www.privacyromania.ro

January 29-30, 2021

PRIVACY ROMANIA 2021

Romanian National Conference on Privacy and Data Protection

ACHIEVING GDPR COMPLIANCE THROUGH ISO STANDARDS

ASCPD

Asociația Specialiștilor în Confidențialitate și Protecția Datelor

Mihai DANȚIȘ

Cybersecurity Division Manager TUV Austria România

ACHIEVING GDPR COMPLIANCE THROUGH ISO STANDARDS

Mihai DANȚIȘ,
Cyber Security Division manager, TUV Austria Romania

OUTLINE

1. **ISO’s related to EU General Data Protection Regulation (GDPR)**
2. **The GDPR view of the ISO/IEC 27701**
3. **Applying the ISO27701 approach to GDPR**
4. **Q/A**

ISO’s related to EU General Data Protection Regulation (GDPR)

- ✓ **ISO 27001**:2013 – Information security management systems – **Requirements**
- ✓ **ISO 27018**:2019 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ✓ **ISO 27701**:2019 – Extension to ISO 27001 and ISO 27002 for privacy information management – **Requirements** and guidelines
- ✓ **ISO 29100**:2011/ AMD 1:2018 Privacy framework –and principles
- ✓ **ISO 29151**:2017 – Code of practice for personally identifiable information protection

To have in mind:

- Best practices ≠ regulations
- Privacy ≠ Data Protection
- Data protection ≠ Information Security
- ISO: Requirements (ref. audit) vs. guidelines

Why ISO 27701?

Scope:

- “specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO 27001 and ISO 27002 for privacy management”;
- “specifies PIMS-related requirements and provides guidance for PII controllers and PII processors…”;
- “applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations”.

Source: ISO/IEC 27701:2019

The GDPR view of the ISO/IEC 27701

Annex D: Mapping of the controls of ISO 27701 to the GDPR

Airplane view

As initially established:

- ISO 27001 is the baseline
- With ISO 27701 on top (extra measures)
- With focus on "privacy when processing PII"

GDPR requirements/ compliance is ...

- Ref. Annex D:
- By replacing word "privacy" with "data protection"
- Extend the ISO27001 mindset to GDPR mindset
- Extended stakeholders/interested parties/external parties
- Extended requirements

The GDPR mapping in ISO27701

Annex D – Mapping to the General Data Protection Regulation

Table D.1 – Mapping of ISO/IEC 27701 structure to GDPR articles

Subcase of this document	GDPR article
5.2.1	(24)(3), (25)(3), (28)(5), (28)(6), (28)(10), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)
5.2.2	(31), (35)(9), (36)(1), (36)(2), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
5.2.3	(32)(2)
5.2.4	(32)(2)
5.4.1.2	(32)(1)(b), (32)(2)
5.4.1.3	(32)(1)(b), (32)(2)
6.2.1.1	(24)(2)
6.3.1.1	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)
6.3.2.1	(5)(1)(f)
6.4.2.2	(39)(1)(b)
6.5.2.1	(5)(1)(f), (32)(2)

How to implement

Enterprise first

- ISO 27001 first + extension to personal data (GDPR)

GDPR only

- Scoping ISO27001 to GDPR only (with help from ISO27701)

GDPR - requirements facing first

Keep in mind:
implementation is **process** based, it's an ISMS/PIMS, you **cannot** protect GDPR **data only**

Applying the ISO27701 approach to GDPR

5.1. General

“The requirements of ISO/IEC 27001:2013 mentioning "information security" shall be extended to the protection of privacy as potentially affected by the processing of PII.”

