



Data Protection Certification Mechanisms

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

**Final Report
Annexes**

Justice and
Consumers

Authors: Irene Kamara, Ronald Leenes, Eric Lachaud, Kees Stuurman (TILT), Marc van Lieshout, Gabriela Bodea (TNO)

Contributors: Camille Salinier, Kris Best (CIVIC Consulting), Mirell Piir, Magdalena Brewczyńska (TILT)

ISBN: 978-92-76-01377-8 DOI:10.2838/115106

© European Union, and the authors 2019. All rights reserved. Reproduction is authorised provided the source is acknowledged.

Table of Contents

Annex 1 Glossary	4
Annex 2 Overview of existing certifications in data protection.....	12
Annex 3 Factsheets per analysed certification	17
Annex 4 Accreditation survey	98
Annex 5A Stakeholder survey	126
Annex 5B Overview of additionally relevant standards	176
Annex 6 Workshop Reports	188

Annex 1 Glossary

1. Aim and methodological approach

The aim of this glossary is to provide clarity and ensure consistency in the use of terms regularly encountered in certification mainly for the purposes of this study. Given the lack of definitions of the terms related to certification mechanisms in the General Data Protection Regulation, the Glossary may also provide a basis for establishing a common understanding of the terminology for entities engaged with the GDPR certification mechanisms.

The first step in building the Glossary was the identification of existing technical standards of ISO and IEC on conformity assessment activities, which are adopted as European standards. In addition, relevant EU Legislation, such as the Regulation 1025/2012 on standardization and the Regulation 765/2008, was also analysed. The second step in developing this Glossary was to compile the terms used in Articles 42 and 43 GDPR, and other certification-related GDPR Articles. The third step was a matching exercise of all the GDPR terms, as they may be interpreted in light of Art. 42 and 43 GDPR, and the terms identified in Step 1. The outcome is presented in the following Table (1). It should be noted that when there is a conflict or differentiation in the meaning of a term, as implied in the GDPR, and a term as used in the ISO and IEC conformity assessment standards and the aforementioned legislation, the latter is preferred. In case of conflict, the GDPR approach and interpretation of the term is preferred, which is appropriate for the aims of this study. The terms are presented in alphabetical order.

2. Certification Glossary

Term	Definition	Source	GDPR equivalent
accreditation	an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectorial schemes, to carry out a specific conformity assessment activity	R765/2008 art. 2(10)	attestation by a national accreditation body or a supervisory authority (art. 43 GDPR)
accreditation body	authoritative body that performs accreditation Note: The authority of an accreditation body is generally derived from government.	EN ISO/IEC 17011	Art. 43 GDPR: a national accreditation body or a supervisory authority

accreditation symbol	symbol issued by an accreditation body to be used by accredited conformity assessment bodies to indicate their accredited status Note: "Mark" is to be reserved to indicate direct conformity of an entity against a set of requirements.	EN ISO/IEC 17011	-
CE marking	marking by which the manufacturer indicates that the product is in conformity with the applicable requirements set out in Community harmonisation legislation providing for its affixing	R765/2008 art. 2(20)	-
certification	third-party attestation (related to products, processes, systems or persons) 1. Note 1: Certification of a management system is sometimes also called registration. 2. Note 2: Certification is applicable to all objects of conformity assessment except for conformity assessment bodies themselves, to which accreditation is applicable. ¹	EN ISO/IEC 17000:2004	third party certification of processing operations (art. 42(1)) GDPR ²
certification scheme	Certification system related to specific processing operation, to which the same specified requirements, specific rules and procedures apply. Note: The rules, procedures and management for implementing product, process and service certification are stipulated by the certification scheme.	EN ISO/IEC 17067:2013, adapted	data protection certification mechanism
certification body	third-party conformity assessment body operating certification schemes, including monitoring, complaints' handling, and withdrawal of certifications	EN ISO/IEC 17065:2012 (adapted)	third-party conformity assessment body accredited by National Accreditation Authority or supervisory authority
Certification requirement	Specified requirement, including product requirements that is fulfilled by the client as a condition of establishing or maintaining certification. Note: Certification requirements include requirements imposed on the client by the certification body [usually via the certification agreement] to meet the International Standard, and can also include requirements imposed on the client by the certification scheme.	EN ISO/IEC 17065:2012	Both 42(5) and 43 criteria and requirements

¹ Requirements relevant to accreditation are referred to as "accreditation requirements" in the study.

² The scope of certification in Art. 42 and 43 GDPR is different than the scope of certification in line with the ISO/IEC standards. In this study, we follow the GDPR scope, unless indicated otherwise.

complaint	expression of dissatisfaction, other than appeal, by any person or organization to a conformity assessment body or accreditation body (2.6), relating to the activities of that body, where a response is expected	EN ISO/IEC 17000:2004	-
conformity assessment	the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled	R765/2008 art. 2(12)	-
conformity assessment body	a body that performs conformity assessment activities including calibration, testing, certification and inspection	R765/2008 art. 2(13)	-
Equal national treatment	treatment accorded to products or processes originating in other countries that is no less favourable than that accorded to like products or processes of national origin, or originating in any other country, in a comparable situation	EN ISO/IEC 17000:2004	-
equivalence of conformity assessment results	sufficiency of different conformity assessment results to provide the same level of assurance of conformity with regard to the same specified requirements	EN ISO/IEC 17000:2004	-
European standard	standard adopted by a European standardisation organisation	R1025/2012 art/. 2(1)(b)	-

