Privacy & Identity Management Standards and the GDPR

Online Conference
The Future of Standards in Cybersecurity
September 2020

Jan Schallaböck, iRights.Law

1.

How do standards and GDPR relate?

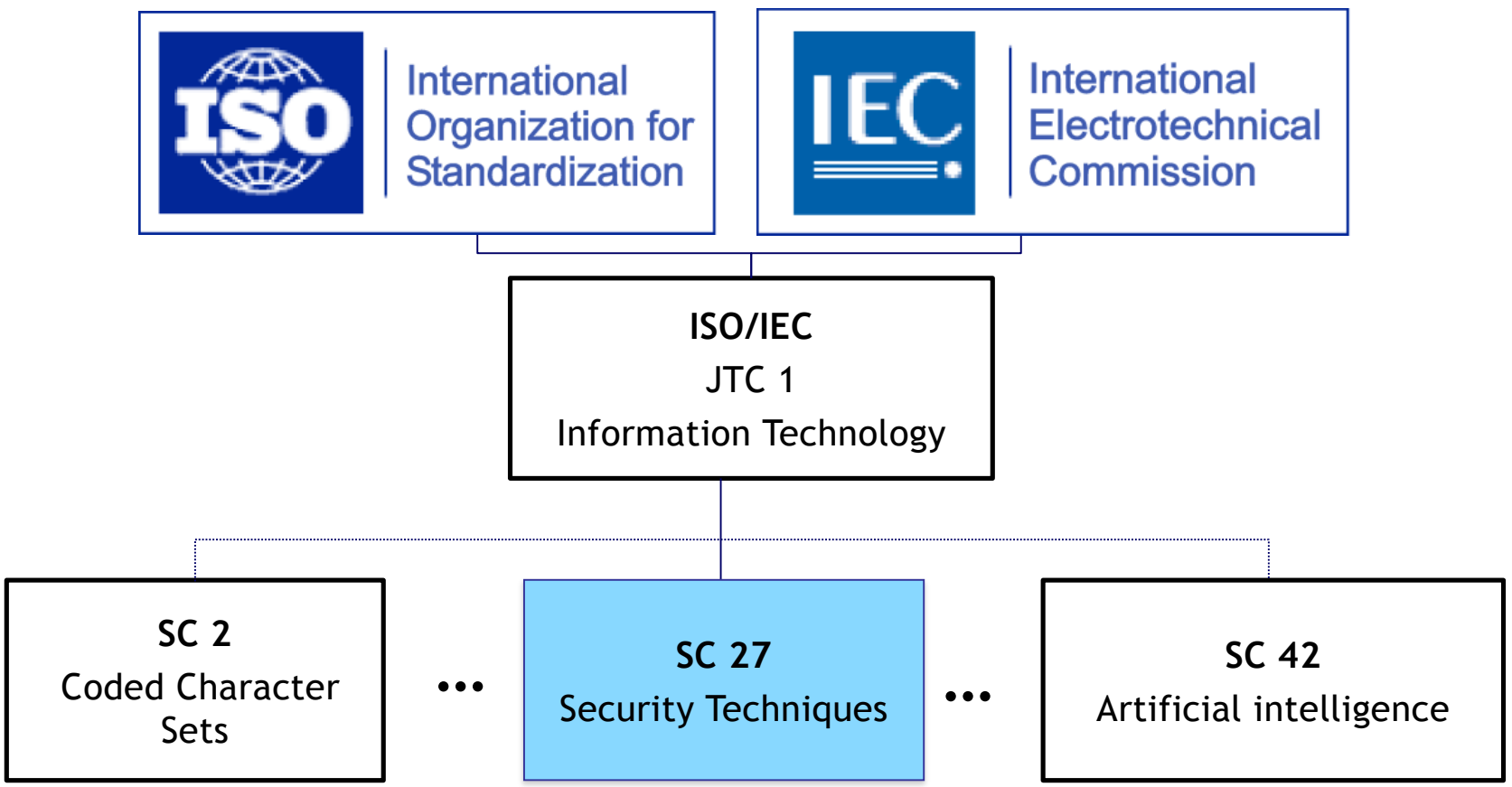
- Standards usually do not have a direct legal implication (in the context of the GDPR)

