



Data Protection Certification Mechanisms

Study on Articles 42 and 43 of the Regulation (EU) 2016/679

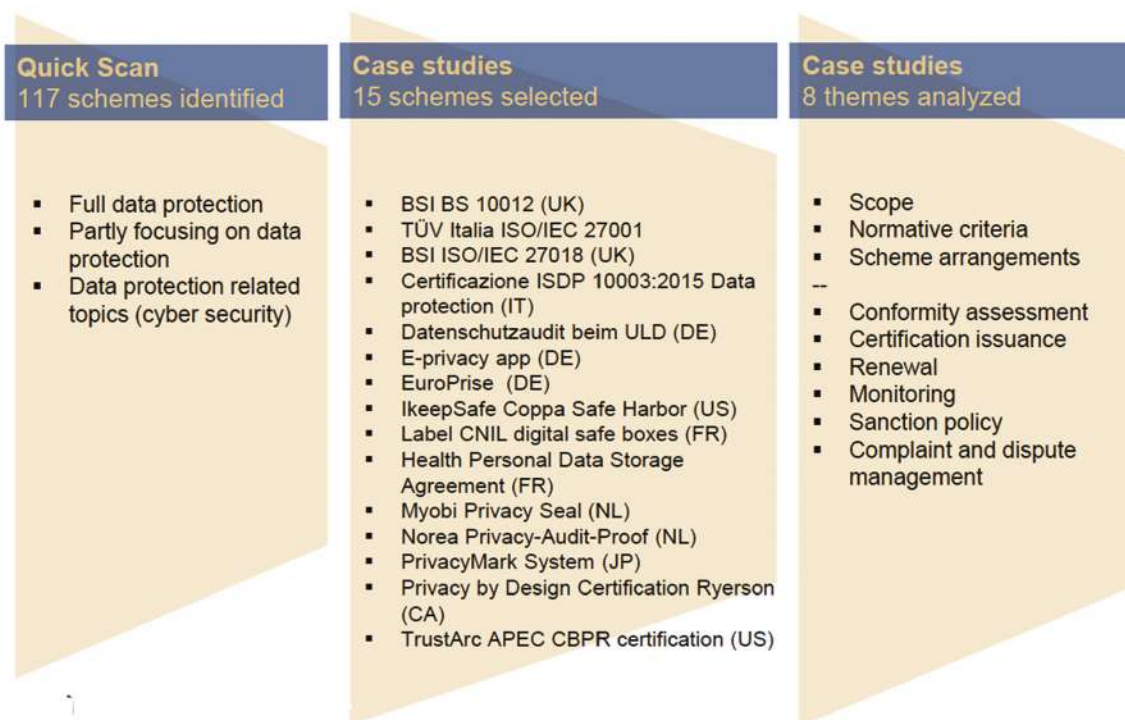
Final Report

The European Commission study on the GDPR certification mechanisms pursuant to art.42 and 43 was commissioned to the prestigious University of Tilburg, in order to verify the opportunities already present at European level in the area of certifications.


TARGET

- **Explain** the art. 42 and 43 and bring them back to the specific terminology of the "certification sector" (ISO 17065: 2012).
- **Map the existing certification schemes**, in the member states and at the level of the main trading partners (total 117) by selecting them on the basis of substantive and procedural requirements and correlating them to technical standards, assessing the advantages and disadvantages in detail.
- **Provide recommendations** (Article 43.8) based on point 2 for:
 - criteria for certifications (art. 42.5)
 - additional requirements for the accreditation of certification bodies
 - technical standards for certification and mechanisms to promote and recognize these certification mechanisms, seals and marks (article 43.9)
 - identification of any appropriate guarantees in relation to the transfer of personal data to third countries

Of these **117 schemes only 15 were selected** as a more in-depth case study.



ISDP©10003 Data Protection Certification

		Licensing	The scheme can be licensed. It has been licensed to 3 other certification bodies.
IDENTITY		Contract arrangement	Scheme licensing agreement A licensing agreement can be signed with another certification body authorizing this licensed body to use Inveo's requirements and ISDP©10003 seal under their own trademark. A License fee has to be paid to Inveo for every certificate issued.
Owner	Inveo srl		Assessment service contract The assessment process can be carried out under a separate agreement when done by an external auditor accredited by Inveo.
Country	Italy		Certification licensing agreement The certification is also subject to a licensing agreement signed between the certified organization and Inveo. The regulation of use ("Regolamento Generale") defines;
Creation date	2015		<ul style="list-style-type: none"> The user's and Inveo's obligations, Authorized and unauthorized use, License fees, Suspension and termination conditions and consequences, Dispute management process

* Final Report – GDPR Certification study (Annex 3)

All processes v. dedicated processes (tab. 3.4)

Several of the certifications that were analysed, certify all types of processes while half of them focus on dedicated processes and two schemes only certify the conformity to management systems dedicated to personal data.

	Certification scope models
All processes model The scheme applies to all process types	EuroPriSe, ISDP 10003:2015, JIPDEC PrivacyMark, Privacy by design certification Ryerson, Privacy-Audit-Proof, Privacy Seal MYOBI
Dedicated processes model The scheme applies to some dedicated processes included or not in a product range	BSI-BS 10012 (management systems) BSI- ISO/IEC 27018 (cloud processes) CNIL - ASIP Santé (Health data storage) Datenschutzaudit beim ULD (public processes) ePrivacy App (mobile app processes) TRUSTArc APEC CBPR (data transfers) TUV Italia - ISO/IEC 27001 certification (information security)

Multi-sector (or sector-neutral) vs single sector (tab. 3.5)

Several schemes claim a multi-sectoral coverage, offering certification of processes in all business activities, while some others focus on dedicated business activities.

