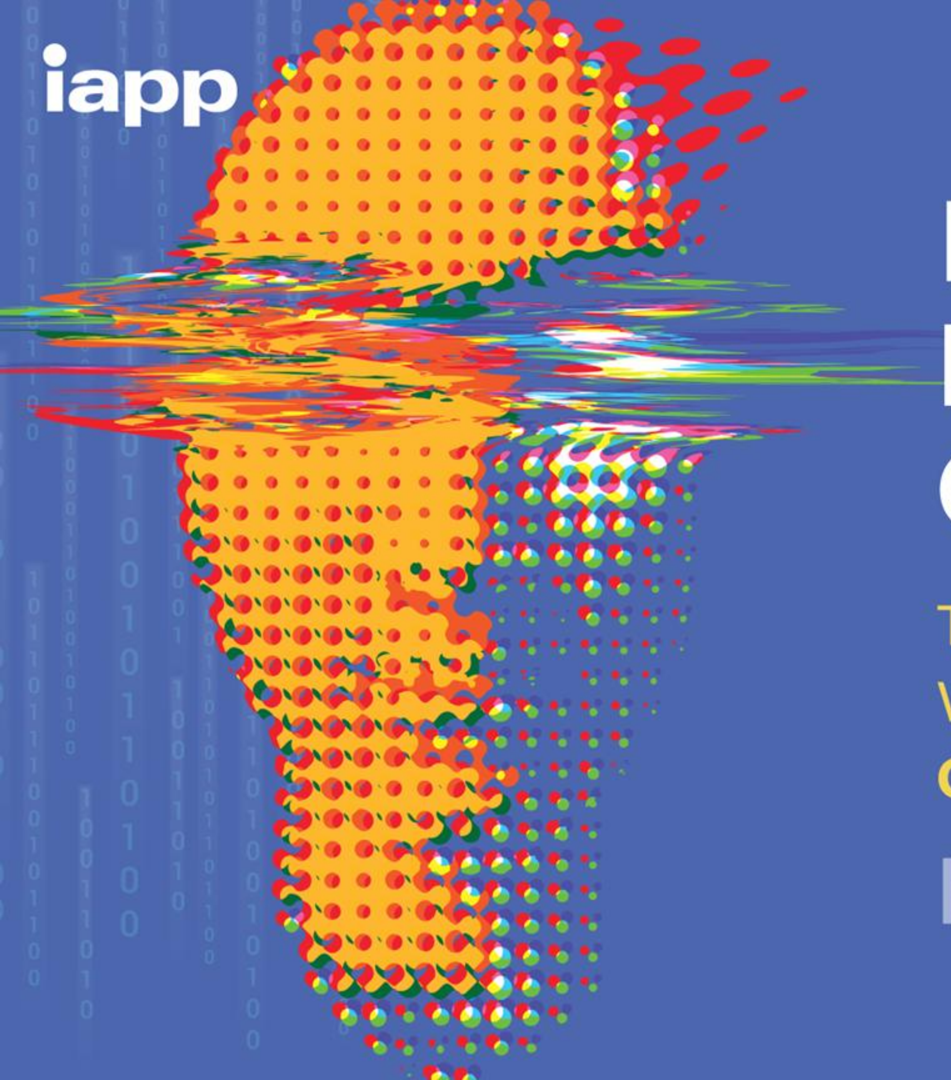
iapp



IAPP Europe **Data Protection Congress 2024**

Training 18-19 November

Workshops 19 November

Conference 20-21 November

BRUSSELS

#DPC24

ISO 27701 & ISO 42001:
How to Integrate Privacy and AI Management Systems

WELCOME AND INTRODUCTIONS

Dr. Sebastian Kraska
External DPO
IITR Datenschutz GmbH

Anna Rocke
Director Data Privacy, Ethics & Compliance
Celonis SE

Cristina Sirera
Global Data Protection Director, CIPP/E
Colt Technology Services

Srinivas Poosarla
Senior VP and Group Chief
Infosys

ISO 27001, ISO 27701, ISO 42001

ISO27001

Standard to establish an **Information Security Management System (ISMS)** to protect **confidentiality**, **integrity** and **availability** of (any) data.