European standardisation deliverable	any other technical specification than a European standard, adopted by a European standardisation organisation for repeated or continuous application and with which compliance is not compulsory	R1025/2012 art. 2	-
European standardisation organisation	1. CEN — European Committee for Standardisation 2. CENELEC — European Committee for Electrotechnical Standardisation 3. ETSI — European Telecommunications Standards Institute	Annex I R1025/2012	-
harmonised standard	European standard adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation	R1025/2012 art./ 2(1)(c)	-
International standard	a standard adopted by an international standardisation body	R1025/2012 art.2(1)(a)	-
international standardisation body	International Organisation for Standardisation (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU)	R1025/2012 art.2(9)	-
national accreditation body	the sole body in a Member State that performs accreditation with authority derived from the State	R765/2008 art. 2(11)	Same meaning within the GDPR, with the differentiation that the National Accreditation Body is not the sole body performing accreditation (Art.43 GDPR)

national standardisation body	body notified to the Commission by a Member State in accordance with Article 27 of this Regulation	R1025/2012 art. 2(10)	-
National standard	a standard adopted by a national standardisation body	R1025/2012 art. 2(1) (d)	-
peer evaluation	process for the assessment of a national accreditation body by other national accreditation bodies, carried out in accordance with the requirements of this Regulation, and, where applicable, additional sectoral technical specifications	R765/2008 art. 2(16)	-
recognition	Recognition of conformity assessment results acknowledgement of the validity of a conformity assessment result provided by another person or body	EN ISO/IEC 17000:2004	-
(product/process/system) requirement	Requirement that relates directly to a product/process/system specified in standards or in other normative documents identified by the certification scheme. NOTE: Product requirements can be specified in normative documents such as regulations, standards and technical specifications.	EN ISO/IEC 17065:2012	certification criterion Note: different scope than the ISO/IEC standard. Limited to processing operations
Scheme owner	Person or organization responsible for developing and maintaining a specific certification scheme.	EN ISO/IEC 17065:2012	-
scope of certification	identification of the product(s), process(es) or service(s) for which the certification is granted, the applicable certification scheme, and the standard(s) and other normative document(s), including their date of publication, to which it is judged that the product(s), process(es) or service(s) comply	EN ISO/IEC 17065:2012	The GDPR has a more narrow scope: processing activities (see Chapter 2 of the study)

standard	<p>technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory, and which is one of the following:</p> <p>(a) 'international standard' means a standard adopted by an international standardisation body;</p> <p>(b) 'European standard' means a standard adopted by a European standardisation organisation;</p> <p>(c) 'harmonised standard' means a European standard adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation;</p> <p>(d) 'national standard' means a standard adopted by a national standardisation body</p>	R1025/2012 art.2(1)	-
surveillance	<p>systematic iteration of conformity assessment activities as a basis for maintaining the validity of the statement of conformity</p>	EN ISO/IEC 17065:2012	-
technical specification	<p>document that prescribes technical requirements to be fulfilled by a product, process, service or system and which lays down one or more of the following:</p> <p>(a) the characteristics required of a product including levels of quality, performance, interoperability, environmental protection, health, safety or dimensions, and including the requirements applicable to the product as regards the name under which the product is sold, terminology, symbols, testing and test methods, packaging, marking or labelling and conformity assessment procedures;</p> <p>(b) production methods and processes used in respect of agricultural products as defined in Article 38(1) TFEU, products intended for human and animal consumption, and medicinal products, as well as production methods and processes relating to other products, where these have an effect on their characteristics;</p> <p>(c) the characteristics required of a service including levels of quality, performance, interoperability, environmental protection, health or safety, and including the requirements applicable to the provider as regards the information to be made available to the recipient, as specified in Article 22(1) to (3) of Directive 2006/123/EC;</p> <p>(d) the methods and the criteria for assessing the performance of construction products, as defined in point 1 of Article 2 of Regulation (EU) No 305/2011 of the European Parliament and of the Council of 9 March 2011 laying down harmonised conditions for the marketing of construction products (1), in relation to their essential characteristics;</p>	R1025/2012 art.2(4)	-

third-party mark of conformity	protected mark issued by a body performing third-party conformity assessment, indicating that an object of conformity assessment (product, process, person, system or body) is in conformity with specified requirements EXAMPLES Third-party marks of conformity can be: product certification marks, quality/environment management system certification marks, environmental conformity marks, etc. NOTE 1 A protected mark is a mark legally protected against unauthorized use. NOTE 2 The specified requirements are generally stated in "normative" documents such as International Standards, regional or national standards, regulations and specifications.	EN ISO/IEC 17030:2013	mark or data protection certification mark
withdrawal	revocation cancellation of the statement of conformity	EN ISO/IEC 17000:2004	same meaning for withdrawal of certification- Art. 42(7) GDPR

