New EU Data Protection Regulation: To what extent does ISO 27001 certification help?

The new EU Regulation for Europe-wide uniform data protection is to be published in 2013 and supersede the national Data Protection Acts from 2015. This means that penalties to the amount of up to Euro 1 million will become possible. Certificates for data protection should also become more important. An ISO 27001 certification relating to information security already covers significant contents of these requirements relating to data protection. A comment written by Herbert Bieber, Technical Expert for Data Protection, who works for the Certification Body CIS.

The EU Directive 95/46/EC (Data Protection Directive), which forms the basis for the Austrian Data Protection Act “DSG 2000”, has grown old and is to be completely superseded by the new EU Data Protection Regulation. Optimists start upon the assumption that the Regulation will still be passed in 2013. The draft intends the Directive to enter into force two years after its publication, i.e. presumably in 2015.

The EU Base Regulation supersedes the national Data Protection Acts

Other than the Directive, the Regulation shall directly apply in each member state. Implementation in national law will no longer be necessary. This means that the Austrian Data Protection Act will be superseded and that uniform rules will be reached all over Europe. It is true that some key issues of the Regulation still are open. Nevertheless, significant innovations may be expected: The maximum range of administrative penalties will be increased drastically - up to Euro one million or two per cent of the corporate sales are under discussion. This also refers to offences that are regarded as being “peccadillos” today: For example, this refers to the processing of personal data without a legal basis.

Estimating the consequences of data protection

Many new duties are inflicted upon the organizations. For example, the organizations will be compelled to provide a Data Protection Representative, the criteria still being discussed vehemently. The draft wants to see a Data Protection Representative for organizations that have 250 employees or more. As for public authorities, this obligation shall apply, in general. A completely new topic consists in starting to analyze systems as to what effects there might be for the persons concerned in case of data leaks. All the new IT systems will have to be designed as to be friendly to data protection (Privacy by Default). In order to reach this, risk analysis as they have been very common in information security for many years will be prescribed by law.

Certifications in terms of data protection

Article 39 of the draft announces the intensification of seals and certifications: *“The member states … promote … the introduction of certification procedures as well as data protection seals and labels that are specific to data protection.”* The goal is that persons concerned can rapidly get to know the data protection level of IT products and IT based services. Known seals, such as the European Privacy Seal, review data protection compliance in analogy to the EU Data Protection Directive while considering such contents as the type of data, sensitivity, processing/transfer/cession, rights of persons concerned or notices of consent. From a technical/organizational perspective, it is reviewed whether the data is processed securely. According to the audit catalogue, the relevant criteria include security policy, entry protection, access protection, network security, risk management and, above all, the way a management system is established - so it is, de facto, a question of controls that are described in the Information Security Standards of the ISO 27k Series.

ISO 27001 as a basis for data protection

By way of summary, it can be stated that it will, without an Information Security Management System (ISMS), be much more difficult to meet the requirements placed by the new IT Baseline Protection Regulation. As for such topics as privacy impact analyses, risk analyses, technical/organizational controls or data protection certifications, an ISMS acc. to ISO 27001 enormously facilitates work to be done by the Data Protection Representative. In case of disputes, an ISO 27001 Certificate will furnish evidence that a technical/organizational management system has been implemented and security at data processing is fulfilled in conformity to legislation, appropriately and to the state of the art.

Availability, confidentiality and integrity of data

Conclusions: As a Standard for Information Security, ISO 27001 covers all types of business information. As compared to this Standard, the Data Protection Act only refers to personal data. The contents of ISO 27001 go beyond those of the Data Protection Act. On the other hand, ISO 27001 does not cover more profound specifics of data protection - such as review of conditions for admissibility, compliance with the secrecy interests worthy of protection or keeping of the rights of persons concerned - in detail. On the whole, certification acc. to ISO 27001 significantly supports European data protection certifications in terms of availability, confidentiality and integrity of data, covers an important part of data protection requirements or supports their fulfilment.

Ing. Herbert Bieber, MSc, CISA (Certified Information Systems Auditor), is an independent Technical Advisor and Trainer in the fields of information security and data protection. He acts as a Technical Expert for issues relating to data protection by order of the Certification Body CIS.

www.cis-cert.com