

Dealing with ISO/IEC 27701 and the GDPR

Square Table, ISACA Netherlands Chapter

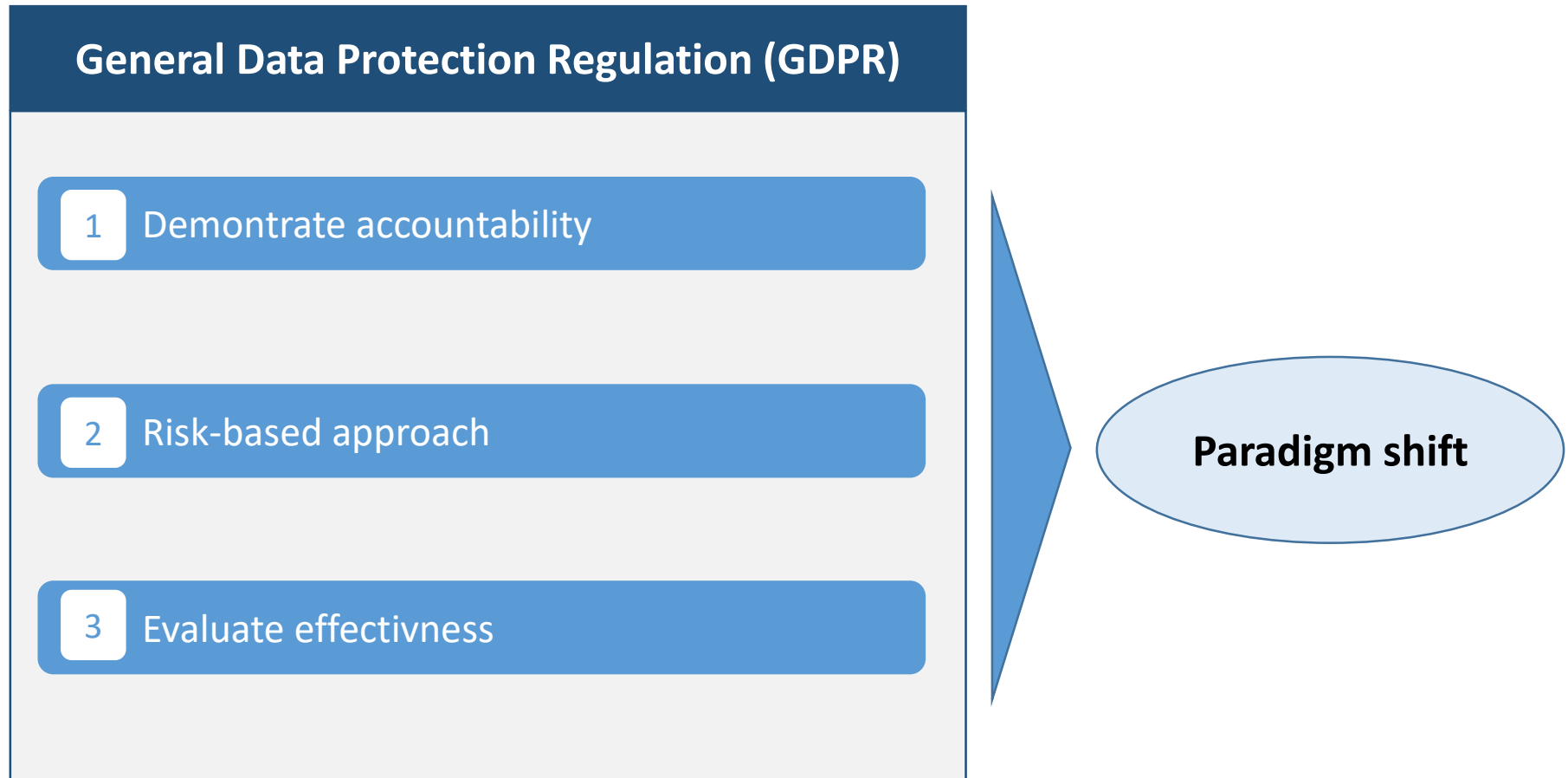
25 November 2020,
Markus Gierschmann

Agenda

- **GDPR as a game changer**

- International PIMS standard: ISO/IEC 27701
- ISO certification versus GDPR certification
- Outlook: Refinement of ISO 27701 in European Context

Game changer



Accountability = Shifting the burden of proof?

Product liability
in the production



Concept of quality
= perceptible form of state

Process orientation
for repetitive quality assurance
→ PDCA

Quality management system
QMS according to ISO 9001

Accountability
in data protection



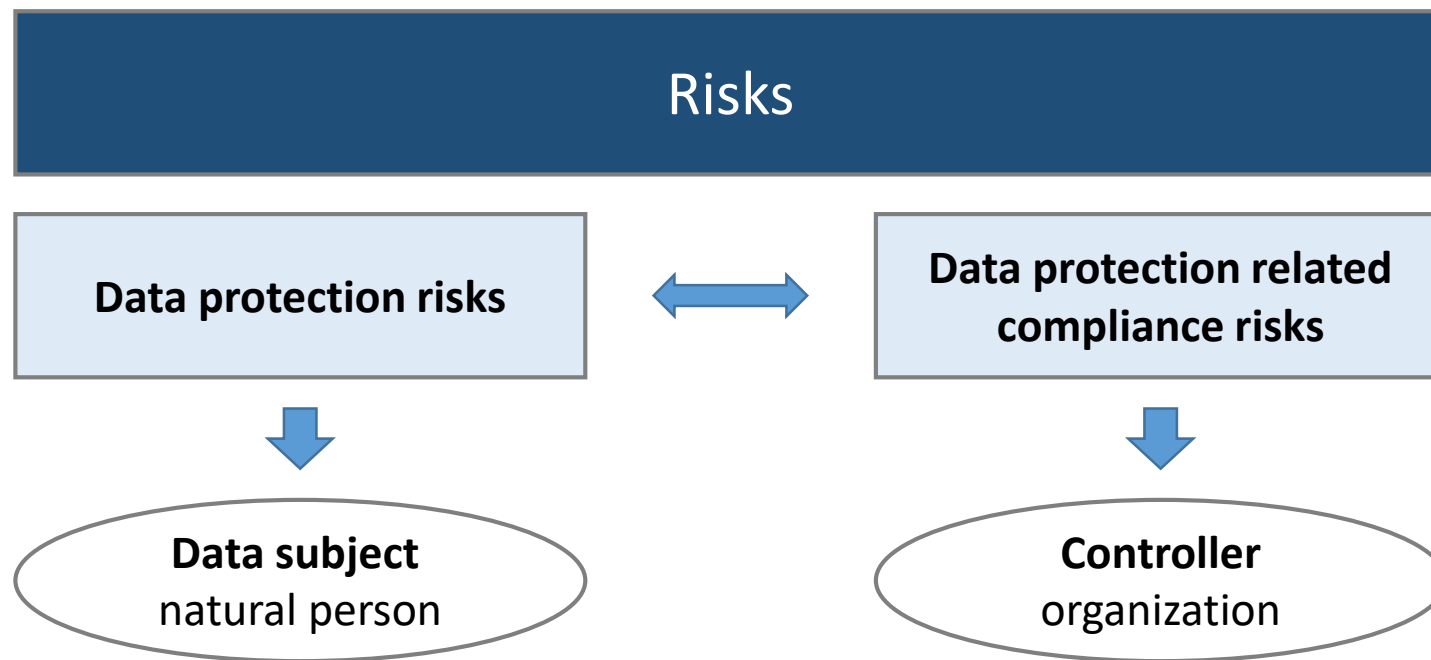
Be able to provide evidence
How responsibility is verifiably
perceived