	Certification scope models
Multi-sector model The scheme applies to all or certain processes in all business activities	EuroPriSe, ISDP 10003:2015, JIPDEC PrivacyMark, Privacy by design certification Ryerson, Privacy-Audit-Proof, Privacy Seal MYOBI, TRUSTArc APEC CBPR, TUV Italia - ISO/IEC 27001 certification
Single-sector model The scheme applies to one specific business activity	BSI- ISO/IEC 27018 CNIL Safebox, CNIL - ASIP Santé Datenschutzaudit beim ULD E-Privacy App IKeepSafe

All processes v. dedicated processes (tab. 3.7)





Several schemes have an international scope in the sense that they offer to certify entities established inside and outside the EU. Other certifications certify entities registered within the national territory of the scheme operator.

	Certification scope models
Subnational model The scheme applies within a subdivision of the national territory	Datenschutzaudit beim ULD
National model The scheme applies to a national territory	CNIL Safebox, CNIL - ASIP Santé, Datenschutzaudit beim ULD, IKeepSafe, (USA) JIPDEC PrivacyMark, (Japan) Privacy-Audit-Proof, TRUSTArc APEC CBPR (USA)
EU-wide model The scheme applies to all the EU Member States	BSI-BS 10012, BSI- ISO/IEC 27018, EuroPriSe, ISDP 10003:2015, Privacy by design certification Ryerson, TUV Italia - ISO/IEC 27001 certification.
International model The scheme applies worldwide or, at least, in the EU and outside the EU	BSI-BS 10012, BSI- ISO/IEC 27018, EuroPriSe, ISDP 10003:2015, Privacy by design certification Ryerson, TUV Italia - ISO/IEC 27001 certification.

All processes v. dedicated processes (tab. 3.8)

A Comprehensive model encompasses certifications certifying against the vast majority of provisions included in the GDPR or other data protection laws. On the other hand, a single-issue certification model encompasses the schemes certifying the conformity with a single or limited number of legal obligations in the regulation.

	Certification scope models
Dedicated GDPR provisions model ('single-issue') The scheme helps to demonstrate with specific GDPR provisions	BSI - ISO/IEC 27018 (Article 28) CNIL - SafeBox (Article 28) CNIL - ASIP Santé (Article 28) Privacy by design certification Ryerson (Article 25) TUV Italia - ISO/IEC 27001 certification (Article 32)
All GDPR model ('comprehensive') The scheme helps to demonstrate compliance with all GDPR provisions	BSI - BS 10012 Datenschutzaudit beim ULD E-Privacy App EuroPriSe ISDP 10003:2015

Scheme				
Benefits	<p>One-size-fits-all solution: The BSI BS 10012 is covering all facets of the GDPR in one scheme. This approach might be more efficient and cost-effective for SMEs</p> <p>Management system approach: The management system certification is less impacted by technological changes than process and product certification and this potentially more affordable for SMEs. Issuer legitimacy: BSI is a well-known and recognized certification body worldwide. GDPR readiness The scheme is active and the requirements have been updated to be aligned with the GDPR</p>	<p>ISO/IEC holistic approach: ISO/IEC 27001 standard also contributes to the ISO's holistic approach articulating security and privacy standardization within a consistent series of technical standards.</p> <p>Widespread adoption The ISO/IEC 27001 also leverages the businesses familiarity with the ISO vocabulary and approach following the ISO 9001 success. The ISO/IEC 27001 is progressively becoming a market standard increasingly required by IT buyers.</p>	<p>One-size-fits-all solution: ISDP©10003 is covering all facets of GDPR compliance in one scheme. This approach could be easier and cheaper for SMEs.</p> <p>Readiness: The scheme is active. The requirements are GDPR ready and have been recently translated in english.</p>	<p>One-size-fits-all solution: EuroPrise is covering all facets of GDPR compliance in one scheme. This approach could be easier and cheaper for small companies. The scheme also offers to both certify products and processes demonstrating that a holistic approach sounds sustainable.</p> <p>Coverage: EuroPrise is covering all facets of GDPR compliance in one scheme. This approach could be easier and cheaper for small companies. The scheme also offers to both certify products and processes demonstrating that a holistic approach sounds sustainable.</p>
Limits	<p>Management system certification The scheme certifying management systems are out of Article 42's scope</p> <p>Paying access: The standard is available upon payment</p>	<p>ISO/IEC holistic approach: Out of the GDPR's scope. Refers to management systems, out of Art. 42's scope</p> <p>Paying access: The standard is available with a fee</p>	<p>Paying access: The standard is available with a fee</p>	<p>Scalability: EuroPrise is covering all facets of GDPR compliance in one scheme. This approach could be easier and cheaper for small companies. The scheme also offers to both certify products and processes demonstrating that a holistic approach sounds sustainable.</p>
GDPR relevance	Art. 28	Art. 32	Art. 24	Art. 24/Art. 28
GDPR accordance	Out of the scope art. 42	Out of the scope art. 42	In scope art. 42	In scope art. 42
Accreditation	ISO/IEC 17021:2012 Management system	ISO/IEC 17021:2012 Management system	ISO/IEC 17065:2012 Product, process, services	ISO/IEC 17065:2012 Product, process, services

* synoptyc table of Annex by Osservatorio 679