- They can be very helpful nevertheless…

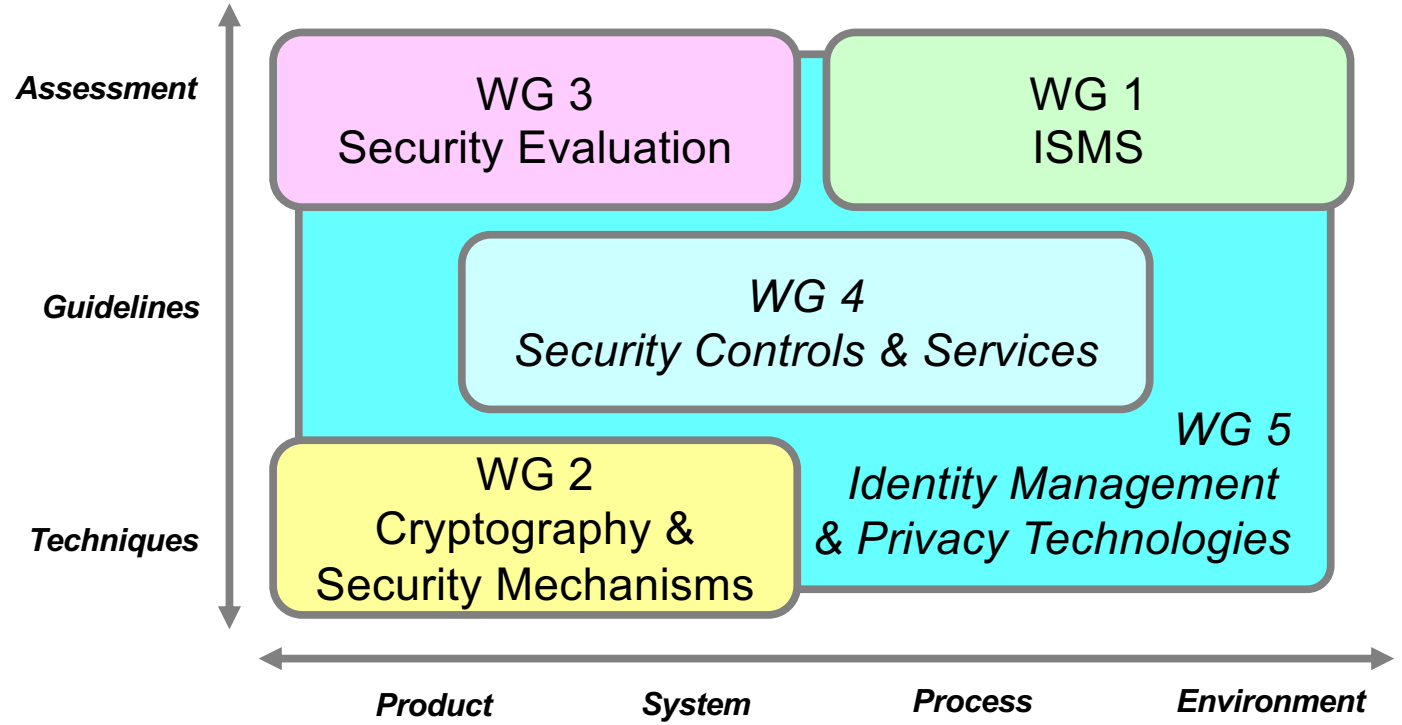
2.