„Compliance-Programs“

Regulated certificates
as reliable evidence
→ Harmonisation of the „standards“

Art. 29-Gruppe, WP 173, 2010


Risks for organization and natural person

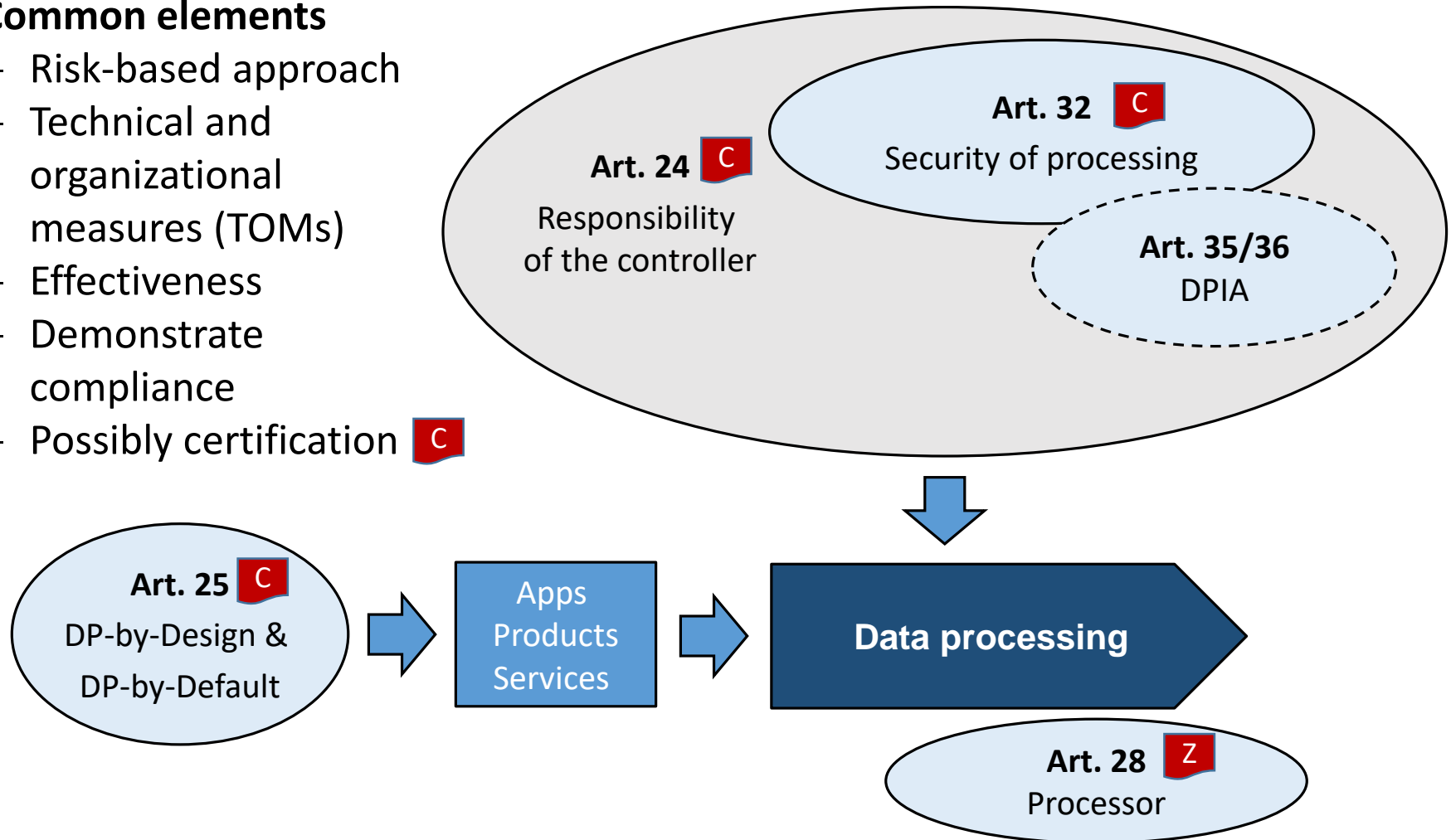


GDPR only considers only risks for the rights and freedoms of natural persons (data subjects); non conformance with regulations/obligations is a compliance risk for controllers.

Risk-based approach

Common elements

- Risk-based approach
- Technical and organizational measures (TOMs)
- Effectiveness
- Demonstrate compliance
- Possibly certification 



„A Privacy Management Program is a must to demonstrate accountability.“

Andrea Jelinek, Vorsitzende EDSA
ICDPPC 2019, Tirana, Albanien

Agenda

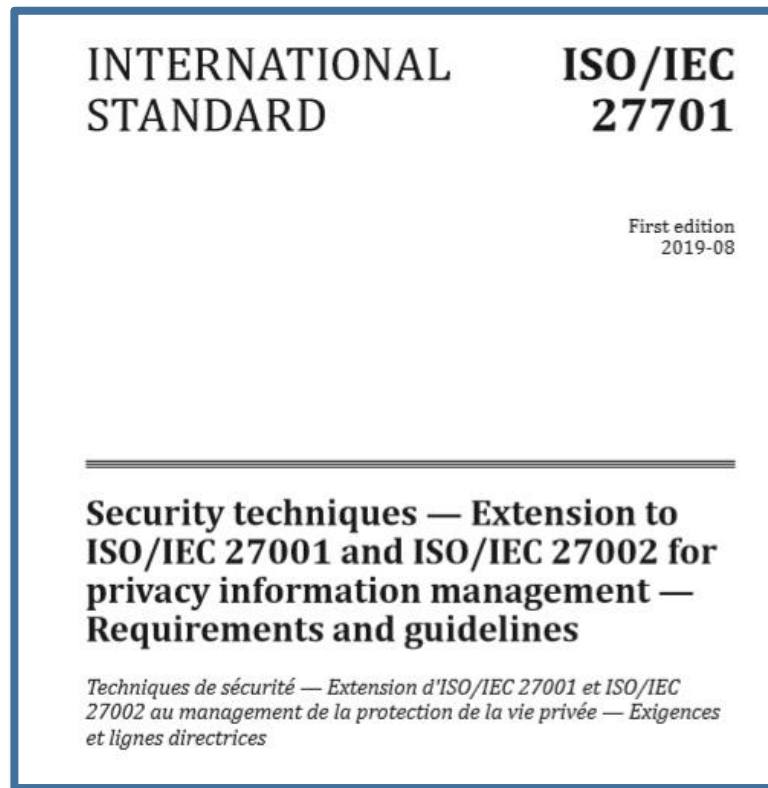
- GDPR as a game changer

- **International PIMS standard: ISO/IEC 27701**

- ISO certification versus GDPR certification

- Outlook: Refinement of ISO 27701 in European Context

Privacy Information Management System (PIMS)



Privacy Information Management System (PIMS)

ISMS required

No GDPR
compliance

No certification
according to
Art. 42 GDPR

INTERNATIONAL
STANDARD

ISO/IEC
27701

First edition
2019-08

**Security techniques — Extension to
ISO/IEC 27001 and ISO/IEC 27002 for
privacy information management —
Requirements and guidelines**

*Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC
27002 au management de la protection de la vie privée — Exigences
et lignes directrices*

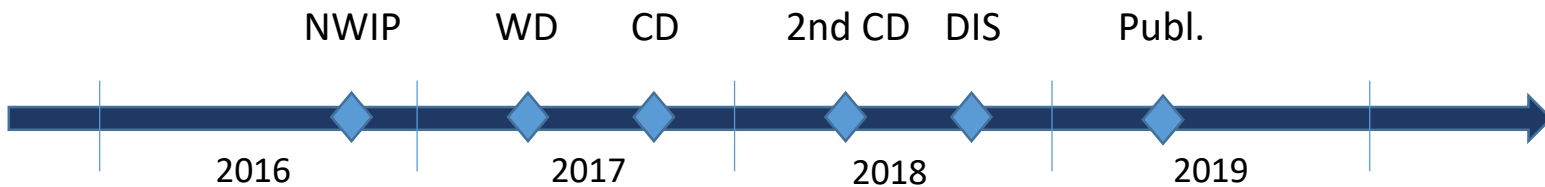
Structured
approach

Integrated
management
system

Global
application

Background and development

- **ISO/IEC meetings and development of ISO-Standard**
 - **JTC 1/SC 27** *Information security, cybersecurity and privacy protection*
 - **WG 5** *Identity Management & Privacy Technologies*



- **ISO/IEC 27701**, *Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*
 - Privacy Information Management System (PIMS) as an extension of an information management system (ISMS)
 - Information security → Information security and privacy

Key design elements

Extension of an ISMS

PIMS is an information security management system (ISMS) which addresses the protection of privacy as potentially affected by the processing of PII

PIMS-specific requirements and guidance

Establishing, implementing, maintaining and continually improving a PIMS in the form of an **extension to ISO/IEC 27001 and ISO/IEC 27002** for privacy management within the context of the organization

Extended interpretation of information security

Where "information security" is used in ISO/IEC 27001 or 27002, "**information security and privacy**" applies instead

Key design elements

Extension of an ISMS

5.2.3 Determining the scope of the information security management system

A requirement additional to ISO/IEC 27001:2013, 4.3 is:

When determining the scope of the PIMS, the organization shall include the processing of PII.