Table 1.1 Glossary of certification and accreditation terms

3. Glossary for GDPR-specific terms on certification

Term	Description	Provision
Assessment	Evaluation conducted by an accredited certification body or a supervisory authority with a view to award a data protection certification or to withdraw awarded data protection certification.	43(4) GDPR
Additional requirements	requirements established by the competent supervisory authority and against which an accreditation is performed ³ (See Chapter 5 of the study)	43(1), (6) GDPR
Certification procedure	The procedure conducted by an accredited certification body or a supervisory authority (including assessment, granting, issuance) in response to an application of a data controller or a processor for data protection certification.	42(6) GDPR
Common certification	See European Data Protection Seal	42(5) GDPR
Criteria	criteria' or certification criteria shall mean the criteria against which a certification (conformity assessment) is performed ⁴	42(5)
Data Protection Certification	The attestation granted by an accredited certification body or a supervisory authority in line with Art. 42 and 43 GDPR to a successful applicant controller or processor in relation to one or more data processing activities following an evaluation and a decision based	Multiple GDPR provisions

³ EDPB, Guidelines on Accreditation, 4/2018, p.5

⁴ EDPB, Guidelines on Accreditation, 4/2018, p.5

	on approved certification criteria.	
Data Protection Certification Mechanism	The mechanism in line with Art 42 and 43 GDPR which describes the approved certification criteria, the assessment methodology, the certification process and other organisational/procedural arrangements including complaint handling and non-conformities.	Multiple GDPR provisions
Data Protection Mark	See mark of conformity in table 1 of this Annex. Note: the data protection mark is granted by an accredited certification body or a supervisory authority in line with Art. 43 GDPR	Multiple GDPR provisions
Data Protection Seal	The seal granted to an applicant controller or processor, following a successful evaluation and decision of its processing activity (-ies) based on approved certification criteria. The visual representation of a granted data protection certification	42(1), 42(2), 43(1)(c) GDPR
European Data Protection Seal	Data Protection Seal, the certification criteria of which are approved by the European Data Protection Board.	42(5) GDPR
Grant (certification)	The decision of an accredited certification body or a supervisory authority following a positive assessment.	43(5) GDPR
Issue (accreditation)	The stage of the accreditation procedure following the granting of accreditation. It entails the awarding of the accreditation to the certification body.	43(4) GDPR
Issue (certification)	The stage of the certification procedure following the granting of certification. It entails the awarding of the certification to the controller or processor, and its right to use the data protection seal and/or mark.	42(5), 42(7), 43(1) GDPR
Renew (certification)	The renewal of certification after the passage of three years period provided that the requirements continue to be met.	42(7), 43(1) GDPR
Revoke (accreditation)	The act of withdrawal of granted certification before the expiry period of the certification, due to the fact that the conditions for granting the certification are no longer met.	Art. 43(7)
Technical rules and Methods and procedures for the certification bodies	Conformity assessment standards	Art. 43(3)

Table 1.2 Glossary of GDPR-specific terms related to certification and accreditation

Annex 2 Overview of existing certifications in data protection

Zertifizierter Datenschutz	ICG Zertifizierung GmbH	Germany	PII Management System	
Website TrustLogo	Comodo Group	USA	Process security	Website
Webassured	WebAssured	USA	Processes	Website
VeraSafe Privacy Shield Certification	VeraSafe	USA	Processes	International data flows
Unified Capabilities Approved Products List	Corsec Security, Inc.	USA	Product security	
Trygg e-Handel	Svensk Digital Handel	Sweden	Processes	E-Commerce
Trusted Site Privacy	TÜV Informationstechnik	Germany	Processes	Website
Trusted Shops	Trusted Shop GmbH	Germany	Processes	E-Commerce
Trusted Cloud Datenschutzprofil	TÜV Informationstechnik	Germany	Processes	Cloud
MedCom	Danish Government	Denmark	Processes	Health PII
TRUSTe Enterprise Privacy	TrustArc	USA	Processes	
TRUSTe Children's Privacy Certification	TrustArc	USA	Products and processes	Website/app/ game
TRUSTe APEC CBPR	TrustArc	USA	Processes	International data flows
Thuiswinkel	Nederlandse Thuiswinkel Organisatie	The Netherlands	Processes	E-Commerce
Tacticx Datenschutz Siegel	Tacticx GmbH	Germany	Products and processes	
SwissDRG certification	Federal Data Protection and Information Commissioner (FDPIC)	Switzerland	Processes	Health PII
Smart Card Testing and Certification	Ministry of Electronics & Information Technology	India	Products	Smart Card
Service Providers with Certified Data Privacy Management	TÜV Rheinland	Germany	Processes	
Produits certifiés SSCD	Agence Nationale de la Sécurité des Systèmes d'Information (ANSI)	France	Product security	Electronic signature
Produits Certifiés Conformes PSC	Agence Nationale de la Sécurité des Systèmes d'Information (ANSI)	France	Product security	Encryption
ISO/IEC 15408 CC Certification	Agence Nationale de la Sécurité des Systèmes d'Information (ANSI)	France	Product security	
iKeepSafe COPPA Safe Harbor Certification	iKeepSafe	USA	Products and processes	Website/app/ game
Privacy Shield	International Trade Administration (ITA)	USA	Processes	International

