EuroPriSe and ISDP©10003:2015

Certification models in scope of Art. 42 GDPR

Marco Moreschini

Osservatorio 679, SNE from Italian Ministry of Interior to the EU institutions

Certification as business card for accountability

Giovanni Buttarelli said in a **video-speech** on 22 January 2018 , spoke of

Certification is a business card for accountability.

He advised to "**treasure past good practices taking into account of the novelties"**.

ISO context, but also on national practices, moving towards a harmonization of experiences through the EDPB criteria.

Technologically neutral approach" so as to avoid market distortions and trust enhancers for consumers and users.

Clear criteria on who can accredit and certify

Sustainable criteria at European level + dialogue with the organizations involved in the world, such as the Consortium W3C and ISO.

Application of the certifications can make an **innovative contribution**, **create new skills and jobs** and compensate for the technological gap

Paramount to involve all the stakeholders, including the certification bodies.

OSSERVATORIO 679

General Methodology of the Commission Study

Quick Scan
117 schemes identified

- Full data protection
- Partly focusing on data protection
- Data protection related topics (cyber security)

Case studies
15 schemes selected

- BSI BS 10012 (UK)
- TÜV Italia ISO/IEC 27001
- BSI ISO/IEC 27018 (UK)
- Certificazione ISDP 10003:2015 Data protection (IT)
- Datenschutzaudit beim ULD (DE)
- E-privacy app (DE)
- EuroPrise (DE)
- IkeepSafe Coppa Safe Harbor (US)
- Label CNIL digital safe boxes (FR)
- Health Personal Data Storage Agreement (FR)
- Myobi Privacy Seal (NL)
- Norea Privacy-Audit-Proof (NL)
- PrivacyMark System (JP)
- Privacy by Design Certification Ryerson (CA)
- TrustArc APEC CBPR certification (US)

Case studies
8 themes analyzed

- Scope
- Normative criteria
- Scheme arrangements

--

- Conformity assessment
- Certification issuance
- Renewal
- Monitoring
- Sanction policy
- Complaint and dispute management

OSSERVATORIO 679

A privacy seal for Europe

- Project funding :1,3 Mio by EU
- July 2007 - February 2009
- 18 pilot projects
- Over 65 experts accredited
- Consortium: 9 partners from 8 EU Countries

ULD
Agencia de Protección de Datos de la Comunidad de Madrid APDCM
CNIL
LONDON metropolitan university HRSJ Human Rights & Social Justice Research Institute
ITA INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
TÜViT
ERNST & YOUNG
BORKING CONSULTANCY
VaF
OSSERVATORIO 679

From a small state to a EU wide certification

Deployment 1

- Responsible entity: Office of Data Protection Commissioner of Schleswig-Holstein (ULD), DE
- Location of Certification Authority (CA): Kiel, DE
- Time frame: 03/2009 – 12/2013

Deployment 2

- Responsible entity: EuroPriSe GmbH
- Location of Certification Authority: Bonn, DE
- Time frame: since 01/2014
- Approx. 110 admitted experts in 19 countries

IT products

- Hardware (e.g., an external hard disc drive secured by strong encryption methods)
- Software (e.g., a software module for obfuscation of video data or a fraud prevention software tool)

OSSERVATORIO 679

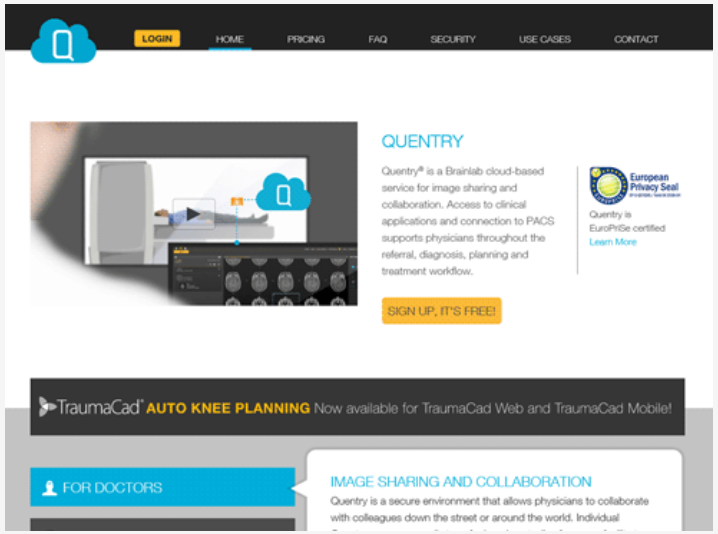
Europrise services

IT-based services

- Web-based services(e.g., a metasearch engine or a service for collaboration of medical professionals)
- Other services(e.g., a digitising service for photo negatives)