ISO 27701

Extension of ISO 27001 for **Controllers** and **Processors** to protect Personal Identifiable Information (PII) in compliance with regulations such as GDPR through a **Privacy Information Management System (PIMS)**.

ISO 42001

Standard focused on creating trustworthy, ethical, and responsible **Artificial Intelligence Management System (AIMS)** to ensure **transparency**, **accountability** and **fairness** in AI practices.

→ **Designed to be (partially) combined: harmonized High-Level Structure** ←

ISO 27701 Certification - Prerequisites

- **“Money talks”**
  - Resources, budget and management commitment.
- **“Recording is rewarding”**
  - Records of privacy policies, procedures, risk assessments, and incidents.
- **“Best team wins”**
  - Integration of privacy considerations into existing processes and systems.
- **“There is no privacy without security”**
  - Ensure your organization is already ISO 27001 certified.

ISO 27701 Certification - Checklist (1/2)

1. **Become a norm nerd!**
    - Familiarize yourself with ISO 27701 and its requirements.
    - Provide training for your team on ISO 27701 requirements and privacy governance.

2. **Mind the gap!**
    - Assess your current privacy management practices against ISO 27701 requirements.
    - Identify gaps/areas that need improvement or additional measures.

3. **Be able to tick the boxes!**
    - Establish a Privacy Information Management System (PIMS) tailored to your organization.
    - Ensure all documentation aligns with ISO 27701 requirements.

ISO 27701 Certification - Checklist (2/2)

4. **Better safe than sorry!**
   - Conduct internal audits and review to assess the effectiveness of your PIMS.
   - Identify areas for improvement and take corrective actions.

5. **Strike a bargain!**
   - Choose an accredited certification body to perform the external audit.
   - Prepare your people and do a final check on your documentation.

6. **Enjoy the ride!**
   - Undergo the external audit conducted by the certification body.
   - If no major gaps identified, the certification body will issue the ISO 27701 certificate.

Costs and Efforts for 27701 journey (1/2)

Obtaining ISO 27701 certification involves several external costs and internal efforts:

EXTERNAL COSTS

- Certification fees
- Consultancy fees for external experts
- Training programs for employees
- Fees for initial and surveillance audits

It is important for organizations to understand these costs before considering ISO 27701 certification.

Costs and Efforts for 27701 journey (2/2)

INTERNAL EFFORTS

- **Resource Allocation** for dedicated team members to implement and maintain the Privacy Information Management System (PIMS) effectively.
- **Policy Development and Updates** for privacy policies is a significant effort required to achieve ISO 27701 certification. They must be in line with privacy regulations and should be frequently updated.
- **Internal Training Sessions** for staff help in creating awareness and enforcing the privacy policies to assure that everyone in the organization understands privacy regulations and their privacy roles.
- **Record Keeping** and documentation is necessary to ensure that all privacy-related activities are tracked and documented. This helps to ensure that the privacy policies are enforced, and the organization is compliant with privacy regulations.

Benefits of the ISO 27701 (1/2)

1. **Demonstrate Reliability and Trust.** With a certification and/or quality label, companies have the opportunity to demonstrate their reliability to their surroundings, such as purchasers, suppliers, business partners and government. Reliability is an abstract term and is expressed in quality, safety, environment and durability of products and/or services.

