

TECHNICAL STANDARDS TO ACHIEVE DATA PROTECTION BY DESIGN IN DATA SPACES

AEPD – ENISA CONFERENCE ON DATA SPACES

Dr. Irene Kamara

Madrid, 2 October 2023







EXISTING TECHNICAL STANDARDS ON DATA PROTECTION BY DESIGN AND BY DEFAULT

European Standard FN 17529:2022

Data protection and privacy by design and by default

CEN/CLC/TR 17919:2023

Data protection and privacy by design and by default - Technical Report on applicability to the video surveillance industry - State of the art

(under development)

Privacy management in products and services - Biometric access control products and services

Technical standards

ISO 31700-1:2023

Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements

ISO/TR 31700-2:2023

Consumer protection — Privacy by design for consumer goods and services — Part 2: Use cases (online retailing, fitness company, smart locks)

ISO/IEC/IEEE 15288:2023

Systems and software engineering — System life cycle processes

ISO/IEC TR 27550:2019

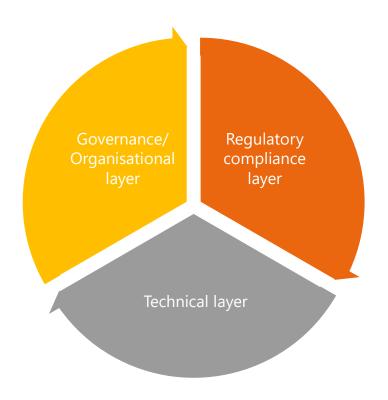
Information technology — Security techniques — Privacy engineering for system life cycle processes





WHAT POSSIBLE USE OF TECHNICAL STANDARDS FOR DATA SPACES?

◆ Data spaces: Infrastructure which facilitates access to data and thus the development of business models based on its exploration and exploitation (AEPD 2022)



| Governance/reg | technical |
|---|---|
| Determination of DPbD requirements | System requirements definition |
| Record of processing activities | Architecture definition process |
| Consumer communication requirements | Design definition process |
| Assessing risk capabilities of third parties | Secure multi-party computation: models & properties ISO/IEC 4922-1:2023 |
| Preparing data breach response plans | |
| Designing & implementing privacy controls | |
| Design interface to enable access of data subjects rights | |





CHALLENGES – NEED FOR NEW DATA SPACE STANDARDS ON DATA PROTECTION BY DESIGN?

- Current DPbD standards focus on organisations, not the processing lifecycle across organisations
 - overview of processing in case of complex configurations of data spaces with multiple data holders, intermediaries and data users?
- For example COM Proposal for EHDS on 'access to data':

"bring questions to data instead of moving data" / compute-to-data approach

→ not reflected in an existing data protection by design standard.

- Need for update of existing European & international standards?
- Need for a Technical Report specifying how EN 17529 applies to Data Spaces?
- Integration of data protection by design and by default in standards on Data Spaces?
 - ◆ DIN SPEC 27070:2020-03 -Requirements and reference architecture of a security gateway for the exchange of industry data and services
- Common specifications?





TILBURG INSTITUTE FOR LAW, TECHNOLOGY, AND SOCIETY

WWW.TILT.NL