				data flows
E-privacy seal	E-privacy GmbH	Germany	Products and processes	
Privacy Safe Trust seal	Trust Guard	USA	Processes	Website
Fair Data	Market Research Society	UK	Processes	
Payment Card Industry Data Security Standard (PCI-DSS)	Banking Industry Consortium	USA	Processes	Financial services
NF S 96-900 Certification	AFNOR	France	Management system for biological resource centers	Bio-Bank resources
PrivacyMark System	JIPDEC	Japan	PII Management System	
McAfee Secure	McAfee	USA	Processes	Website
Label CNIL Safe box	CNIL- French Data Protection Commissioner	France	Products	e-Safebox
Label CNIL Data Protection Training Programmes	CNIL- French Data Protection Commissioner	France	Processes	Training
Label CNIL Data Governance	CNIL- French Data Protection Commissioner	France	PII Management System	
TRUSTe Smart Grid Privacy Certification	TrustArc	USA	Products and processes	SmartGrid
kidSAFE Seal Program	Samet Privacy	USA	Products and processes	Website/app/game
Keurmerk Particulier onderzoeksbureau	Vereniging van Particuliere Beveiligingsbureaus (VPB) Dutch private investigators Association	The Netherlands	Processes	Private investigations
ISO/IEC 27018 Certification	Datenschutz cert GmbH	Germany	PII Management System	Cloud
Privacy Seal	Mind Your Own Business Information	The Netherlands	Processes	Cloud
ISO/IEC 27018 certification	AFNOR	France	PII Management System	Cloud
ISO/IEC 27001 Certification	Certiquality s.r.l	Italy	IT Security Management System	
ISO/IEC 27001 Certification	British Standardization Institution (BSI)	UK	IT Security Management System	
ISO/IEC 27001 certification	AFNOR	France	IT Security Management System	
Privacy by design certification	Ryerson University	Canada	Products and processes	
ISO/IEC 27001 Certification	Bureau Veritas Italia S.p.A.	Italy	IT Security Management System	
ISO/IEC 27001 certification	Duijnborgh Audit BV	The Netherlands	IT Security Management System	
ISO/IEC 20000 Certification	Certiquality s.r.l	Italy	Processes	IT services
ISO/IEC 20000 Certification	Bureau Veritas	France	Processes	IT services

Label CNIL Audit procedures	CNIL- French Data Protection Commissioner	France	Processes	
ISO/IEC 15408 Certification	Corsec Security, Inc.	USA	Product security	
ISO 9001 Certification	Certiquality s.r.l	Italy	Quality Management System	
ISO 9001 certification	AFNOR	France	Quality Management System	
ISDP 10003:2015 Data protection	Inveo srl	Italy	PII Management System	
ISASecure System Security Assurance (SSA) Certification	ISA Security Compliance Institute (ISCI)	USA	IT Security Management System	Industrial Control Systems
ISASecure Security Development Lifecycle Assurance (SDLA) Certification	ISA Security Compliance Institute (ISCI)	USA	IT Security Management System	Industrial Control Systems
ISASecure Embedded Device Security Assurance (EDSA) Certification	ISA Security Compliance Institute (ISCI)	USA	IT Security Management System	Industrial Control Systems
Irish Ecommerce Trustmark	Retail Excellence	Ireland	Processes	E-Commerce
Bio-metric Devices Testing and Certification	Ministry of Electronics & Information Technology	India	Products	Biometric devices
High Assurance evaluation	Australian Signals Directorate	Australia	Product security	
Health Insurance Company with Certified Data Privacy Management	TÜV Rheinland	Germany	Processes	Health PII
Health PII Data Storage Companies (Agrément des hébergeurs de santé de données personnelles)	French Health Ministry/CNIL	France	PII Management System	Health PII
Good Priv@cy	Swiss Association for Quality and Management Systems (SQS)	Switzerland	PII Management System	
FIPS 140-2 Certification	Corsec Security, Inc.	USA	Product security	
FINCSC - Finnish Cyber Security Certification	Finnish Cyber Security Certificate (FINCSC) Businesses.	Finland	IT Security Management System	
FERPA Certification	iKeepSafe	USA	Products and processes	Website/app/game
PRIVO-Cert	Privo	USA	Products and processes	Website/app/game
Datenschutzaudit beim ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)	Germany	PII Management System	Public bodies
EuroCloud Star Audit Certification	EuroCloud Europe	Germany	Processes	Cloud
Euro-Label	EHI Retail Institute GmbH	Germany	Processes	E-Commerce
ESRB Privacy Certified	Entertainment Software Rating Board	USA	Processes	Website/app/game