NOTE The determination of the scope of the PIMS can require revising the scope of the information security management system, because of the extended interpretation of "information security" according to 5.1.

potentially affected by the processing of PII

PIMS-specific requirements and guidance

Establishing, implementing, maintaining and continually improving a PIMS in the form of an **extension to ISO/IEC 27001 and ISO/IEC 27002** for privacy management within the context of the organization

Extended interpretation of information security

Where "information security" is used in ISO/IEC 27001 or 27002, "**information security and privacy**" applies instead

Key design elements

Extension of an ISMS

PIMS is an information security management system (ISMS) which addresses the protection of privacy as

5 PIMS-specific requirements related to ISO/IEC 27001

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 E](#)).

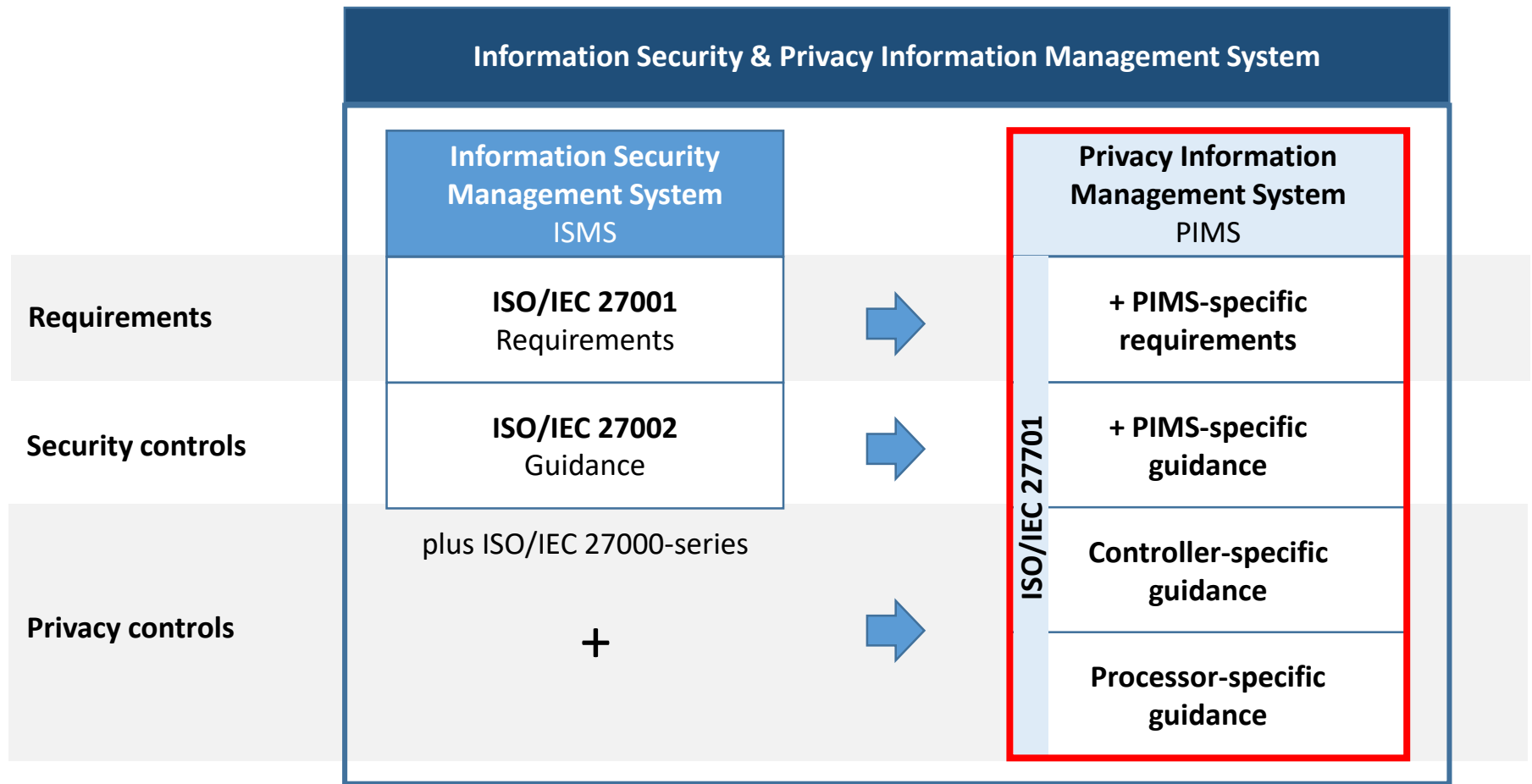
PIMS-specific requirements guidance

the context of the organization


Extended interpretation of information security

Where "information security" is used in ISO/IEC 27001 or 27002, "**information security and privacy**" applies instead

Structure



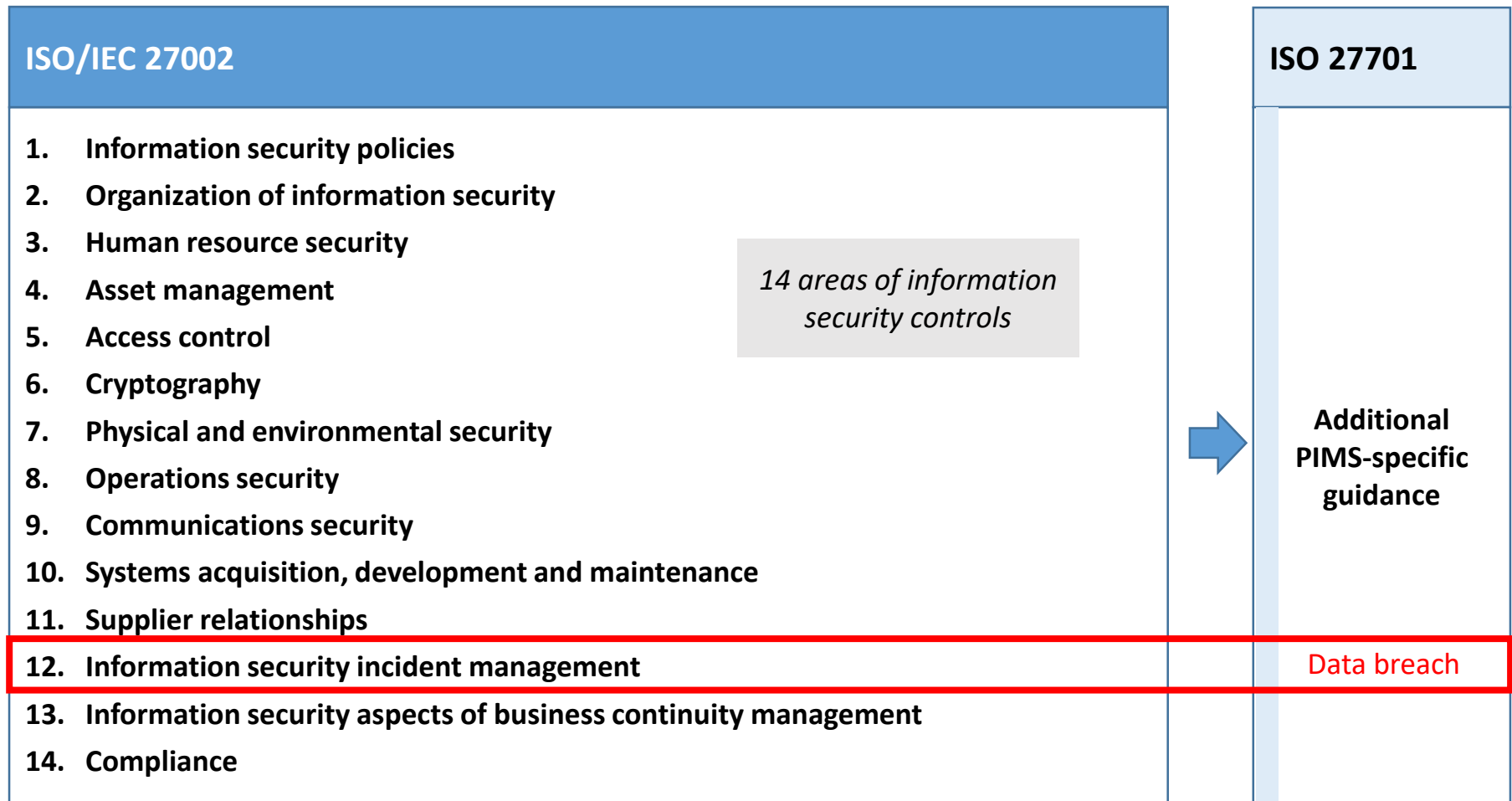
PIMS-specific extension of ISO/IEC 27001

