Use of standards for GDPR compliance

Irene KAMARA, Tilburg Law School
ISO/IEC 27701 - De ontbrekende schakel tussen informatiebeveiliging en AVG
Rotterdam, 26 November 2019
ABOUT US

Tilburg Institute for Law, Technology, and Society

TILT studies emerging technologies and their impact on the individual and society, recognizing the interplay between technology, regulation and fundamental values and human rights.
Outline

• Introduction

• Law perspective: Standards in the General Data Protection Regulation.

• Compliance perspective: Needs of controllers and processors to trust standards.

• Supply perspective: existing standards in privacy & conformity assessment.

• Conclusions
LAW
Standards in the GDPR

2012 Commission proposal

Art. 12 (6)  Procedures and mechanisms for exercising the rights of the data subject.

Art. 14(8)  Information to the data subject.

Art. 18 (3)  Right to data portability.

Art. 23(4)  Data Protection by Design and by Default.


Art. 39 (3)  Certification.
Standards in the GDPR

2014 European Parliament First Reading

Art. 13(a)  Standardized information Policies

Art. 19(2b)  Right to object and profiling

Art. 39(1e)  Certification – standardized data protection mark ‘European Data Protection Seal’

Art. 39(1i)  Certification – the EDPB may certify that a data protection enhancing technical standard is compliant with the Regulation.
Art. 43 - certification

- the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council (1) in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

- The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).
II.

COMPLIANCE
Preference for European standards

Question (Q6): "When considering implementing a technical standard in the field of privacy/data protection would your organisation prefer? Please rate from 1 (not preferred at all) to 5 (strongly preferred). If your answer is "don’t know", please leave the line blank."

National standards: 17% (1), 8% (2), 33% (3), 25% (4), 17% (5)

European standards: 55% (1), 45% (5)

International standards: 27% (1), 36% (2), 36% (3)

Source: Stakeholder survey
Note: N=12, 11, 11.
Figure 5.26
Question (Q8): "Which source(s) would your organisation rely on most as regards obtaining information that could improve your awareness about the availability and effects of technical standards in the field of privacy/data protection?"

- **Our own IT-department**: 30% (very relevant) 27% (relevant) 9% (neutral) 18% (not relevant) 9% (not at all relevant)
- **Our own data protection officer**: 45% (very relevant) 18% (relevant) 36% (neutral) 35% (not relevant) 8% (not at all relevant)
- **The European Union**: 8% (very relevant) 8% (relevant) 33% (neutral) 42% (not relevant) 8% (not at all relevant)
- **National governments**: 8% (very relevant) 38% (relevant) 38% (neutral) 10% (not relevant) 8% (not at all relevant)
- **Data protection authorities**: 27% (very relevant) 36% (relevant) 36% (neutral) 36% (not relevant) 8% (not at all relevant)
- **Consultancy firms**: 8% (very relevant) 33% (relevant) 33% (neutral) 17% (not relevant) 8% (not at all relevant)
- **Business magazines**: 45% (very relevant) 27% (relevant) 18% (neutral) 9% (not relevant) 9% (not at all relevant)
- **Internet websites**: 27% (very relevant) 9% (relevant) 36% (neutral) 18% (not relevant) 9% (not at all relevant)
- **Consultants**: 8% (very relevant) 33% (relevant) 26% (neutral) 26% (not relevant) 8% (not at all relevant)

Source: Stakeholder survey
Note: N=11, 11, 12, 13, 11, 11, 12, 11, 11, 12.
Figure 5.37
What are the most relevant factors when deciding whether to implement privacy/data protection related technical standards?
III.

STANDARDISATION
Privacy focused standards

Framework documents

Privacy management
- ISO/IEC 29190:2015 provides a "Privacy capability assessment model."

Technical implementation of privacy
- ISO/IEC 29101:2013 – Privacy architecture framework
Overview of standards with Privacy relevance in ISO/IEC JTC1/SC27/WG5
Security standards with privacy relevance

**Security evaluation standards**
- ISO/IEC 15408 Evaluation criteria for IT security
- ISO/IEC 18045 Methodology for IT security evaluation
- ISO/IEC 19608 Guidance for developing security and privacy functional requirements based on ISO/IEC 15408

**Implementation of security techniques**
- ISO/IEC 18033 Encryption algorithms
- ISO/IEC 18370 Blind digital signatures
- ISO/IEC 20008 Anonymous digital signatures
- ISO/IEC 20009 Anonymous entity authentication
- ISO/IEC 29191 Partially anonymous partially unlinkable authentication
- ISO/IEC 20889 Privacy enhancing data de-identification techniques
- ISO/IEC 27551 Attribute based unlinkable entity authentication
Conformity assessment standards

DRAFTING
- ISO/IEC 17000 – Vocabulary & general principles
- ISO/IEC 17007 Guidance for drafting normative documents suitable for use for conformity assessment

CAB
- ISO/IEC 17065
- ISO/IEC 17011 – General requirements for accreditation bodies accrediting CABs.
- ISO/IEC 17040 - General requirements for peer assessment of conformity assessment bodies and accreditation bodies
CONCLUSIONS
Thank you

Irene KAMARA

Email: i.kamara@tilburguniversity.edu

Website: https://www.tilburguniversity.edu/staff/i-kamara
APPENDIX