EMOTA European ecommerce Trustmark	European eCommerce and Omni-Channel Trade Association	EU	Processes	E-Commerce
EDAA-OBA Certification	E-privacy Consult GmbH	Germany	Processes	Digital advertisement
E-VOTE	Fédération des Tiers de Confiance (FNTC)	France	Products and processes	Electronic voting
BS 10012 Personal Information Management System	British Standardization Institution (BSI)	UK	PII Management System	
E-privacy App	E-privacy Consult GmbH	Germany	Products	App software
E-market	E-mærket	Denmark	Processes	E-Commerce
DPMS 44001: 2016	Know How Certification S.r.l. (KHC)	Italy	PII Management System	
DPCO:2014	Swiss Association for Quality and Management Systems (SQS)	Switzerland	PII Management System	
DESAG Zert Datenschutz Gütesiegel	DESAG Zert GmbH	Germany	PII Management System	
Datenschutzgütesiegel Interaktiver Handel	Datenschutz cert GmbH	Germany	Processes	Shopping Online
ISO/IEC 27018 Certification	British Standardization Institution (BSI)	UK	PII Management System	Cloud
Datenschutz-Gütesiegel beim ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)	Germany	Products and processes	Public bodies
Datenschutz Zertifizierung	IITR Institut für IT-Recht GmbH	Germany	Products and processes	
Datenschutz Zertifizierter	Inois Institut für organisatorische Informationssysteme	Germany	Processes	
Data protection audit certificate	Hungarian Data Protection Authority (NAIH)	Hungary	Processes	
Cyber Essentials PLUS	IASME Consortium	UK	IT Security Management System	SMEs
Cyber Essentials PLUS	UK Government	UK	IT Security Management System	SMEs
Confianza Online	Adigital et Autocontrol	Spain	Processes	E-Commerce
ISO/IEC 27001 Certification	APAVE Certification Italia S.r.l.	Italy	IT Security Management System	
CISPE Data ProtectionTrust Mark	Cloud Infrastructure Services Providers in Europe (CISPE)	France	PII Management System	Cloud
Certification de Sécurité de Premier Niveau (CSPN)	Agence Nationale de la Sécurité des Systèmes d'Information (ANSI)	France	Product security	
CBPR certification	JIPDEC	Japan	Processes	International data flows
Card Payment TrustLogo	Comodo Group	USA	Process security	Financial services

California Student Privacy Certification	iKeepSafe	USA	Products and processes	Website/app/ game
buySAFE Guaranteed Shopping	buySAFE	USA	Processes	E-Commerce
Bureau Veritas GDPR Certification	Bureau Veritas	France	PII Management System	
Company with Certified Data Privacy Management	TÜV Rheinland	Germany	PII Management System	
EuroPriSe	EuroPriSe Gmbh	Germany	Products and processes	
Binding Corporate Rules	EU Commission	EU	Processes	International data flows
BeCommerce	BeCommerce	Belgium	Processes	E-Commerce
BBBonline	Council of Better Business Bureaus	USA	Processes	Website
BBB EU Privacy Shield	Council of Better Business Bureaus	USA	Processes	
Basic level cyber essentials	IASME Consortium	UK	IT Security Management System	SMEs
Australasian Information Security Evaluation Program (Aisep)	Australasian Certification Authority (ACA)	Australia	Product security	
ASML - Data & Marketing Association of Finland	Data & Marketing Association of Finland	Finland	Processes	E-Commerce
ASD Cryptographic Evaluation	Australian Signals Directorate	Australia	Product security	Encryption
ANSI/TIA-942 Compliance Certification	Enterprise Products Integration Pte Ltd	Singapore	Products and processes	Data Center
a.s.k. websecure	a.s.k. Datenschutz	Germany	Processes	Website
a.s.k. external data protection	a.s.k. Datenschutz	Germany	PII Management System	
a.s.k. companysecure	a.s.k. Datenschutz	Germany	PII Management System	
Privacy-Audit-Proof	Norea	The Netherlands	Products and processes	
Europrivacy	Europrivacy	Switzerland	Processes	
Appytest	Appytest	Spain	Products and processes	Mobile apps
Re-identification Risk Determination (RRD)	Privacy Analytics	Canada	Processes	Health PII
Re-identification Risk Determination and Anonymization (RRDA)	Privacy Analytics	Canada	Processes	Health PII
Conceptual Re-identification Risk Determination (CRRD)	Privacy Analytics	Canada	Processes	Health PII
Certificación en materia de protección de datos personales	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales	Mexico	Processes	
POPI Certified Seal	Michalsons Compliance Programme	South Africa	PII Management System	

Table 2 Existing certifications in data protection⁵⁵ The information is up-to-date until 15th September 2017.

Annex 3 Factsheets per analysed certification

1. BSI - BS 10012 Personal Information Management System

<p>BSI BS 10012 Personal Information Management System</p>	
IDENTITY	
Owner	BSI Assurance Ltd
Country	United Kingdom
Creation date	2017
No. of certifications issued	No information
List of certified entities	<p>The public directory is accessible online on BSI's website https://www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/</p>
Licensing policy	No
Contract arrangement	No information
Geographical coverage	International
Scope	Management system certification
	<p>The scheme focuses on governance. It specifies requirements for a personal information management system (PIMS), which provides a framework for maintaining and improving compliance with data protection requirements and good practice.</p> <p>It is intended to be used by those responsible for planning, establishing, implementing and maintaining a PIMS within an organization.</p> <p>It provides a common ground for the responsible management</p>

	<p>of personal information, for providing confidence in its management, and for enabling an effective assessment of compliance with data protection requirements and good practice by both internal and external assessors.</p> <p>The scheme is applicable to all sizes and types of organizations (public, private, governmental, non-profit).</p>
Sector	Any
Type	Voluntary
Validity	3 years
Costs	Cost regarding the process of certification process (initial audit and renewal) and the periodical fees differ case-by-case and are available upon request only.
Website	https://www.bsigroup.com/en-GB/BS-10012-Personal-information-management/
FUNCTIONING	
Foundations	The BS 10012 standard is based on UK data protection law and has been recently updated with the requirements included in the General Data Protection Regulation (GDPR)
	The standard is available upon payment
Requirements	<p>The BS 10012 standard contains the following mechanisms:</p> <ul style="list-style-type: none"> • Plan for the implementation of a PIMS that can support compliance with the data protection requirements • Leadership and commitment • Policy • Organisational roles, responsibilities and authorities • Embedding the PIMS in the organization’s culture • Planning: <ul style="list-style-type: none"> • to address risks and opportunities (includes legal basis for processing art. 6 GDPR, PIAs) • PIMS objectives and planning to achieve them • Support: resources, competence, awareness, communications, documentation • Operational planning and control • Implementing the PIMS • Performance evaluation • Monitoring, measurement, analysis and evaluation

