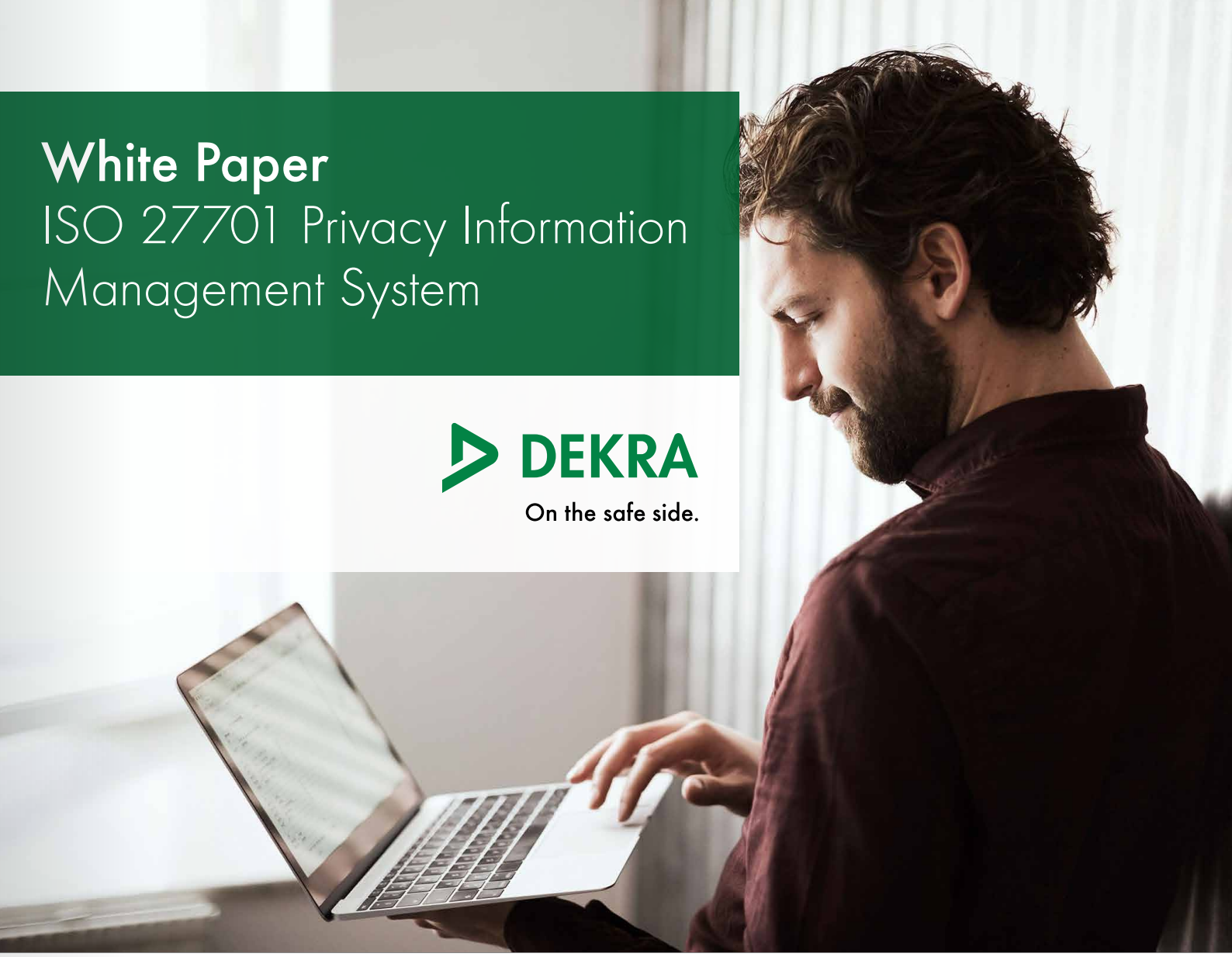
White Paper
ISO 27701 Privacy Information Management System



DEKRA
On the safe side.