| ISO/IEC 27001 | Content | | ISO 27701 |
|---------------------------------------|--|---|--|
| 1. Context of the organization | 1) Organization and its context, 2) Needs and expectations of interested parties, 3) Scope of the ISMS, 4) ISMS | | |
| 2. Leadership | 1) Leadership and commitment, 2) Policy, 3) Organizational roles, responsibilities and authorities | | |
| 3. Planning | 1) Actions to address risks and opportunities, 2) Information security objectives and planning to achieve them | | |
| 4. Support | 1) Resources, 2) Competence, 3) Awareness, 4) Communication, 5) Documented information |  | Additional PIMS-specific requirements |
| 5. Operation | 1) Operational planning and control, 2) Information security risk assessment, 3) Information security risk treatment | | Privacy risk management |
| 6. Performance evaluation | 1) Monitoring, measurement, analysis and evaluation, 2) Internal audit, 3) Management review | | |
| 7. Improvement | 1) Nonconformity and corrective action, 2) Continual improvement | | |

PIMS-specific extension of ISO/IEC 27001

| ISO/IEC 27001 | Content | ISO 27701 |
|--------------------------------|---|---|
| 1. Context of the organization | 1) Organization and its context, 2) Needs and expectations of | |
| 2. Leadership | <p>5.4.1.2 Information security risk assessment</p> <p>The requirements stated in ISO/IEC 27001:2013, 6.1.2 apply with the following refinements:</p> <p>ISO/IEC 27001:2013, 6.1.2 c) 1) is refined as follows:</p> <p>The organization shall apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability, within the scope of the PIMS.</p> <p>The organization shall apply privacy risk assessment process to identify risks related to the processing of PII, within the scope of the PIMS.</p> | <p>Additional PIMS-specific requirements</p> <p>Privacy risk management</p> |
| 3. Planning | The organization shall ensure throughout the risk assessment processes that the relationship between information security and PII protection is appropriately managed. | |
| 4. Support | NOTE The organization can either apply an integrated information security and privacy risk assessment process or two separate ones for information security and the risks related to the processing of PII. | |
| 5. Operation | ISO/IEC 27001:2013, 6.1.2 d) 1) is refined as follows: | |
| 6. Performance evaluation | The organization shall assess the potential consequences for both the organization and PII principals that would result if the risks identified in ISO/IEC 27001:2013, 6.1.2 c) as refined above, were to materialize. | |
| 7. Improvement | 1) Nonconformity and corrective action, 2) Continual improvement | |

PIMS-specific extension of ISO/IEC 27002



PIMS-specific extension of ISO/IEC 27002

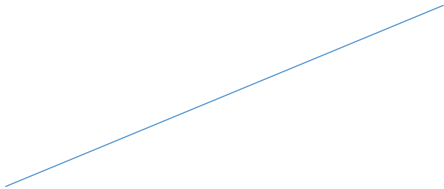
| ISO/IEC 27002 | ISO 27701 |
|---|--|
| <ol style="list-style-type: none"> 1. Information security 2. Organizational measures 3. Human resources 4. Asset management 5. Access control 6. Cryptography 7. Physical and environmental security 8. Operations and maintenance 9. Communications 10. Systems and services 11. Supplier relationships 12. Information security incident management 13. Information security policy 14. Compliance | <p>6.13.1.5 Response to information security incidents</p> <p>The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 16.1.5 and the following additional guidance applies:</p> <p>Additional implementation guidance for 16.1.5, Response to information security incidents, of ISO/IEC 27002:2013 is:</p> <p>Implementation guidance for PII controllers</p> <p>An incident that involves PII should trigger a review by the organization, as part of its information security incident management process, to determine if a breach involving PII that requires a response has taken place.</p> <p>An event does not necessarily trigger such a review.</p> <p>NOTE 1 An information security event does not necessarily result in actual, or the significant probability of, unauthorized access to PII or to any of the organization's equipment or facilities storing PII. These can include, but are not limited to, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks and packet sniffing.</p> <p>When a breach of PII has occurred, response procedures should include relevant notifications and records.</p> <p>Some jurisdictions define cases when the breach should be notified to the supervisory authority, and when it should be notified to PII principals.</p> <p>Notifications should be clear and can be required.</p> |

Additional
specific
ance

breach

Controller- and processor-specific guidance

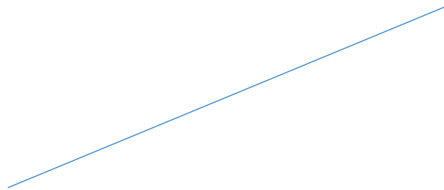
ISO/IEC 27002



Additional ISO/IEC 27002 guidance for PII controller

1. Conditions for collection and processing
2. Obligations to PII principals **Data subject rights**
3. Privacy by design and by default
4. PII sharing, transfer, and disclosure