	<ul style="list-style-type: none"> • Internal audit, management review • Improvement (non-conformities and corrective actions)
Assessors	Internal auditors
	BSI is accredited as organisation against the ISO 17021:2015 Conformity assessment - Requirements for bodies providing audit and certification of management systems
Process	Third party certification
	<p>Assessment process</p> <p>BSI receives the application and appoints a client manager to guide the applicant through the process steps:</p> <ol style="list-style-type: none"> 1. Gap analysis Optional pre-assessment service offering a closer look at the existing system and compare it with the BS 10012 requirements. 2. Readiness review Stage 1 audit consisting of reviewing the organization's preparedness for assessment by checking if BS 10012 procedures and controls have been developed. 3. Formal assessment Stage 2 audit: if all the requirements are in place, BSI assesses the implementation of the procedures within an organization (gathering information, testing compliance and effectiveness of measures etc.) to make sure that fulfils certification requirements.
	<p>Certification issuance</p> <ul style="list-style-type: none"> • BSI issues the certification after having reviewed the audit report • A seal is issued to the certified body • The name, address, status, name of standard and scope are published online
Renewal	Renewal on request at the end of the validity period
	Full assessment process according to the same process than the initial certification process


Monitoring	<p>BSI assigns a client manager to carry out ongoing assessments to support the continual improvement activities of the certified party.</p> <p>A surveillance audit (for maintenance purposes) is conducted by BSI on a yearly basis to ensure continuity of compliance.</p> <p>If minor or major non-conformities are found, the client will be helped to improve them.</p> <p>BSI is also allowed to conduct short notice audits or unannounced audits if there is evidence that the client is no longer in compliance.</p> <p>The client has an obligation to notify BSI in a timely manner if certain changes take place in management, organization structure, incidents such as breaches occur, etc.</p>
Suspension/Withdrawal	<p>BSI may suspend a certificate if the compliance with the standard is no longer met; if the client refuses to provide additional information as required by BSI (e.g. changes in management, changes in the structure of the organization, expansion of activities, data breaches etc.)</p> <p>Under suspension, the certification of a client's management system is invalid until the suspension is lifted. Such suspension will be made clear on the BSI client directory.</p>
Guarantees	No
Complaint handling	<p>Complaints should be submitted in writing, to the Regional Managing Director of the BSI office in the country where the person lodging the complaint resides.</p> <p>The person lodging the complaint will be kept informed of progress. BSI will reply as soon as the complaint has been fully investigated.</p> <p>Complaints about a registered or verified assertion client should also be submitted in writing.</p> <p>Having confirmed that the subject client is registered by BSI , BSI will ensure that they are taking appropriate action and confirm how the issue has been dealt with during a subsequent audit or verification of the client. For this reason, these complaints may take longer to fully resolve.</p>
Dispute resolution process	<p>A certified body with a disagreement concerning the decision of his certification or verification unable to resolve either through his Client Manager/Auditor/Verifier, or with the local management of his BSI office, may appeal in writing within 21 days from receipt of the decision to the Head of Compliance & Risk of the BSI office in his country.</p> <p>Selected BSI personnel will be appointed who are independent</p>

	<p>of the appealed issue. Contact will be made to acknowledge receipt of the appeal, outline the appeals process, gather and verify additional data and information required.</p> <p>The results of the appeal decision will be communicated formally.</p>
--	--

ANALYSIS	
GDPR relevance	Article 24
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 thus potentially more affordable for SMEs.</p> <p>Issuer legitimacy: BSI is a well-known and recognized certification body worldwide.</p> <p>GDPR readiness The scheme is active and the requirements have been updated to be aligned with the GDPR</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>
Evolution and Improvement	-

Table 3.1 BSI - BS 10012 Personal Information Management System

2. BSI - ISO/IEC 27018 - Protection of Personally Identifiable Information

<p align="center">BSI ISO/IEC 27018 - Protection of Personally Identifiable Information</p>	
IDENTITY	
Owner of the scheme	BSI Assurance Ltd
Country	United Kingdom
Creation date	2014
No. of certifications issued	No information
List of certified entities	<p>Accessible online https://www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/</p>
Licensing policy	No
Contract arrangement	No information
Geographical scope	International
Scope	Management system
	<p>According to the ISO, the "ISO/IEC 27018" revised in 2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.</p> <p>In particular, ISO/IEC 27018:2014 specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which might be applicable</p>