Websites (since 2016)

- Publicly accessible parts of a website (focus on interaction between website and website visitors)



OSSERVATORIO 679

Content of certifications – Targets of Evaluation

Cert. of IT products & IT-based services (controller services + processor services):

- The European Privacy Seal certifies that an IT product or IT-based service **facilitates the use** of that product or service in a way compliant with European regulations on privacy & data protection.

Cert. of websites:

- The seal certifies that data processing that results **from the interaction** between a visitor of a website and the website when the visitor browses publicly available parts of the websites **is compliant with European regulations** on privacy & data protection.

OSSERVATORIO 679

Key factors for trust

Trasparency:

- public criteria + procedure

Verifiability:

- publication of results

Credibility :

- reliability of auditors and recognition of certification bodies in DE

Compliance with General Data Protection principles

Technical-Organisational Measures: Accompanying Measures for Protection of the Data Subjects

Technology-specific and Service-specific Requirements

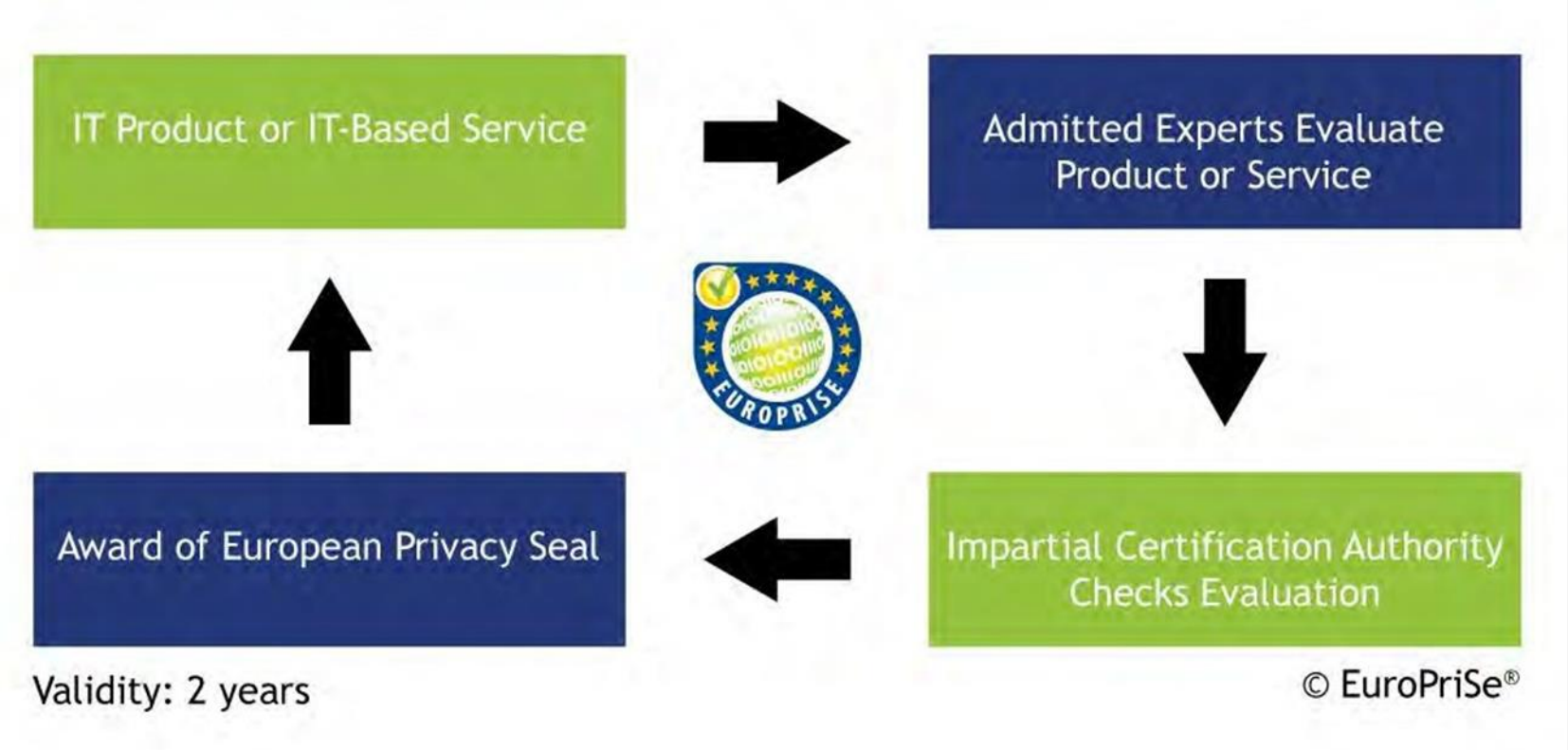
Data Subjects' Rights

Rights under the ePrivacy Directive

OSSERVATORIO 679

Key factors

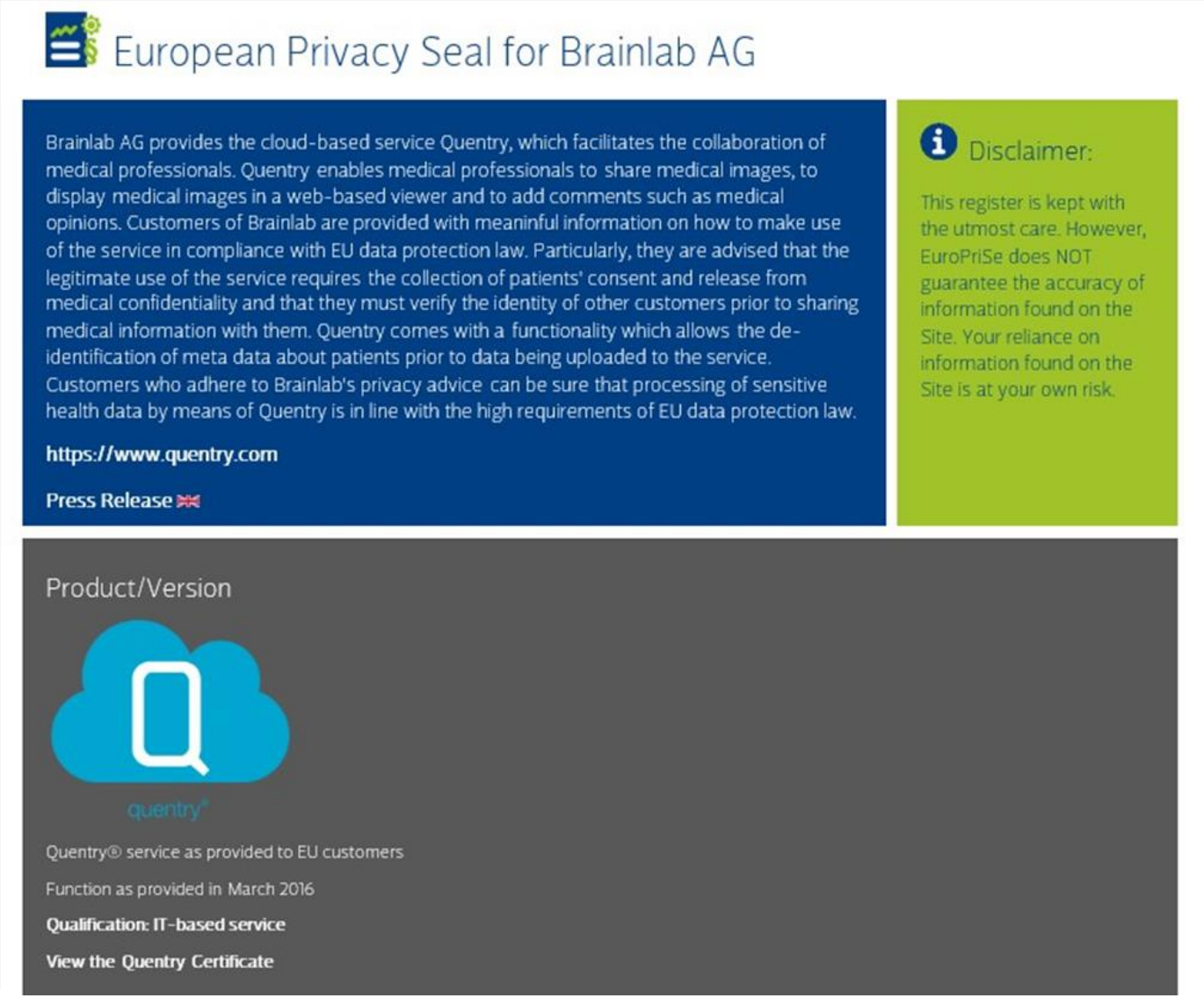
Procedure:



