General overview of standards for conformity assessment certification schemes in data protection

Alessandro Guarino
CEN/CENELEC JTC13/WG5 Convener
Founder & CEO, StAG S.r.l.

CYS Informative Seminar
Nicosia 16/3/2023

The Speaker

20+ Years in Information Security and Data Protection

StAG INFORMATIONGOVERNANCE

Speaker / Author

CyCon International Conference on Cyber Conflict — 2013

ISSE 2016 — 2013-2019

E-PRIVACY XX — 2016 →

pirate security conference psc — 2017

IET Events The Institution of Engineering and Technology — 2017

Università di Roma Tor Vergata — 2018

NATO OTAN — 2018

12th INTERNATIONAL CONFERENCE CPDP DATA 2019 AND — 2019

CYBER SECURITY 360 Summit — 2020 2022

Standards and Policy

UNINFO

CS·CG CEN/CENELEC/ETSI Cyber Security Coordination Group

ETSI — 2011 →

enisa THE EU CYBERSECURITY AGENCY

cen CENELEC

Key actors in GDPR Certification

Controller/Processor

Certification body: third – party conformity assessment body operating a certification mechanisms

GDPR: the competent supervisory authority or certification body accredited in accordance with EN-ISO/IEC 17065/2012 + additional requirements established by the competent supervisory authority

Accreditation body: the **sole body** in a Member State that performs accreditation with authority derived from the State;

GDPR: the competent supervisory authority or the national accreditation body or both

GDPR Certification - summary

voluntary process

element for controller and processor to **demonstrate compliance** of processing operations with GDPR provisions

.inked to the principle of **accountability**

element to **enhance transparency**

conformity assessment activity against specified requirements

performed and **attested** by a **third party**

.ssued on the basis of **approved certification criteria/scheme**

Standards for accreditation

ISO 17065

Conformity assessment — Requirements for bodies certifying **products, processes and services**

ISO 17021

Conformity assessment – Requirements for bodies providing audit and certification of **management systems**

ISO 17024

Conformity assessment -- General requirements for bodies operating certification of **persons**

CEN/CNELEC JTC 13

EN 17926 Privacy Information Management System per ISOIEC 27701 - Refinements in European context. (Almost) published

Certification scheme as per ISO/IEC 17065 for certification against EN ISO/IEC 27701 - refinements in European context. Work started March 23

EN 17799 Personal data protection requirements for processing activities. Completed but not yet published

Scheme for certification of personal data processing operations against EN17799 Under ballot

EN 17926

This document specifies refinements to ISO/IEC 27701, for processing operations as part of products, processes, and services. It **can** be used for assessment of conformity to ISO/IEC 27701 in **European** context, either by first, second, or third parties.

Certification bodies can use these requirements and refinements to assess the conformity of both a privacy information management system per ISO/IEC 17021 and the processing operations of a product, process or service per ISO/IEC 17065.

EN 17926 – The next step

Data controllers and processors who wants to demonstrate accountability, will benefit rom a stronger certification system with an established certification scheme, hence enhancing trust between stakeholders.

Data subjects can have greater confidence in the way their PII are processed thanks to standardized certification process, allowing reliable 3rd party audits that will verify that the obligations towards them are fulfilled.

Data protections authorities, or governmental entities having responsibilities in data protection, can encourage the adoption of stronger certification in the ecosystem, which results in better ability for all actors to demonstrate their compliance to their legal obligations.

17799

This document specifies baseline requirements for demonstrating processing activities' compliance with the EU personal data protection normative framework in accordance with EN ISO/IEC 17065.

It does not apply to products or management systems destined for processing personal data.
This document is applicable to all organizations which, as personal data controllers and/or processors, process personal data, and its objective is to provide a set of requirements enabling such organizations to conform effectively with the EU personal data protection normative framework.

An organization can decide that the standard is applicable only to a specific subset of its processing activities if such a decision does not involve failure to conform with the EU personal data protection normative framework.

EN 17799 Scheme for certification

This document specifies a certification scheme for certification of data protection processing operations against EN17799 (Personal data protection requirements for processing operations)

EN17799 (like prEN 17926 and EN ISO/IEC 27701), can be subject to conformity assessment by certification bodies.

The technical report will specify the guidelines to achieve the adequate level of assurance for the certification of data processing operations against prEN17799.

The guidelines can be considered for qualification as certification criteria as foreseen by GDPR Article 42.

Thanks for Your Time
What are your questions?

Contact:

a.guarino@stagcyber.eu

StAG – Information Governance
www.stagcyber.eu