	<p>within the context of the information security risk environment(s) of a provider of public cloud services."</p> <p>The scheme is applicable to all sizes of organizations (public, private, governmental, non-profit).</p>
Sector	Cloud service providers
Type	Voluntary
Validity	3 years
Costs	Cost regarding the process of certification process (initial audit and renewal) and the periodical fees differ case-by-case and are available upon request only.
Website	https://www.bsigroup.com/en-GB/ISO-IEC-27018/
FUNCTIONING	
Foundations	<p>The ISO/IEC 27018 standard has been published in 2014 to supplement the ISO/IEC 27002. The ISO/IEC 27018 takes the extensive set of security controls described in ISO/IEC 27002 as a base and then extends them in two ways.</p> <p>First, existing security controls are extended in a number of areas to deal with dividing responsibilities between the cloud service customer and the cloud service provider. ISO 27018 intends to ensure a clear separation of development, testing and operational environments, and organize an information backup and event logging when Personal information are involved.</p> <p>Second, a new set of security controls are added, to reflect the privacy principles defined in the ISO/IEC 29100 privacy framework standard.(e.g. Right of access and deletion Purpose limitation, etc.)</p>
	The standard is accessible upon payment.
Requirements	<p>The ISO/IEC 27018 contains the following mechanisms:</p> <ul style="list-style-type: none"> • Information security policies • Organisation of information security • Human resource security • Asset management • Asset control • Cryptography

	<ul style="list-style-type: none"> • Physical and environmental security • Operations and communications security • System acquisition, development and maintenance • Supplier relationships • Compliance • Information security aspects of business continuity management.
Assessor	Internal auditors
	BSI is accredited as organisation against the ISO 17021:2015 Conformity assessment - Requirements for bodies providing audit and certification of management systems
Process	Third party certification
	<p>Assessment process</p> <p>BSI receives the application and appoints a client manager to guide the applicant through the process steps:</p> <ol style="list-style-type: none"> 1. Gap analysis Optional pre-assessment service offering a closer look at the existing system and compare it with the BS 10012 requirements. 2. Readiness review Stage 1 audit consisting of reviewing the organization’s preparedness for assessment by checking if BS 10012 procedures and controls have been developed. 3. Formal assessment Stage 2 audit: if all the requirements are in place, BSI assesses the implementation of the procedures within an organization (gathering information, testing compliance and effectiveness of measures etc.) to make sure that fulfils certification requirements.
	<p>Certification issuance</p> <ul style="list-style-type: none"> • BSI issues the certification after having reviewed the audit report • A seal is issued to the certified body • The name, adress, status, name of standard and scope are published online
Renewal	Renewal on request at the end of the validity period
	Full assessment process according to the same process than the initial certification process

Monitoring	<p>BSI assigns a client manager to carry out ongoing assessments to support the continual improvement activities of the certified party.</p> <p>A surveillance audit (for maintenance purposes) is conducted by BSI on a yearly basis to ensure continuity of compliance.</p> <p>If minor or major non-conformities are found, the client will be helped to improve them.</p> <p>BSI is also allowed to conduct short notice audits or unannounced audits if there is evidence that the client is no longer in compliance.</p> <p>The client has an obligation to notify BSI in a timely manner if certain changes take place in management, organization structure, incidents such as breaches occur, etc.</p>
Suspension/Withdrawal	<p>BSI may suspend a certificate if the compliance with the standard is no longer met; if the client refuses to provide additional information as required by BSI (e.g. changes in management, changes in the structure of the organization, expansion of activities, data breaches etc.)</p> <p>Under suspension, the certification of a client's management system is invalid until the suspension is lifted. Such suspension will be made clear on the BSI client directory.</p>
Guarantees	No
Complaint handling	<p>Complaints should be submitted in writing to the Regional Managing Director of the BSI office in the country where the person lodging the complaint resides.</p> <p>The person lodging the complaint will be kept informed of progress. BSI will reply as soon as the complaint has been fully investigated.</p> <p>Complaints about a registered or verified assertion client should also be submitted in writing.</p> <p>Having confirmed that the subject client is registered by BSI, BSI will ensure that they are taking appropriate action and confirm how the issue has been dealt with during a subsequent audit or verification of the client. For this reason, these complaints may take longer to fully resolve.</p>
Dispute resolution process	<p>A certified body with a disagreement concerning the decision of his certification or verification unable to resolve either through his Client Manager/Auditor/Verifier, or with the local management of his BSI office, may appeal in writing within 21</p>

	<p>days from receipt of the decision to the Head of Compliance & Risk of the BSI office in his country.</p> <p>Selected BSI personnel will be appointed who are independent of the appealed issue. Contact will be made to acknowledge receipt of the appeal, outline the appeals process, gather and verify additional data and information required.</p> <p>The results of the appeal decision will be communicated formally.</p>
--	---

ANALYSIS	
GDPR relevance	Article 28
Benefits	<p>ISO/IEC holistic approach: ISO/IEC 27018 standard 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 leverages the businesses familiarity with the ISO vocabulary and approach following the success ISO 9001 and at a lesser extent, the ISO/IEC 27001.</p> <p>Maturity level approach: The ISO/IEC 27018 standard can be seen as an additional layer to the ISO/IEC 27001 for cloud processors. This maturity level approach could be generalized to all businesses with the publication of the ISO/IEC 27552 - Enhancement to ISO/IEC 27001 for privacy management.</p>
Limits	<p>Paying access: The standard is available upon payment of a fee</p> <p>ISO privacy approach: The ISO approach does not take into account all the GDPR requirements for processors.(e.g. breach notification).</p>
Evolution and Improvement	<p>Suggestion 1 Certification schemes based on ISO/IEC 27018 could define additional requirements to align it with the GDPR.</p> <p>Suggestion 2 Consider updating the standard itself to align it with the GDPR. TAs the ISO/IEC 27018 is scheduled to be revised in 2019.</p>