OSSERVATORIO 679

Key factors

Publication of results



OSSERVATORIO 679

Key factors : expertise of auditors

Mandatory accreditation (*note: not to be confused with art. 43 accreditation*) process called 'admission' managed by EuroPriSe board

· External auditor can be accredited on legal or/and technical audit side

· 1st step: Applicant self-declaration of probity and independence

· 2nd Step: Technical or/and legal exam from a use case

· The admission is granted for three years, renewable if the auditors conducted a EuroPriSe audit at least in this area in the meantime or if s/he followed an upgrade training proposed by EuroPriSe.

International high profile Advisory Board

OSSERVATORIO 679

International Scheme Data Protection ISDP©10003

Creation date: 2015

Certification released : 31

Licensed to three other Certification bodies

Updated to 2018

Geographical coverage International

Scope Processes and products

Sector Any, any organisation

Type Voluntary

Validity 3 years

Certification of processes for the protection of the physical person regarding personal data and the free circulation of said data.

Compatibility ISO HLS

- ISDP 10003 was developed using the rules specified in the ISO Annex SL Directives and follows the common structure to allow compatibility with the main ISO standards

OSSERVATORIO 679

What for

The scheme provides the principles and lines of control for a complete compliance assessment of the organisation's internal processes regarding protection of personal data with particular reference to proper risk management.

Additionally, it details security requirements and controls, so that the data respect the levels of precision, accuracy, timeliness, consistency, completeness, credibility and updating required by current regulations regarding the protection of personal data, with particular attention to the principles of quality and security of the data processed, in compliance with the main international standards.

OSSERVATORIO 679

Technical Structure ISDP©10003

A PROCESS APPROACH

ISDP©10003:2018	
Macro processes	7
Processes	20
Controls	96
Operational Check list	562

ISDP©10003:2018	
Macro-Processes	7
Policy and controller's obligations	1
Subjects involved in the processing operation	2
Principles applicable to the processing operation and data subjects rights.	3
Adjustment processes in the development, design and selection of product and service applications (privacy by design and by default)	4
General obligations and security of personal data	5
DPIA	6
Cloud and IoT management	7

OSSERVATORIO 679

Guidelines ISDP©10003

The scheme also represents an aid for all organizations that intend to make their standard operating procedures adequate without proceeding to certification
.

The certification of conformity through the ISDP scheme © 10003, does not reduce the responsibility of the data controller or of the person in charge of the processing operation, regarding the obligations of compliance with the data protection regulations

The organization that obtains ISDP certification © 10003, in relation to the processes, products and company services to which it is applicable ...

"(...) provides a guarantee to the interested parties of the adoption of a method of analysis and control of the principles and rules of reference to protect individuals with regard to the processing of personal data and the free movement of the same data".

HLS-ISDP©10003:2018

HLS - ISDP©10003:2018	
Introduction	§0
Scope and field of application	§1
Legal bases	§2
Glossary and definitions	§3
Context	§4
Awareness and accountability	§5
Planning (Sytstem review)	§6
Support	§7
Operational activities	§8
Performance evaluation	§9
Improvement	§10
Annex	98

Outcome - Certification models

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

Multi-sector v. Single-sector

	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

OSSERVATORIO 679

Outcome - Certification models

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)

OSSERVATORIO 679

Outcome - Certification models

International v. national and sub-national certifications

- 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.