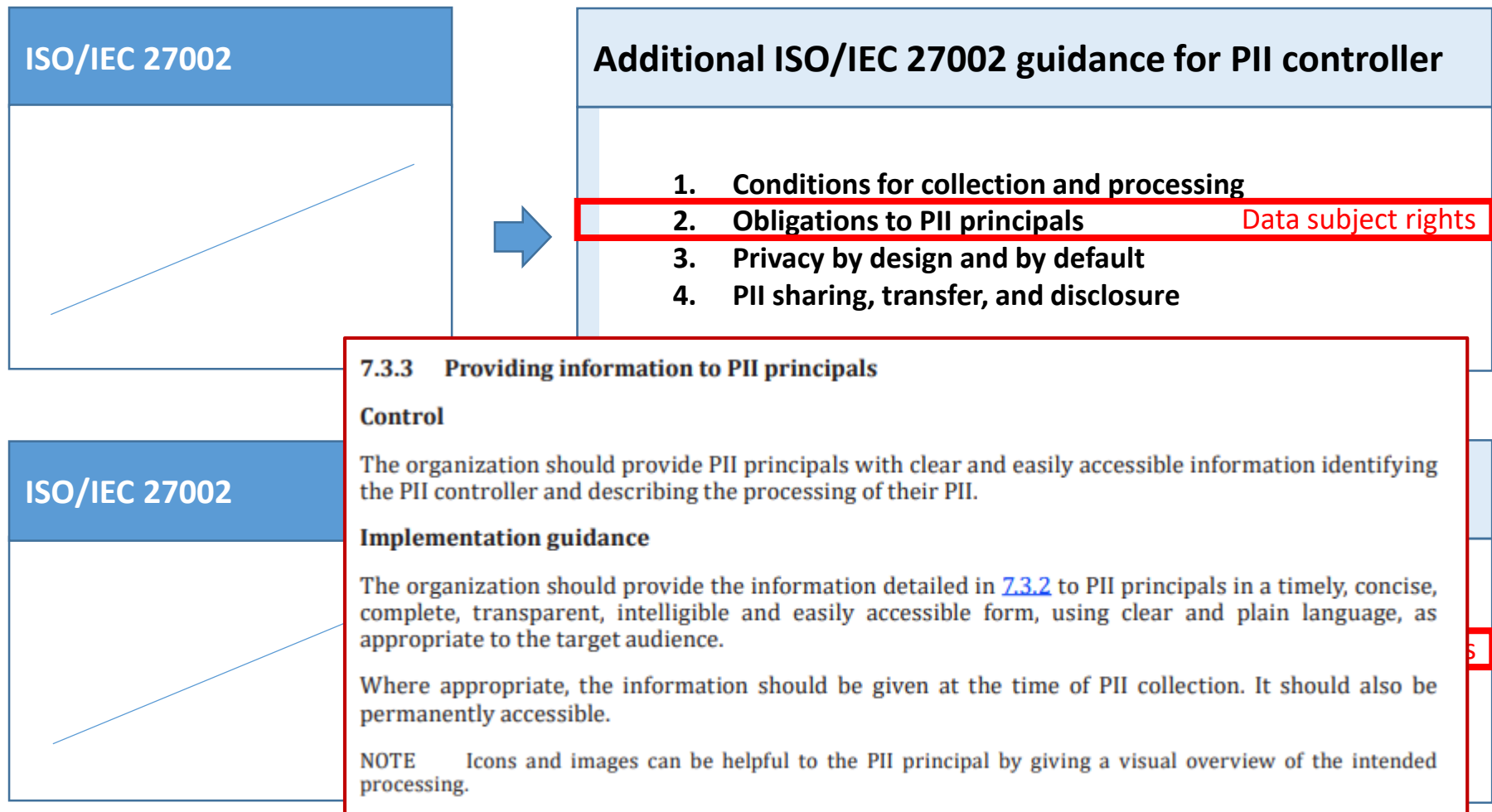
ISO/IEC 27002



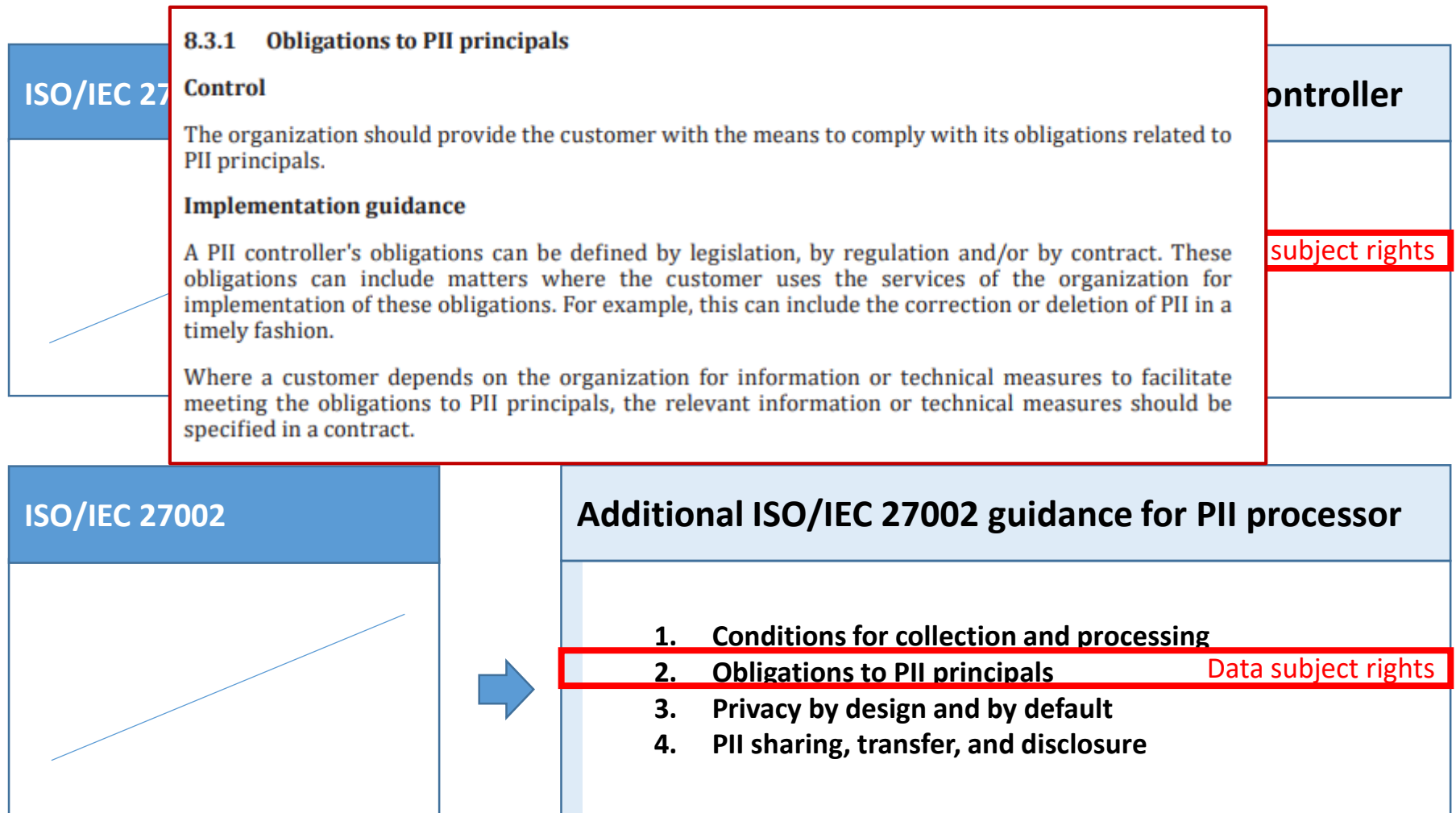
Additional ISO/IEC 27002 guidance for PII processor

1. Conditions for collection and processing
2. Obligations to PII principals **Data subject rights**
3. Privacy by design and by default
4. PII sharing, transfer, and disclosure