ISO/IEC JTC 1/SC 27/WG 5

SC 27 “IT Security Techniques” within ISO/IEC JTC 1

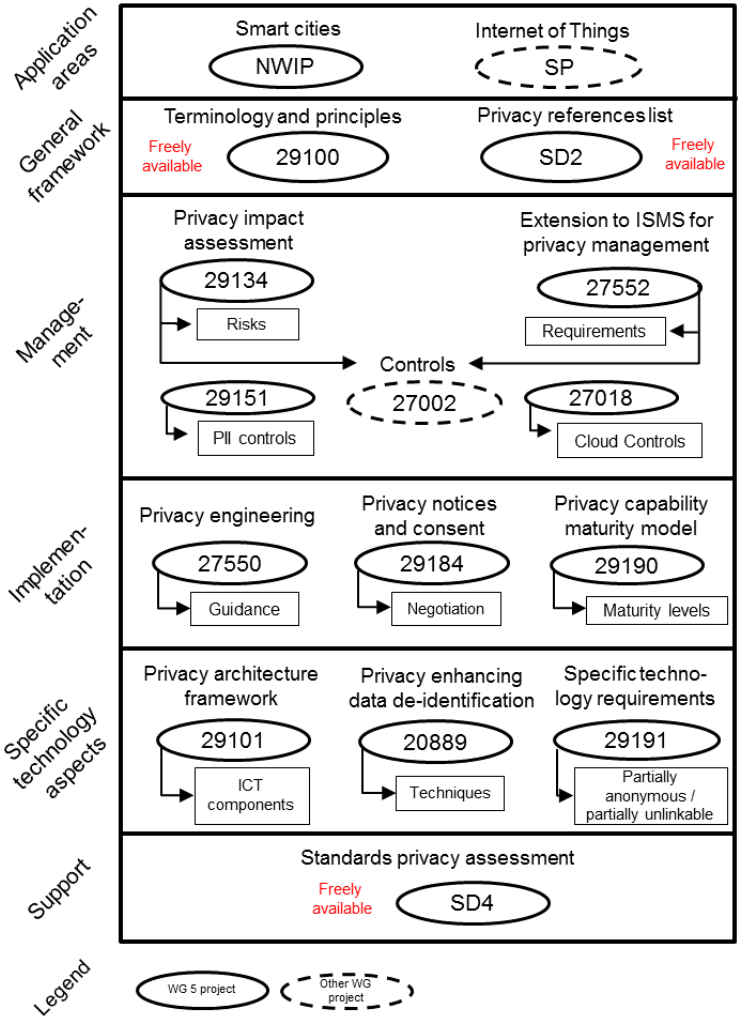


WGs in ISO/IEC JTC 1/SC 27 – IT Security Techniques

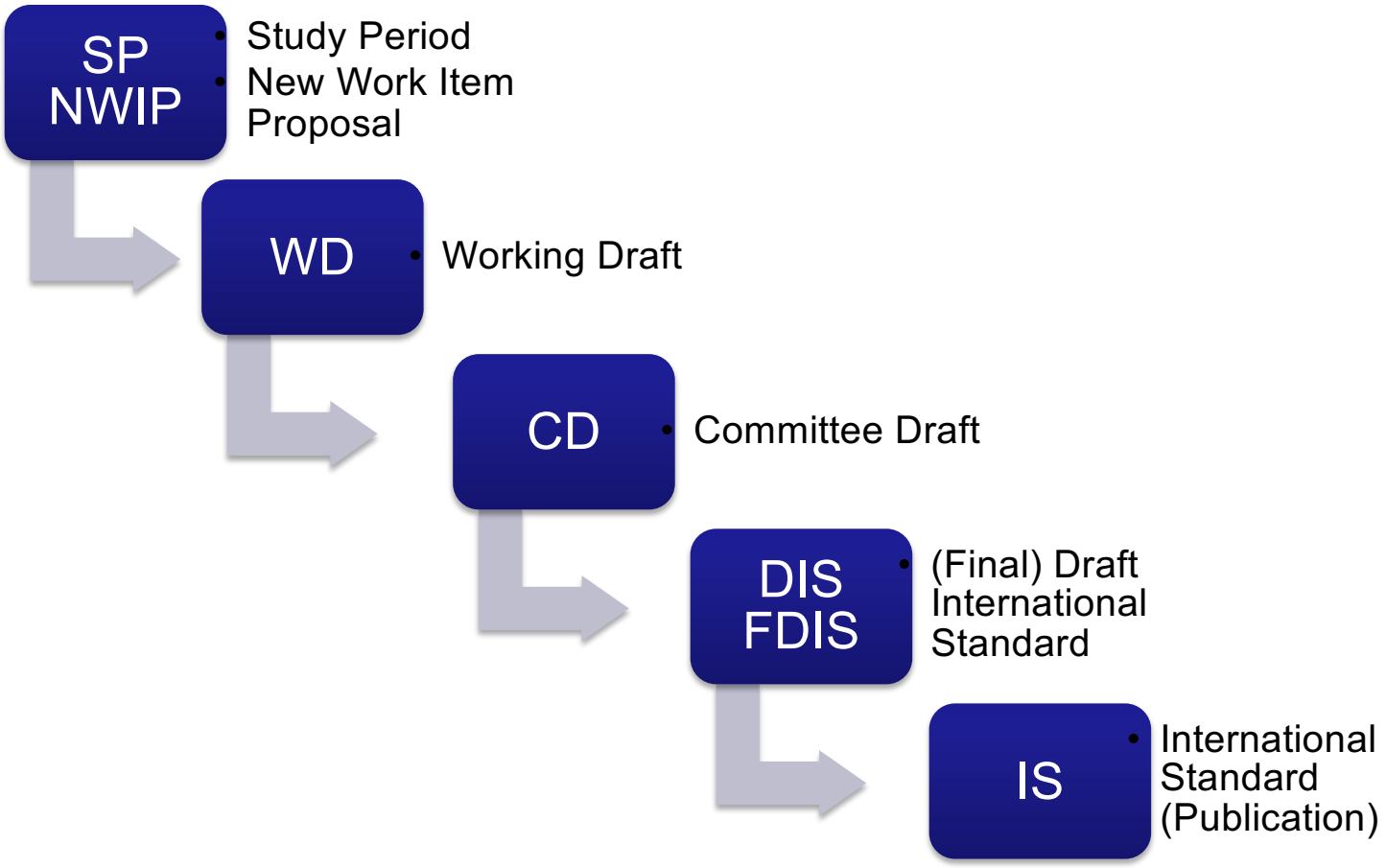


Privacy standards in SC 27/WG 5

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies



ISO development process



3.

