



Experiences from data protection certification and the use of standards or the lack thereof

Sebastian Meissner, Head of EuroPriSe Certification Authority

CEN-CENELEC - ENISA workshop on standards - Sep. 19, 2017 - Brussels



Brief Introduction of EuroPriSe

p. 2 Experiences from data protection certification and the use of standards or the lack thereof

2016: Entry into force of GDPR: §§ on data protection certification on EU level for the very first time (incl. the option of a European Data Protection Seal)

May 25, 2018:

GDPR directly applicable

Objective of EuroPriSe:
Accreditation as certification body + approval of certification criteria by European Data Protection Board (EDPB)

2014: Operator change: ULD → EuroPriSe GmbH
Advisory Board with (former) DPA representatives from several MS
More than 100 legal + technical experts located in 19 countries

2009 - 2013: German DPA ULD operates EuroPriSe und acts as certification body

2007 - 2009: EuroPriSe starts as an EU-funded project: DPAs from Germany, France and Spain as well as other project partners specify certification criteria and procedures and conduct pilot certifications


- 🕒 Development of EuroPriSe certification criteria for IT products + IT-based services
 - 🕒 The initial version of the criteria catalogue was drafted in 2007/08 - experienced IT-security auditors were involved in the drafting process.
 - 🕒 Art. 17 Directive 95/46/EC does not list concrete TOMs, but only establishes general guidelines on technical and organisational measures to be implemented in order to ensure a sufficient level of data security.
 - 🕒 Hence: Set 3 of the criteria catalogue dealing with technical and organisational measures relies on control objectives and controls specified in ISO/IEC 27001 and ISO/IEC 27002 for services and security functions defined in ISO/IEC 15408 (Common Criteria) for products.

EuroPriSe Criteria for IT products and IT-based services


Set 3: Technical-Organisational Measures: Accompanying Measures for Protection of the Data Subject.....	70
3.1 General Duties	70
3.1.1 Preventing Unauthorised Access to Data, Programs, Premises and Devices	71
3.1.1.1 Physical Access Control.....	71
3.1.1.2 Access to Media and Mobile Devices.....	71
3.1.1.3 Access to Data, Programs and Devices.....	72
3.1.1.4 Identification and Authentication	73
3.1.1.5 Use of Passwords	73
3.1.1.6 Organisation and Documentation of Access Control.....	74
3.1.2 Logging of Processing Personal Data.....	75
3.1.2.1 Logging Mechanisms	75
3.1.2.2 Operation of Logging Mechanism	76
3.1.3 Network and Transport Security	77
3.1.4 Mechanisms to Prevent Accidental Loss of Data; Back-up Mechanisms and Recovery	77

- 🕒 Application of certification criteria / required depth of technical inspection
 - 🕒 At the beginning of a certification project, the technical evaluator submits an inspection concept to the EuroPriSe certification body for approval.
 - 🕒 The required depth of inspection may be reduced considerably if the seal applicant or one/several of his/her contractors possesses a widely recognized IT-security certification such as ISO/IEC 27001 that is current and relevant to the target of evaluation (ToE).
 - 🕒 Example: If the applicant relies on a data center which is in possession of a current ISO/IEC 27001 certification, it might be appropriate for the technical evaluator to dispense with an on-site visit of this data center.

Application of certification criteria / required depth of technical inspection

-  However, a mere reference to a certificate / statement of applicability does not suffice:

Rather, the technical evaluator is required to describe and assess the implemented TOM in the evaluation report. Hereby, the next bullet point is to be considered.

-  Evaluators must keep in mind the different perspectives / protection goals of IT-security (assets of an organisation) and privacy / data protection (fundamental rights of the data subjects).

Typical example of a (potential) conflict:

Retention of log files containing personal data

🕒 Application of certification criteria / required depth of technical inspection

- 🕒 A future International Standard ISO/IEC 27552 (“PIMS standard”) will be even more useful in this respect than ISO/IEC 27001 is today.

In particular, possession of a current 27552 certification may allow for a further reduction of the evaluation efforts that are required from EuroPriSe’s evaluators.

- 🕒 Certifications based on sector-specific enhancements to ISO/IEC 27001 can be useful as well for a certification according to EuroPriSe.

This is particularly true for sector-specific enhancements containing privacy-specific controls such as ISO/IEC 27018.

EuroPriSe GmbH

Sebastian Meissner

Head of EuroPriSe Certification Authority

Joseph-Schumpeter-Allee 25

53227 Bonn

Germany

Tel: +49 228 763 679 - 30

Email: ca@european-privacy-seal.eu