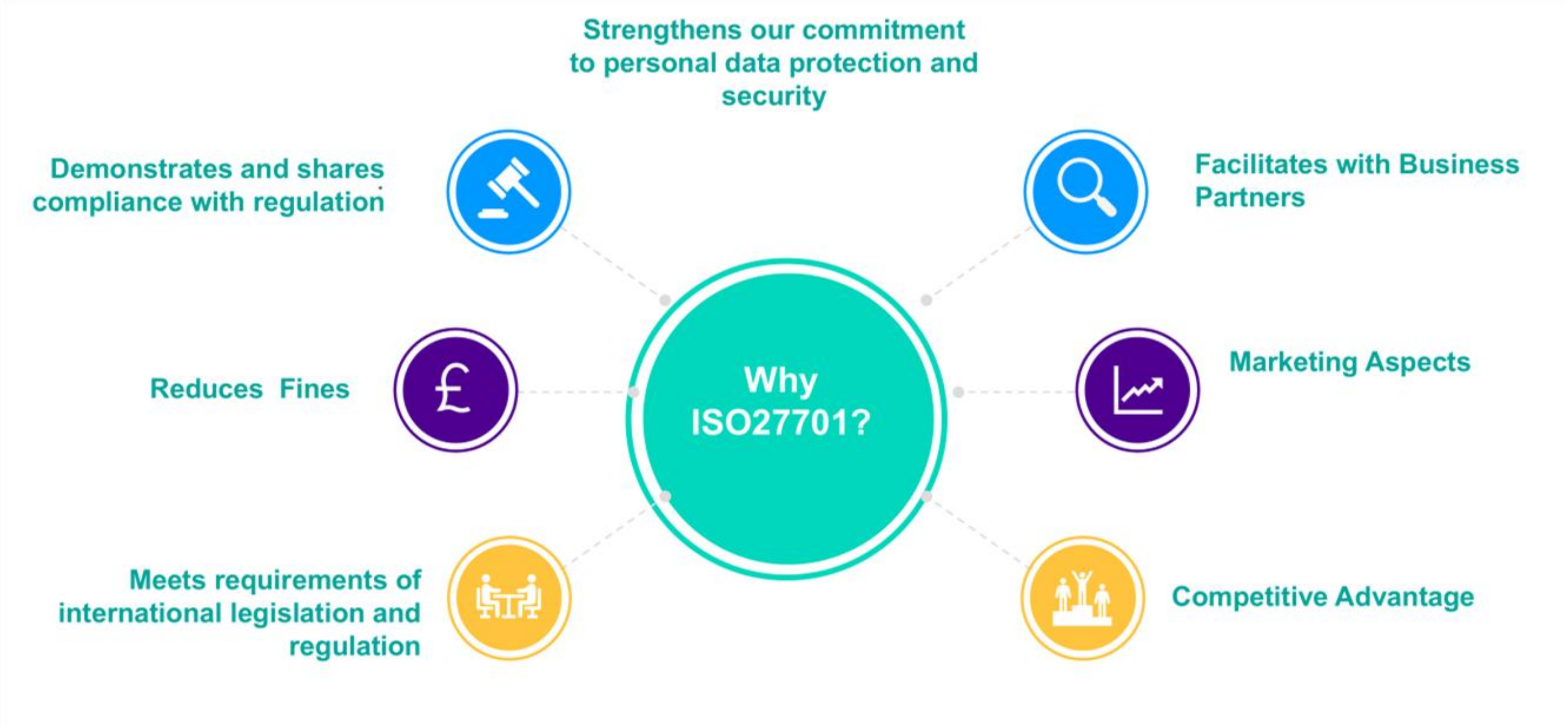
2. **Well-known 3rd certified body** (BSI auditor) **and International Standard Organisation used** (ISO, International Organization for Standardization), an independent, non-governmental, international organization that develops standards to ensure the quality, safety, and efficiency of products, services, and systems).

3. **Meet requirements of international legislation and regulation**. With an ISO standard, companies demonstrate that they meet the requirements of international legislation and regulation and adhere to these.

4. **To participate and be considered in tenders and RFPs**. Particularly in the field of tendering, it’s important that companies have an ISO certificate. ISO can also be a requirement to be considered for orders by large contractors or from decentralized government and municipalities, for instance.

5. **Consistency of standards and quality across industries and nations.**

Benefits of the ISO 27701 (2/2)



Why ISO27701?