ISO 27701 focuses on the development, implementation, maintenance and continual improvement of a privacy information management system (PIMS). It is an extension of the already established ISO/IEC 27001 information security management system (ISMS) and ISO/IEC 27002 information security controls code of practice requirements. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have incorporated requirements of various national laws, such as the GDPR, and the data protection principles of ISO/IEC 29100 into ISO 27701, making it the premium international standard for managing privacy risks and meeting regulatory requirements for protecting personal data.

Defining data privacy

While data protection secures data from unauthorized access, data privacy is concerned with issues facing authorized access – namely how it is defined and who has it. Personally identifiable information (PII) such as names, social security numbers, addresses, phone numbers, and other information with the potential to expose a person's identity must be protected during the collection, usage, and sharing of data. With a whopping 4.5 billion internet users worldwide as of mid-2019[1] and 7.098 data breaches that exposed over 15.1 billion records in 2019, there is growing global concern regarding data privacy[2].

Eight out of 10 people (78%) surveyed in 2019 worried about their online privacy, with over half (53%) more nervous than they were the year before. This marked the fifth year in a row that a majority of those surveyed felt more anxious about their online privacy than in the previous year[3].

1 https://www.internetworldstats.com/stats.htm
2 https://www.riskbasedsecurity.com/2020/02/10/number-of-records-exposed-in-2019-hits-15-1-billion/
3 https://www.cigionline.org/internet-survey-2019

The importance of ISO 27701

Almost every organization processes personally identifiable information (PII), including private, client and employee data. As organizations grow, expand, and adopt new technologies, the volume and variety of processed PII increases. Data privacy laws and regulations in force around the world must also adapt to the demands and risks of the changing online environment.

Released in the summer of 2019, ISO 27701 is the latest standard extension to the well-known ISO 27001 norm for information security management system (ISMS) requirements. ISO 27701 provides guidelines to extend an already existing ISMS by adding components to support a privacy information management system (PIMS). ISO 27701 certification is solely awarded as a supplement to ISMS certification according to ISO/IEC 27001.

Composition of ISO 27701 for privacy information management

Benefits of ISO 27701

- **Reliable support with privacy laws and regulations governing PII for controllers and processors**
- **Covering requirements of standards such as GDPR, UK DPA, HIPPA, and CCPA as well as other ISO standards**
- **Practical, clear measures on how to safeguard PII**
- **Increased trust and privacy awareness**
- **Assured transparency between stakeholder**

Compliance challenges

ISO 27701 addresses three key compliance challenges:

- **Numerous regulatory requirements**
  Reconciling multiple regulatory requirements through the use of a universal set of operational controls enables consistent and efficient implementation.
- **Costly regulation-by-regulation auditing**
  Both internal and third-party auditors can assess regulatory compliance using a universal operational control set within a single audit cycle.
- **Risk of non-compliance without proof**
  Commercial agreements involving the transfer of personal information may warrant certification of compliance[4].

Defined roles in privacy management

The roles specified in the ISO 27701 standard include controllers and processors, which are defined in Article 4 of the GDPR or in the ISO 29100 standard.

A **controller** is a "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."

A **processor** is a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller[5]."

4 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3uDwE
5 https://ec.europa.eu/info/law/law-topic/data-protection_en

Structure of ISO 27701

ISO 27701 is divided into privacy-centric clauses (5-8) and annexes (A-F). The clauses provide additional requirements or implementation guidance including:

- PIMS-specific modifications to the ISO 27001 (Clause 5)
- PIMS-specific requirements to the ISO 27002 (Clause 6)
- Additional requirements to ISO 27002 for PII controllers (Clause 7)
- Additional requirements to ISO 27002 for PII processors (Clause 8)

Six important annexes provide guidance for the standard addressing topics such as:

- PII Controllers (Annex A)
- PII Processors (Annex B)
- Mapping to ISO 29100 (Annex C)
- Mapping to GDPR (Annex D)
- Mapping to ISO 27018 & 29151 (Annex E)
- Mapping to ISO 27001 & 27002 (Annex F)

