qualityaustria
Succeed with Quality

ISO 27701

Integrated approach: Data privacy and information security

MOTIVATION AND BENEFITS

ISO 27701:2019 can be used to verify compliance with privacy regulations and is an extension to ISO 27001. The standard adds a wide range of aspects relevant to the protection of privacy.

The official name of the standard is „ISO/IEC 27701:2019-08 – Information technology – Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines".

The title already indicates the thematic relation within the ISO 27000 family of standards and shows how strongly information security and privacy are connected. Both standards, as well as the combined management system are based on the principles of confidentiality, integrity and availability of data and information. Therefore, an interaction of these ISO standards is not surprising and implementing them together is highly recommended.

In addition to the Information Security Management System (ISMS) in ISO 27001, ISO 27701 provides specific guidance for implementing a Privacy Information Management System (PIMS) – as an integral part of the existing ISMS, specifically extended to include data privacy aspects. The PIMS provides better control over Personally Identifiable Information (PII), gives an opportunity to manage this PII and, if desired, share it with other users.

With an implemented management system according to ISO 27701, an organization achieves systematic further development, including optimization of processes in the area of protection of privacy. Internal and external audits support this process.

The benefits of a certification for organizations are therefore obvious:

- It provides a systematic and clear management tool and control system for all privacy protection issues that need to be addressed and for the treatment of sensitive data and Personally Identifiable Information.
- It proves that the handling and processing of Personally Identifiable Information complies with the requirements of the GDPR (General Data Protection Regulation).
- The risk-based approach can identify and prevent possible areas of liability at an early stage.
- The integrated approach of a PIMS for information security and privacy has several advantages of integrated management systems, such as rapid implementation, a common risk management process and a significant increase in efficiency due to numerous synergy effects.

CIS is one of the first internationally accredited providers to offer the certificate "Privacy Information Management according to ISO 27701" – as an addition to ISO 27001 – which provides objective evidence that your organization complies with the privacy protection requirements of the GDPR. The certificate creates confidence – both internally and externally – and is a clear signal on the market.

OBJECTIVES

- Increases legal certainty and transparency
- Ensures sound mechanisms for the protection of privacy
- Increases the competence for the protection of privacy
- Minimizes the risk of data breach and possible consequences
- Creates confidence with existing and potential customers

qualityaustria
Succeed with Quality

TARGET GROUP

This standard includes the requirements for comprehensive protection of data and information. The requirements set out are generic and are intended to be applicable to all organizations, regardless of type and size, sector or legal form.

REQUIREMENTS

Prerequisite for a successful certification according to ISO 27701 is a valid ISO 27001 certificate. Due to the content-related similarity with information security, the new extension to protection of privacy can be built on existing systems and structures. For many organizations this means only little additional effort. In particular for organizations that already comply with the GDPR, it can be assumed that most parts of the requirements and measures have already been implemented, as ISO 27701 is to a large extent built on the regulations of GDPR.

OTHER RELEVANT STANDARDS

- ISO/IEC 27001 or ISO/IEC 27002
- ISO/IEC 27018
- ISO/IEC 29100 and ISO/IEC 29151
- GDPR

CIS – ABOUT US

As a recognized certification body, CIS is specialized in information security, data privacy, IT services, cloud computing, data center as well as business continuity management. The excellent reputation of CIS certificates nationally and internationally is regarded as a real competitive advantage and a door opener in business cases worldwide. The reason for this is the high quality of CIS accreditation awarded by the Federal Ministry for Digital and Economic Affairs (BMDW) as well as the proven certification procedure. CIS auditors also actively provide their in-depth technical knowledge during the preparations for certification as well as the subsequent audits.

QUALITY AUSTRIA – WHO WE ARE

Quality Austria - Trainings, Zertifizierungs und Begutachtungs GmbH is the leading Austrian contact for system and product certification, verification and validation, assessments, trainings and certification of persons as well as the Austria Quality Seal. Basis are worldwide applicable accreditations by the Federal Ministry for Digital and Economic Affairs (BMDW). Furthermore, since 1996 the Austrian Excellence Award is presented together with the BMDW. The organization cooperates with some 50 partner and member organizations worldwide and is national representative of IQNet, EOQ and EFQM.

Klaus Veselko
Executive Vice President
CIS - Certification & Information Security Services GmbH
klaus.veselko@cis-cert.com

Dr. Anni Koubek
Executive Vice President
Innovation, Business Development, Certification Quality
anni.koubek@qualityaustria.com

CIS
Certification & Information Security Services GmbH
www.cis-cert.com
office@cis-cert.com
Salztorgasse 2/6/14,
1010 Vienna, Austria
Tel.: +43 1 532 98 90
Fax: +43 1 532 98 90 89

qualityaustria
Succeed with Quality
Quality Austria
Trainings, Zertifizierungs und Begutachtungs GmbH
www.qualityaustria.com office@qualityaustria.com

Headquarters
Zelinkagasse 10/3
1010 Vienna, Austria
Tel.: +43 1 274 87 47
Fax: +43 1 274 87 47-100

Customer Service Center
Am Winterhafen 1
4020 Vienna, Austria
Tel.: +43 732 34 23 22
Fax: +43 732 34 23 23

Doc. Nr.: RE 24_00_105, Edition: August 2020