Strengthens our commitment to personal data protection and security

Demonstrates and shares compliance with regulation

Facilitates with Business Partners

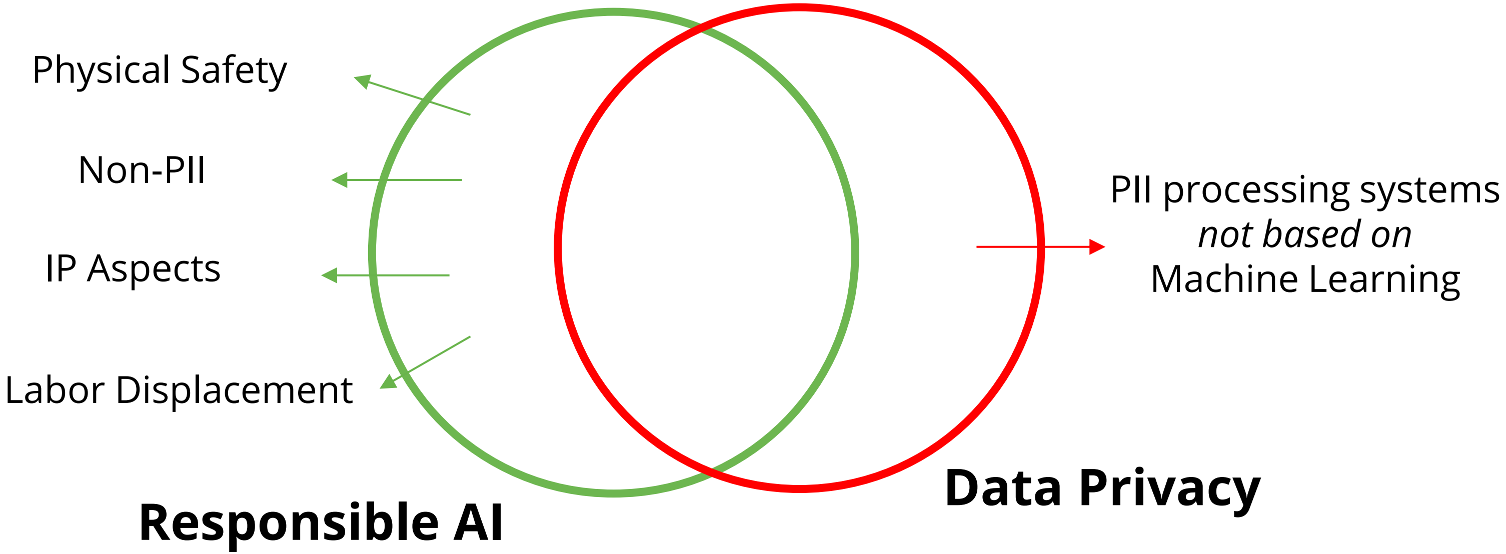
Reduces Fines

Marketing Aspects

Meets requirements of international legislation and regulation

Competitive Advantage

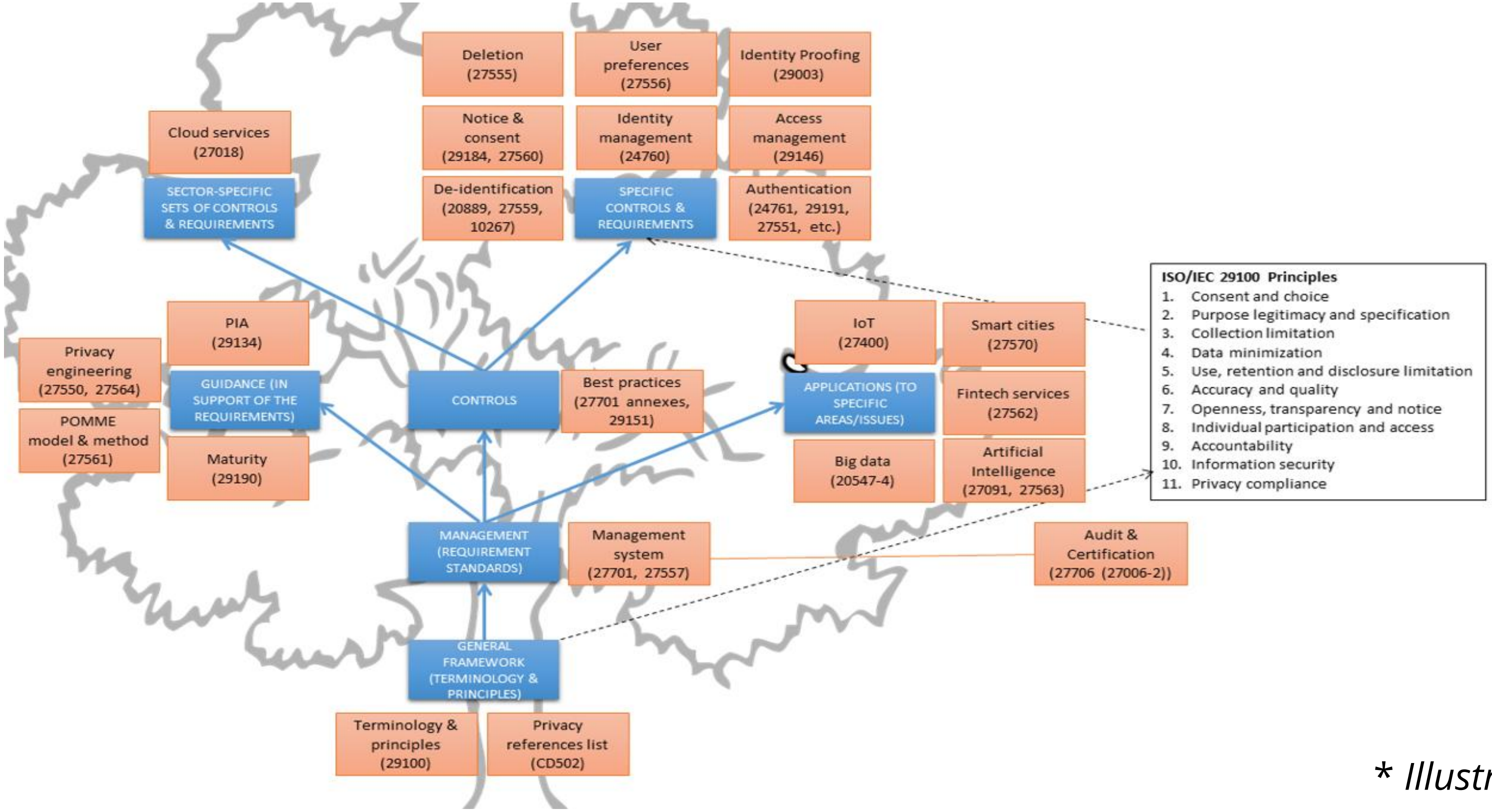
Intersection of Privacy & AI



Integrating PIMS and AIMS

- Both ISO 27701 and 42001 are based on continuous improvement framework
  - Organizational Context: Needs & Expectations of Stakeholders form key input to Scoping & Policies
  - Leadership: Policy, Commitment & Governance structure
  - Planning & Operation: primarily Managing Risk & Identifying opportunities for improvement
  - Support: Resources, Competence, Awareness & communication
  - Measurement, monitoring & Continuous improvement
- Control Objectives, Controls their Implementation Guidance are different for AI and Privacy
- Bulk of AI principles are also part of Data Privacy (as shown in venn diagram)
- Common set of procedures for bulk of RAI and Privacy requirements
- SoA of ISO 42001 may be made to cross refer to PIMS
- Non-privacy related AI requirements can have distinct procedures
- DPO and RAI is often part of same organization independent of business functions