International v. National

Subnational model
The scheme applies within a subdivision of the national territory

National model
The scheme applies to a national territory

EU-wide model
The scheme applies to all the EU Member States

International model
The scheme applies worldwide or, at least, in the EU and outside the EU

Certification scope

Datenschutzaudit beim ULD

CNIL Safebox,
CNIL - ASIP Santé,
Datenschutzaudit beim ULD,
IKeepSafe, (USA)
JIPDEC PrivacyMark, (Japan)
Privacy-Audit-Proof,
TRUSTe APEC CBPR (USA)

BSI-BS 10012,
BSI- ISO/IEC 27018,
EuroPriSe,
ISDP 10003:2015,
Privacy by design certification Ryerson,
TUV Italia - ISO/IEC 27001 certification.

BSI-BS 10012,
BSI- ISO/IEC 27018,
EuroPriSe,
ISDP 10003:2015,
Privacy by design certification Ryerson,
TUV Italia - ISO/IEC 27001 certification.

Outcome - Certification models

Single-issue certification v. Comprehensive certification	Certification scope models
Dedicated GDPR provisions model ('single-issue') The scheme helps to demonstrate with certain 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 EuroPrie ISDP10003 2015

Certifications based on international standards seem to follow ISO/IEC's approach that is encouraging a dedicated/sectoral approach, while European schemes seem to prefer a more generic all-encompassing model.

Two opposing models

- On the one hand, 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.

OSSERVATORIO 679

Outcome - Certification models

Legal framework
v.
Standard
v.
Combined

	Normative criteria
Normative basis: law The scheme is based on a legal framework (EU or non-EU one)	CNIL Safebox, CNIL - ASIP Santé, Datenschutzaudit beim ULD E-Privacy App, EuroPriSe, IKeepSafe (US) ISDP 10003:2015, Privacy by design certification Ryerson, Privacy Seal MYOBI, Privacy-Audit-Proof
Standard model The scheme is based on a standard issued by a national or an international standardization body	BSI -BS 10012, BSI- ISO/IEC 27018, JIPDEC PrivacyMark, TUV Italia - ISO/IEC 27001 certification
Combined model The schemes both refer to a regulation and to one or several other(s) normative basis (Technical standard(s) or and code of conduct)	BSI -BS 10012, BSI- ISO/IEC 27018, E-Privacy App, ISDP 10003:2015, Privacy by design certification Ryerson, TUV Italia - ISO/IEC 27001 certification

In scope of Art.42

Because already accredited for certification for process, service and product having been accredited for 17065 2012 and in line with the requirements of Art. 43.1.b).

Scheme	BS 10012 Data Protection	TÜV SÜD ISO 27001	ACCREDIA ISDP©10003	European Privacy Seal
Benefits	**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 **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	**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. **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.**	**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. **Readiness:** The scheme is active. **The requirements are GDPR ready and have been** recently translated in english.	**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. **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.
Limits	**Management system certification** The scheme certifying management systems are out of Article 42's scope **Paying access:** The standard is available upon payment	**ISO/IEC holistic approach:** Out of the GDPR's scope. Refers to management systems, ou of Art. 42 's scope **Paying access:** The standard is available with a fee	**Paying access:** The standard is available with a fee	**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.
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

Certification 17065 vs 17021

ISO 17021-1ISO/IEC 17021-1:2015 -Conformity assessment — Requirements for bodies providing audit and **certification of management systems**

- Ensures the company's ability to organise itself and manage internal resources and processes in order to meet customer needs
- Usable as best practice
- Partially referred to in the GDPR (Art. 32)

Principles and requirements for the competence, consistency and impartiality of the audit and certification of **management systems of ALL types** and for the bodies providing these activities

Management system – system to establish policy and objectives and to achieve those objectives

ISO/IEC 17065:2012 Conformity assessment — Requirements for bodies certifying products, processes and services.

- The overall aim of certifying products, processes or services is to give confidence to all interested parties that a product, process or service fulfils specified requirements. The value of certification is the degree of confidence and trust that is established by an impartial and competent demonstration of fulfilment of specified requirements by a third party.
- Certification of products, processes or services is a means of providing assurance that they comply with specified requirements in standards and other normative documents.
- It specifies requirements, the observance of which is intended to ensure that certification bodies operate certification schemes in a competent, consistent and impartial manner, thereby facilitating the recognition of such bodies and the acceptance of certified products, processes and services on a national and international basis and so furthering international trade.
- This International Standard can be used as a criteria document for accreditation or peer assessment or designation by governmental authorities, scheme owners and others

OSSERVATORIO 679