Relevant Projects in WG 5

WG 5 in the context of the GDPR (preliminary assessment)

Art 4: Definition of personal data and pseudonymisation	**ISO/IEC CD 20889** **Privacy enhancing data de-identification techniques**
Art 5: Principles	**ISO/IEC 29100** **Privacy Principles**
Art 6 & 7: Consent Art. 13 & 14: Information	**ISO/IEC CD 29184** **Guidelines for online privacy notices and consent**
Art 15 & Art 20: Access and data portability	*Not yet available in ISO/IEC JTC 1/SC 27/WG 5*
Art 25: Privacy by design	**ISO/IEC WD 27550** **Privacy Engineering**
Art. 28: Processor	**ISO/IEC 27018** **Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors**
Art 33 & 34: Breach notification	Not available a in ISO/IEC JTC 1/SC 27/WG 5, but related to **ISO/IEC WD 27552 Enhancement to ISO/IEC 27001 for privacy management – Requirements**
Art. 35: DPIA	**ISO/IEC 29134** **Privacy Impact Assessment – Methodology**
Art 40: Codes of Conduct	*n/a, but* *standards bodies as fora for defining the latter?*
Art. 42 & 43: Certification	**ISO/IEC CD 27552** **Privacy-specific application of ISO/IEC 27001**

WG 5 in the context of the GDPR (preliminary assessment)

Art 4: Definition of personal data and pseudonymisation	ISO/IEC CD 20889 Privacy enhancing data de-identification techniques
Art 5: Principles	**ISO/IEC 29100** **Privacy Principles**
Art 6 & 7: Consent Art. 13 & 14: Information	**ISO/IEC CD 29184** **Guidelines for online privacy notices and consent**
Art 15 & Art 20: Access and data portability	*Not yet available in ISO/IEC JTC 1/SC 27/WG 5*
Art 25: Privacy by design	ISO/IEC WD 27550 Privacy Engineering
Art. 28: Processor	**ISO/IEC 27018** **Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors**
Art 33 & 34: Breach notification	Not available a in ISO/IEC JTC 1/SC 27/WG 5, but related to ISO/IEC WD 27552 Enhancement to ISO/IEC 27001 for privacy management – Requirements
Art. 35: DPIA	**ISO/IEC 29134** **Privacy Impact Assessment – Methodology**
Art 40: Codes of Conduct	*n/a, but* *standards bodies as fora for defining the latter?*
Art. 42 & 43: Certification	ISO/IEC CD 27552 Privacy-specific application of ISO/IEC 27001

ISO/IEC 29100 Privacy Principles

Overview

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

Related to

- Art 5 GDPR Principles

Status

- Published & freely available

ISO/IEC CD 29184 - Guidelines for online privacy notices and consent

Scope

This document is a specification for the content and the structure of online privacy notices as well as process of asking for consent to collect and process personally identifiable information (PII) from PII principals.

This document is applicable in any online context where a PII controller or any other entity processing PII informs PII principals of processing.

Related to

- Art 6 & 7 GDPR Consent
- Art. 13 & 14 GDPR Information

Status:

- published

ISO/IEC 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

- **Scope**

[...] establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

[...] specifies guidelines based on ISO/IEC 27002, [...] within the context of the information security risk environment(s) of a provider of public cloud services.

[...] applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which provide information processing services as PII processors via cloud computing under contract to other organizations.[...]

- **Related to:**
  - Art. 28 GDPR Processor

- **Status**
  - published

ISO/IEC 29134
Privacy Impact Assessment – Methodology

Scope

This document gives guidelines for

— a process on privacy impact assessments, and

— a structure and content of a PIA report.

It is applicable to all types and sizes of organizations, including public companies, private companies, government entities and not-for-profit organizations.

This document is relevant to those involved in designing or implementing projects, including the parties operating data processing systems and services that process PII.

Related to

- Art. 35 GDPR DPIA

Status

- published

There is more within WG 5 and elsewhere...

- Study Period on the Potential internationalisation of

  DIN 66398 "Guideline for development of a concept for data deletion with derivation of deletion periods for personal identifiable information"

- ISO/IEC 27552
- Work on data portability in SC 38

Thank you for your attention