- Governance, Oversight & Audits may also be integrated

Overview of SC27 Standards (Privacy)*



Deletion (27555)

User preferences (27556)

Identity Proofing (29003)

Notice & consent (29184, 27560)

Identity management (24760)

Access management (29146)

De-identification (20889, 27559, 10267)

SPECIFIC CONTROLS & REQUIREMENTS

Authentication (24761, 29191, 27551, etc.)

Cloud services (27018)

SECTOR-SPECIFIC SETS OF CONTROLS & REQUIREMENTS

PIA (29134)

Privacy engineering (27550, 27564)

GUIDANCE (IN SUPPORT OF THE REQUIREMENTS)

POMME model & method (27561)

Maturity (29190)

CONTROLS

Best practices (27701 annexes, 29151)

IoT (27400)

Smart cities (27570)

APPLICATIONS (TO SPECIFIC AREAS/ISSUES)

Fintech services (27562)

Big data (20547-4)

Artificial Intelligence (27091, 27563)

MANAGEMENT (REQUIREMENT STANDARDS)

Management system (27701, 27557)

Audit & Certification (27706 (27006-2))

GENERAL FRAMEWORK (TERMINOLOGY & PRINCIPLES)

Terminology & principles (29100)

Privacy references list (CD502)

ISO/IEC 29100 Principles

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

** Illustrative only*

Questions?

RESOURCE LIST

- ISO/IEC 27701:2019: https://www.iso.org/standard/71670.html
- ISO/IEC 42001:2023: https://www.iso.org/standard/81230.html