: e-privacy	Standardisation of web browser functionalities aiming to convey user wishes on online tracking
	Location data by mobile applications
Specific focus areas	Standards to provide requirements for GDPR certification
	Privacy policies & statements
	Anonymisation and pseudonymization of data
	Privacy management & user-centric approach
	Data protection by design and default to prevent unwarranted pervasive monitoring
	Secure coding standards for secure application development

Challenges & Opportunities

For regulators:

- The role of conformity assessment
  - EU law sometimes limits the (formal) role of standards to support certification – e.g. GDPR
- Different approaches within EU law (sometimes NLF-presumption of conformity v. looser role of standards)

For companies:

- how to navigate & select the most suitable standards
  - Companies often informed by media, associations
    - Especially SMEs with limited budget

For legislative goals:

- Need for cross-sector & horizontal standards
  - E.g. connecting AI Regulation with privacy and data security

Challenges & Opportunities II

- Trust in the standardization system: standards pertaining to fundamental rights → increased participation of civil society, ensuring representation of different stakeholders at national committees
  - Good practice: NEN – thematic workshop on data protection: updates to larger stakeholder group, beyond TC experts
  - Online platform SPICE with updates and news - community building
- Alignment of harmonised standards with EU law
  - 2022 COM Report of Implementation Regulation 1025/2012 2015-2020
    - *"Across all sectors, only 27,58% of the HAS assessments came out as positive31, mainly due to inadequacy with EU law, showing that more work is to be invested in the development process of standards – e.g. within the technical committees – so that the work is more aligned with the policy and legal requirements. "*
  - ENISA Study 2018
    - *The existence of stable mechanisms and experts pools would guarantee consistency in the long-term and ensure avoidance of overlap of standards. Furthermore, such practice would identify potential overlap even among European standards developed by CEN and CENELEC on the one hand, and ETSI on the other.*
- Clear benefits for companies processing personal data

Thank you

i.kamara@tilburguniversity.edu