Controller- and processor-specific guidance



Controller- and processor-specific guidance

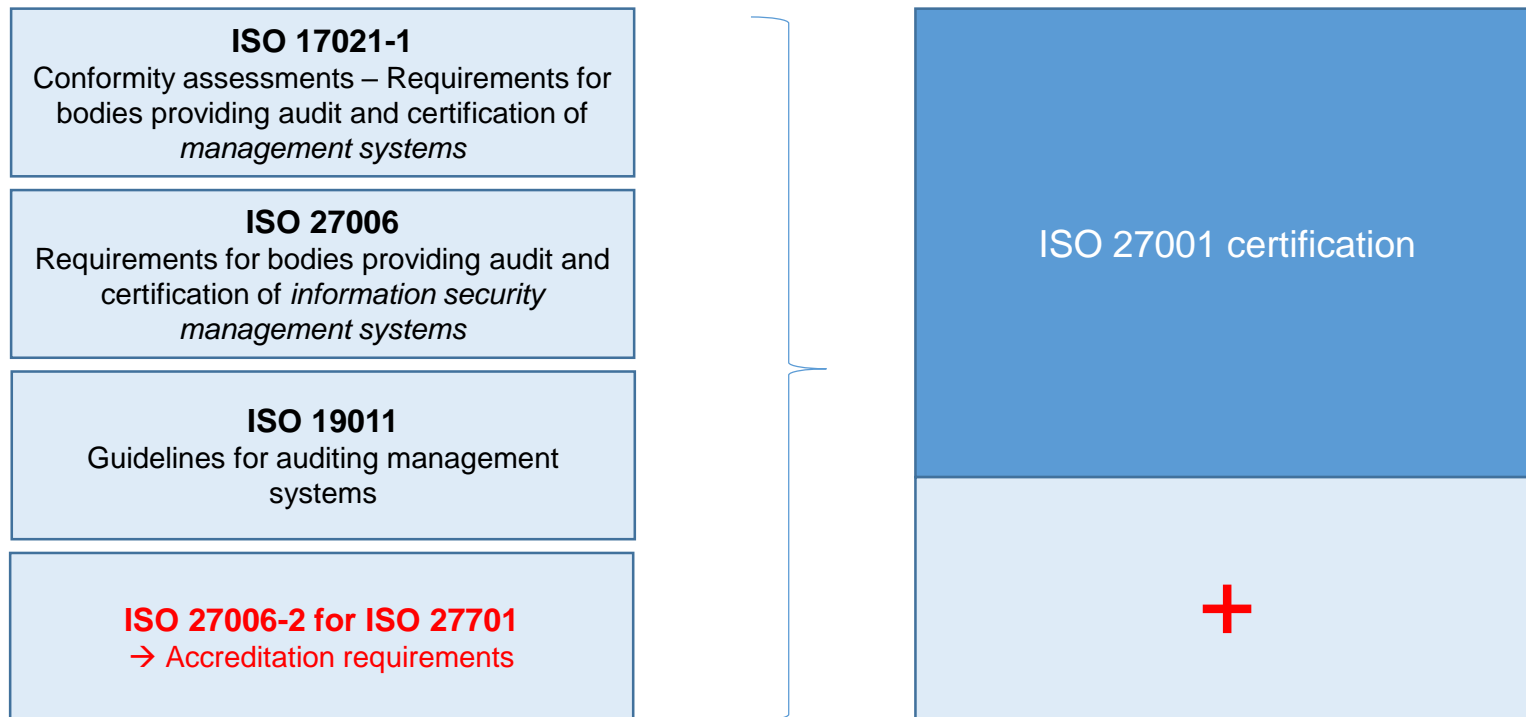


Agenda

- GDPR as a game changer
- International PIMS standard: ISO/IEC 27701
- **ISO certification versus GDPR certification**
- Outlook: Refinement of ISO 27701 in European Context

ISO 27701 certification and accreditation

ISO 27701 certification requires ISO 27001 certification



Certification doesn't equal certification!

ISO 27001+
certification

≠

Certification
according to
Art. 42 GDPR

Conformity assessment

Requirements for certification bodies

INTERNATIONAL
STANDARD

**ISO/IEC
17021-1**

First edition
2015-06-15

**Certification of management
systems**

**Conformity assessment —
Requirements for bodies
providing audit and certification of
management systems —**

**Part 1:
Requirements**

INTERNATIONAL
STANDARD

**ISO/IEC
17065**

First edition
2012-09-15

**Certification of products,
processes and services**

**Conformity assessment — Requirements
for bodies certifying products, processes
and services**

INTERNATIONAL
STANDARD

**ISO/IEC
17024**

First edition
2012-07-03

Certification of persons

**Conformity assessment - General
requirements for bodies operating
certification of persons**

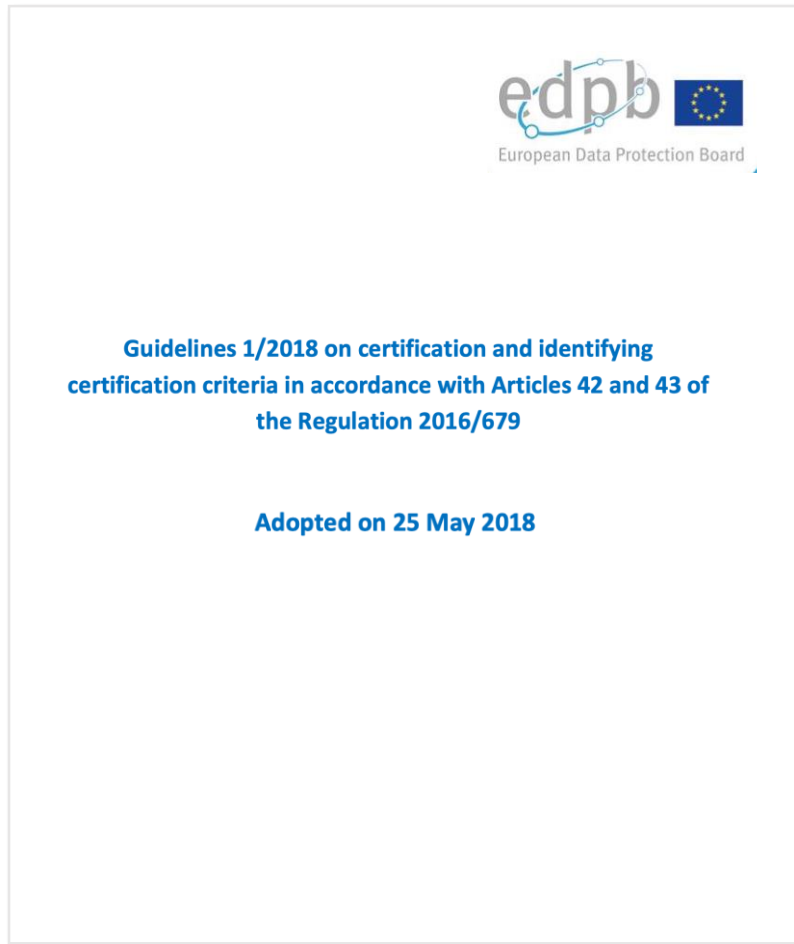
Certification bodies, Art. 43 (1) GDPR

Certification bodies

- issue and renew certification;
- are **accredited by** one or both of the following:
 - a) the competent **supervisory authority** or
 - b) the **national accreditation body** named in accordance with
 - Regulation (EC) No. 765/2008,
 - **EN-ISO/IEC 17065/2012** and
 - the **additional requirements** established by the competent supervisory authority.

The naming of the accreditation body shall be in accordance with ISO 17065!

EDPB Guidelines 1/2018



Definition of certification:

Third party conformity assessment (ISO)
or

*“Certification shall refer to **third party attestation related to processing operations by controllers and processors.**”*

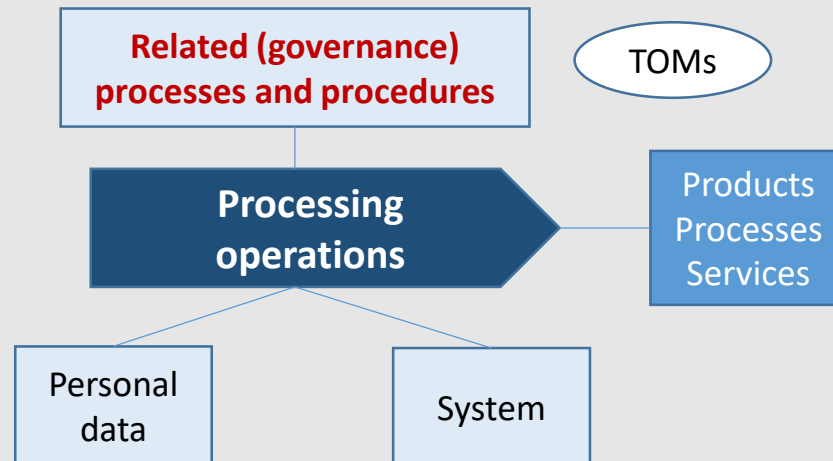
Usage of certification mechanisms:

*“... an **element to demonstrate compliance** with specific obligations of the controllers and processors.”*

What can be certified under GDPR?