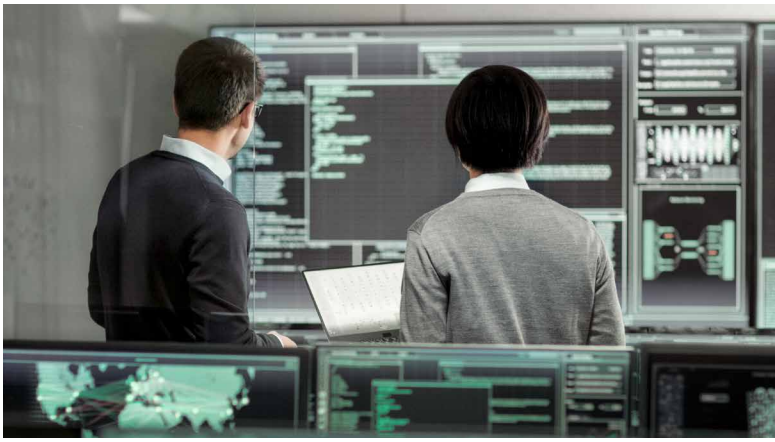
How to incorporate ISO 27701 into various ISMS setups

ISMS extension according to ISO 27701 is a bit more complicated for organizations that have included ISO/IEC 27017 or ISO/IEC 27018 in their management systems. Key modifications must be made to the overall ISMS structure, existing controls described in Annex A, and the implementation of the control objectives relevant to PII processors and controllers. Transition to ISO 27701 may be a little simpler for organizations with a structure and processes supporting GDPR requirements. In both cases, however, the appropriate and effective implementation of processes into the scope of the ISMS must be ensured.

The successful incorporation of ISO 27701 into an existing information security management system (ISMS) depends on:

- A gap assessment of the existing ISMS according to ISO 27701 requirements
- Identification of gaps and an action plan providing a gap solution strategy
- Adjusting the scope
- Adaptation of controls from ISO 27001 to the new requirements
- Clarifying whether you are a PII controller, processor - or most likely, both
- Extension of the SOA or new SOA for Annex A and B of ISO 27701
- List of processing activities
- Expansion of the asset management
- Incorporation of new requirements into the ISMS design
- Evaluate the expanded ISMS with risk assessment, measurement and monitoring, internal auditing, management review, and other relevant appraisal tools

Operational results are measured to ensure that the extended ISMS meets both previously existing and new requirements. Areas that are deficient or non-conformant in any way must be managed through established continual improvement strategies or corrective action procedures.



Keeping proper records of breaches

Any breach of PII must be recorded to provide a report for regulatory and/or forensic purposes with sufficient information including the:

- Description and time period of the incident
- Consequences of the incident
- Name of the individual who reported the incident
- Name of the individual to whom the incident was reported
- Steps taken to resolve the incident (including the person in charge and the data recovered)
- Assessment of whether the incident resulted in unavailability, loss, disclosure or alteration of PII

ISO 27701 support services

Nearly every company deals with large amounts of electronic data in the rapidly changing global digital economy. Because privacy goes hand-in-hand with security, if you are already ISO 27001 certified, most of the work for 27701 certification has already been done.

To ensure the privacy of your personally identifiable information (PII), our accredited auditors can provide:

- Security and privacy gap assessments between your existing systems and the requirements of ISO 27001 and ISO 27701
- PII processing assessments to examine the scope of PII collected, processed, and shared

Do you require support for your ISO 27701 certification? Contact our experts now!

Other beneficial services

We certify numerous management systems e.g. according to ISO 9001, ISO 14001, ISO 45001 and their combinations. Our portfolio includes over 40 accreditations and approvals!

The DEKRA Group provides comprehensive services focused on information security including:

- Training and education, e.g. to become an IT specialist
- Product certifications, e.g. electromagnetic compatibility (EMC)
- Personal certifications, e.g. data protection specialist

The DEKRA seal of excellence

Setting maximum quality and reliability – across different industries and internationally – the DEKRA seal is an excellent hallmark and marketing instrument which sets you apart from the competition. Use it to show your customers and business partners the value of what you offer. We are here to help you.

DEKRA Audits
Mail audits@dekra.com
Web www.dekra.com/en/audits/