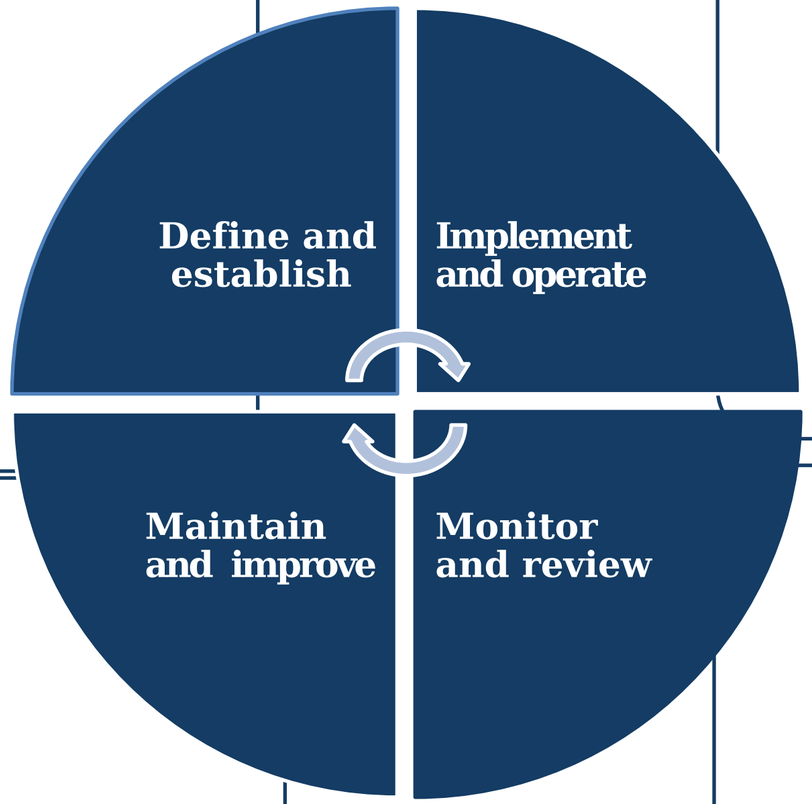
NOTE In practice, where "information security" is used in ISO/IEC 27001:2013, "information security and privacy” applies instead (see Annex F).“

*GDPR : refers only to "**data protection**“, but doesn't mention "privacy",*

When applying GDPR: apply the same principle, extend "information security" to "information security and (personal) data protection"

PIMS/GDPR implementation

- 1.1 Initiation of the PIMS implementation
  1.2 Analysis of the ISMS scope and Statement of Applicability
  1.3 PIMS scope
  1.4 Management approval
  1.5 Privacy policy
  1.6 Privacy risk assessment
  1.7 Privacy impact assessment
  1.8 PIMS Statements of Applicability



- 2.1 Documentation management
  2.2 Selection of controls
  2.3 Implementation of controls
  2.4 Awareness, training, and communication

- 4.1 Treatment of nonconformities
  4.2 Continual improvement

- 3.1 Monitoring, measurement, analysis, evaluation, and Management review
  3.2 Internal audit

Attention to:

- Terminology
  - no "privacy" but info security and data protection)
- EVERYONE on board
  - Internal (employees, interims, and … contractors)
  - External (customers, prospects, visitors,… subjects)
- Policies
- Communication requirements as:
  - Information notice
  - Responding to subjects
- Crisis management & Incident Management C
- Continuous improvement
  - ISO27001 : PDCA
  - GDPR: “state of the art” protection, “shall implement appropriate technical and organizational measures”

Attention to:

- GDPR & ISO27701 is a multidepartment job for:
  - Business
  - Legal
  - IT
  - HR, Security, ….
  - External parties
- Required expertise for ALL these areas

- Mind Murphy’s law
  - What can go wrong, will go wrong
  - In cyber & GDPR: it's not "IF", but "when",…
  - you only need 1 mouse click for disaster

The mission is:

- Protect the subject and his/her data
- Protect your company data as subject data
- Get in control (especially working with vendors)
- Stay in control, even when something goes wrong
- Keep up to speed, everything is moving (even law)
- Keep improving

Companies will be judged not because they were hacked, but how prepared they were and how they handled and communicated about the breach...".

(Jan De Bondt)

The ISO auditor mindset

A different point of view

Why is this important?

- If you know how the audit works, you know better what to implement
- Both In the right spirit
  - Results based,
  - not check list based

- Growth mindset
  - Not perfect at first step but perfectible
  - Better done than perfect (at firs iteration)
  - Think big, act small… (step by step)

The auditor view helps to…

- The audit cycle pushes the implementation of PDCA
  - Continuous improvement
  - Step by step
- Have an independent / external view
- Keep good relation between
  - Business
  - IT
  - DPO
  - Legal
  - Security

ISO27001 vs security & data protection

Typical feedback related to ISO 2700:

- "Old" framework
- "too general"
- "Not fit" for current evolutions

Major advantages:

- General
- Best practice
- Flexible, pluggable
- Universal & uniform
- Extremely Compatible with other frameworks and standards like:

ISO 22301 – Business Continuity;
ISO 27035 – Incident Management;
ISO 20000 – IT Service Management; etc.

Why is this important?

ISO27001

- International,
- Standardized
- Mutual recognition

GDPR

- EU Regulation, BUT…
- Certification controlled by
- National DPA
- Accreditation bodies

THANK YOU!

✉ mihai@dantis.ro