The EDPB considers that the GDPR provides a broad scope for what can be certified under the GDPR, as long as the focus is on helping demonstrate compliance with this Regulation of processing operations by controllers and processors (Article 42.1).

Processing operations and core components:



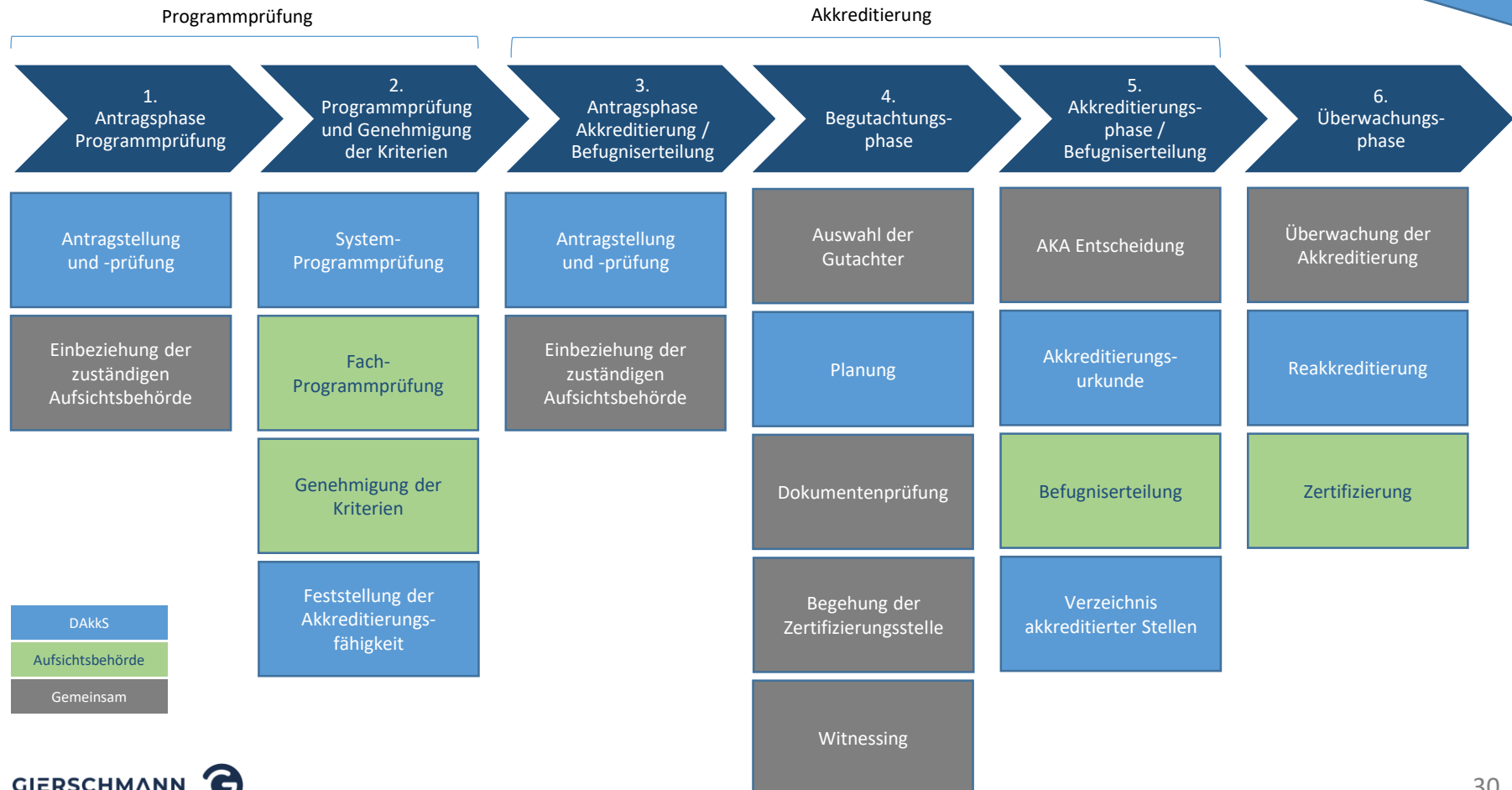
Influencing factors:

1. Organisational / legal structure
2. Who performs the processing
3. IT infrastructure

..., the EDPB considers that the scope of certification under the GDPR is directed to processing operations or set of operations. These may comprise of governance processes in the sense of organisational measures, hence as integral part of a processing operation (e.g. the governance process established for complaints' handling as part of the processing of employee data for the purpose of salary payment).

German accreditation process according to Art. 42, 43 GDPR (Illustrative)

DSK Version 1.0
(15.03.19)

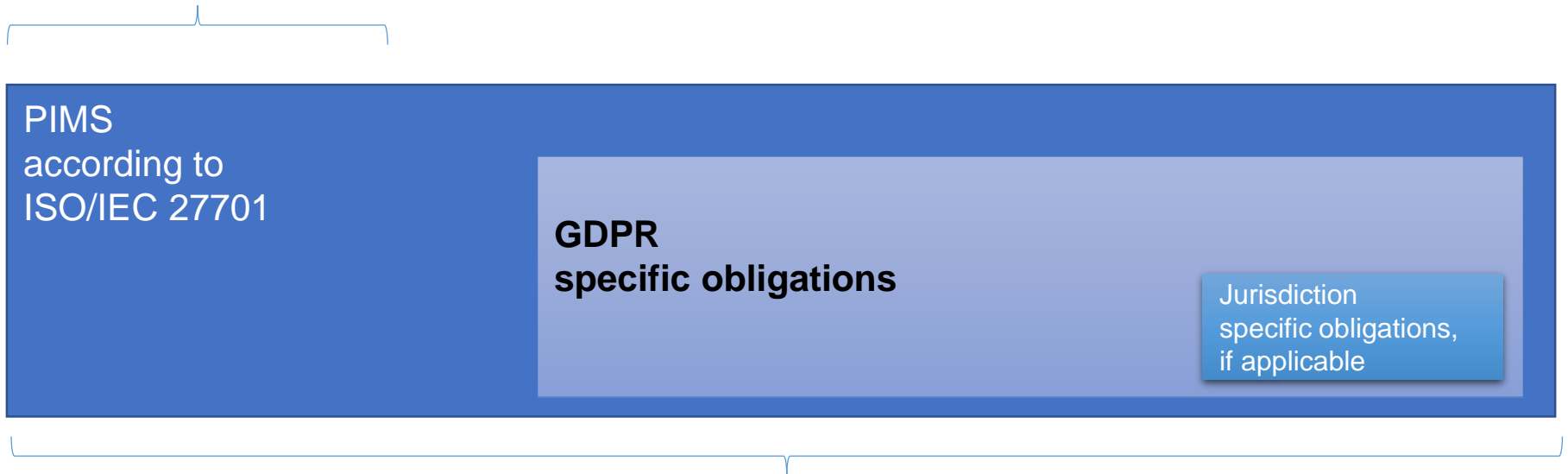


Agenda

- GDPR as a game changer
- International PIMS standard: ISO/IEC 27701
- ISO certification versus GDPR certification
- **Outlook: Refinement of ISO 27701 in European Context**

PIMS according to ISO/IEC 27701: An international framework

Generic requirements, which are designed to encompass GDPR requirements, but do not always detail them explicitly → must be further refined in GDPR context



PIMS can be used as a **framework**
in which requirements and obligations of GDPR and
respective jurisdictions can be implemented

Data Protection Mapping Project

| ISO/IEC 27701 | GDPR | Australia | Canada | Hong Kong | Singapore | South Korea | Turkey | California CCPA | Brazil |
|--|------|-----------|--------|-----------|-----------|-------------|--------|-----------------|--------|
| Section 5 Requirements related to ISO 27001 | | | | | | | | | |
| Section 6 Guidance related to ISO 27002 | | | | | | | | | |
| Section 7 Guidance for Controllers | | | | | | | | | |
| Section 8 Guidance for Processors | | | | | | | | | |

Source: <https://dataprotectionmapping.z21.web.core.windows.net/#/dashboard>

Demonstrate compliance according to GDPR and a certification scheme according to Art. 42 GDPR

GDPR specific PIMS according to ISO/IEC 27701

PIMS
according to
ISO/IEC 27701

GDPR
specific obligations

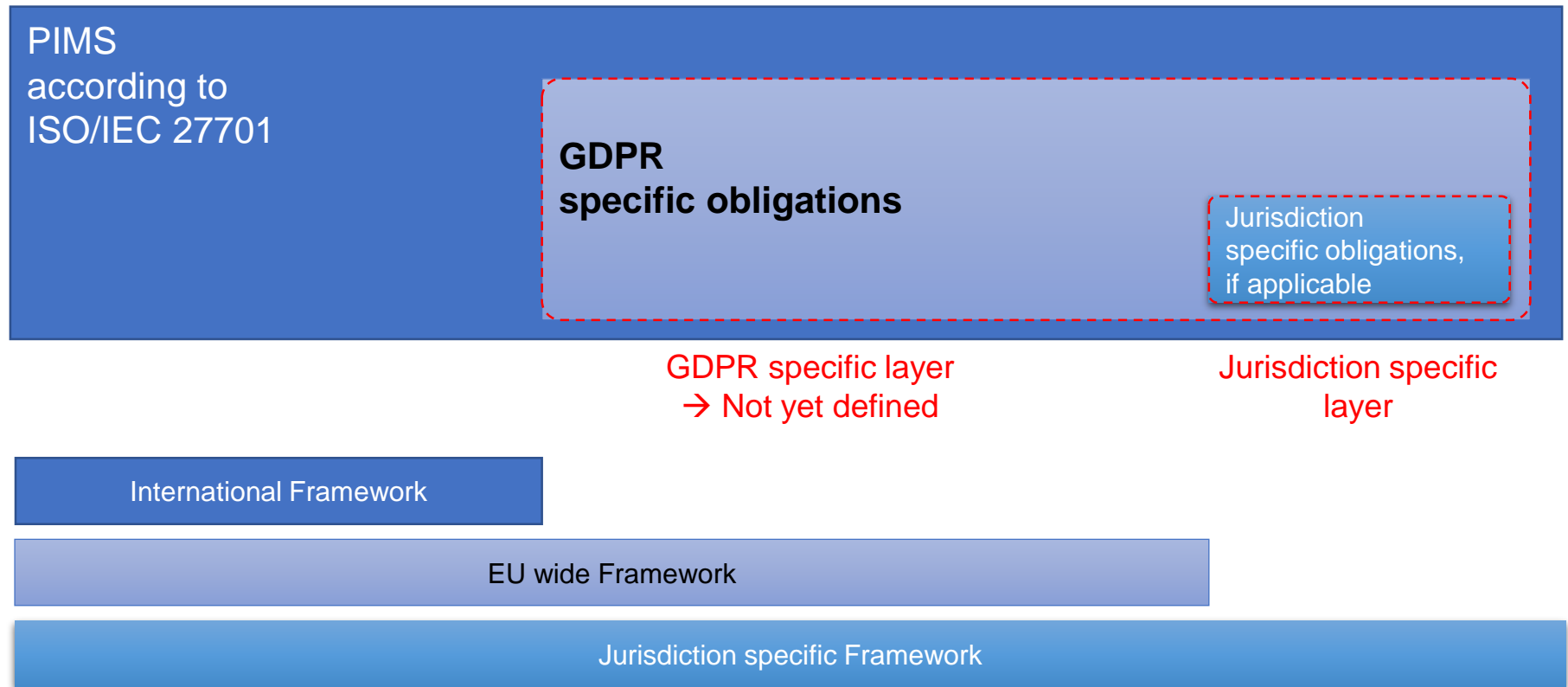
Jurisdiction
specific obligations,
if applicable

PIMS can be used to demonstrate compliance according to Art. 5(2) GDPR

Certification of PIMS according to ISO 27001+

Certification according to Art. 42 GDPR?

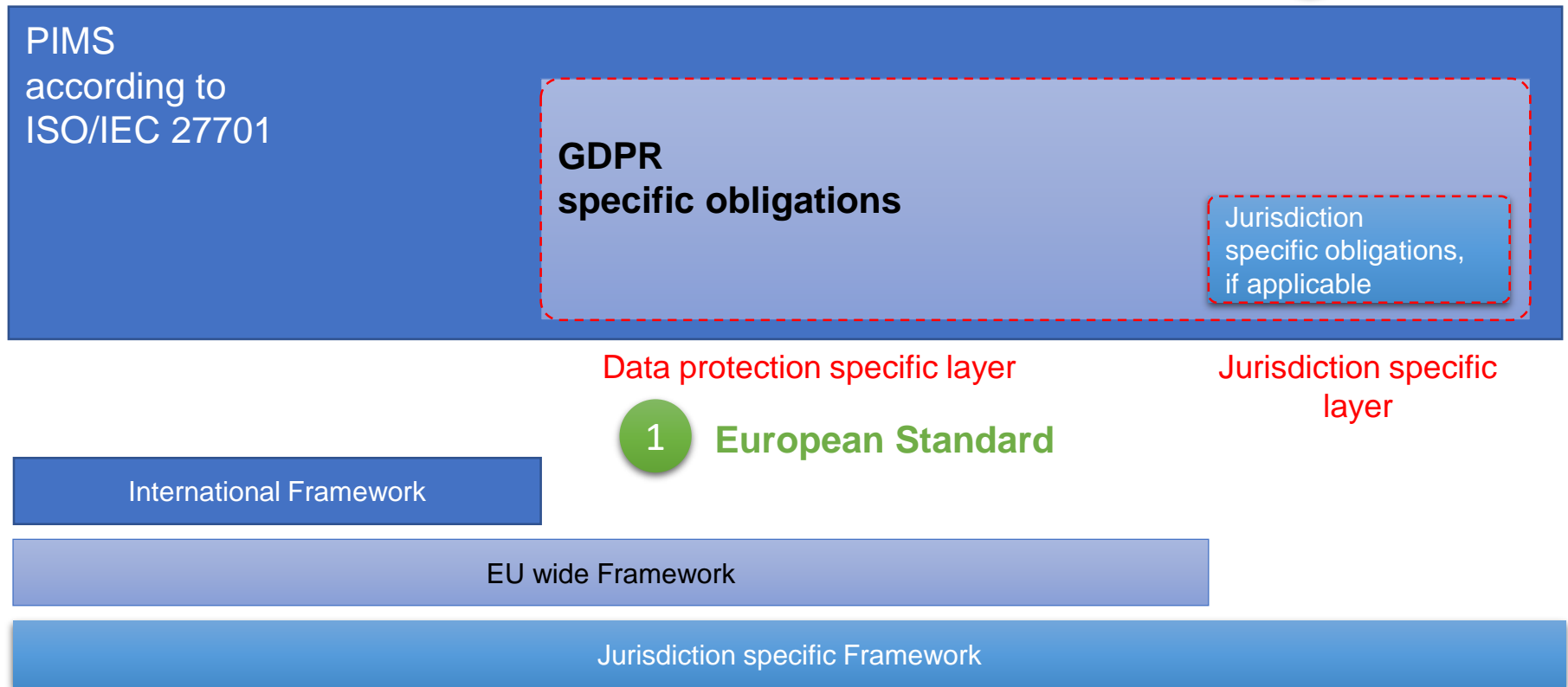
Missing standardized GDPR specific layer



Standardized GDPR specific layer and consistent application

2

Guidance





Markus Gierschmann

Dipl.-Ing. oec.

Finanzökonom (ebs)

CIPP/E, CIPM

Gierschmann Consulting

Kattjahren 4

22359 Hamburg

T + 49 40 419 239 40

M + 49 175 596 1553

m.gierschmann@gierschmann.com

www.gierschmann.com