Table 3.2 BSI - ISO/IEC 27018 - Protection of Personally Identifiable Information

3. CNIL - ASIP Santé - Authorization procedure dedicated to processors storing personal health data

<p>Ministère de la santé - CNIL et Agence des Services d'Information Partagés de Santé (ASIP-Santé) Agrément des Hébergeurs de Données de Santé à Caractère Personnel</p> <p>French Ministry of Health - CNIL and French agency for shared health IT systems - (ASIP- Santé) Authorization procedure dedicated to processors storing personal health data</p>	<p>No sign issued</p>
IDENTITY	
Owner of the scheme	French Ministry of Health
Country	France
Licensing policy	<p>No Licensing policy.</p> <p>The authorisation procedure is owned by the French Ministry of Health but managed by a Ministry's agency dedicated to the regulation of health IT systems (ASIP Santé) with the help of the CNIL.</p>
Contract Arrangement	Authorization (administrative act) issued in writing by the French Ministry of Health to the compliant body
Creation date	2006
No. of certification issued	96
List of certified entities	Public list accessible from the ASIP's website http://esante.gouv.fr/services/referentiels/securite/hebergeurs-agrees
Geographical scope	National
Functional scope	Processes

	<p>The approval process applies to processors storing personal health data on behalf data controllers.</p> <p>The approval process applies to processors storing personal health data collected during prevention, diagnosis, care or social follow-up activities.</p> <p>Data controllers directly storing personal health data are not required to undergo this authorization process.</p>
Sector	Personal health data storage
Type	Mandatory
Validity	3 years
Costs	<p>The process of certification with the ASP is free of charge</p> <p>No license</p>
Contact	contact-agreement-hebergeurs@sante.gouv.fr.
Website	<p>Only in French</p> <p>http://esante.gouv.fr/services/referentiels/securite/hebergement-faq#1</p>
FUNCTIONING	
Foundations	<p>The authorization process is based on Article L. 1111-8 and following of the French Health Code derived from law n° 2002-303 of 4 march 2002 on the rights of health patient and quality of the healthcare system.</p> <p>Article L. 1111-8 and following have been modified by law 2016-41 of 26 January 2016 dedicated to the modernization of the healthcare system</p> <p>Article L. 1111-8 and following are accessible for free from the website below (In French only)</p> <p>https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000021941353&cidTexte=LEGITEXT000006072665</p>
Requirements	<p>Article R1111-9 of French Health Code requires from processors storing health data to be compliant with the following requirements:</p> <ul style="list-style-type: none"> • Use skilled operators in the data management, • Identify people in charge of the data management. The

	<p>team must encompass a doctor of medicine. The contract must detail its contractual relationship with the data storage company,</p> <ul style="list-style-type: none"> • Identify the legal responsible(s), • Set up processes ensuring secure storage, accessibility and preventing unauthorized access to the data, • Isolate health data storage from other activities in the storage company organization, • Set up a communication process towards the data controllers in case of breach or any other incidents.
Assessor	<p>Internal auditors.</p> <p>The assessment process is simultaneously done by</p> <ul style="list-style-type: none"> • CNIL's agents • ASIP authorization committee ("Accreditation Committee") created by article R.1111-10 of French Health Code.
	<p>No accreditation (authorities' agents)</p>
Process	<p>Third party certification process</p>
	<p>The conformity assessment process is done from a questionnaire review. The questionnaire is available from the ASIP's website (in French only)</p> <p>http://esante.gouv.fr/services/referentiels/securite/formulaires-du-referentiel-de-constitution-des-dossiers-de-demande-d</p> <ul style="list-style-type: none"> • The applicant sends the completed questionnaire to the ASIP Santé, • The application is then transmitted to the CNIL, • The CNIL has 2 months for evaluating the data protection, • measures set by the applicant to handle personal health data • The CNIL transmits its evaluation to the accreditation committee, • The accreditation committee also has 2 months to evaluate the application. • The two evaluations are transmitted to the French Ministry of health for final decision.
	<p>The Ministry of health has two months for granting or not the authorization once the report has been transmitted</p>
Renewal	<p>The authorization is renewable on request at the end of the validity period.</p>
	<p>Full reassessment according to the same procedure than the initial one.</p>


	<p>In addition, the applicant shall submit the results of an external third party audit done at its own expenses, before the renewal request.</p> <p>The third party audit must report the possible changes happened in the applicant's situation and demonstrate that the conditions required to obtain the authorization are maintained.</p>
Monitoring	<p>No active monitoring</p> <p>Article L.1111-8 of French Health Code authorizes the General Inspection of Social Affairs (IGAS) to randomly enforce the compliance of authorized bodies.</p> <p>The authorized bodies can also be included into the random enforcement program annually scheduled by the CNIL. (Done in 2015).</p>
Suspension/Withdrawal	<p>No suspension and withdrawal process defined</p> <p>The authorization may be withdrawn in case of persistent non-compliance or important changes in the situation of the authorized body.</p> <p>No case to date</p>
Guarantees	<p>A processor storing personal health data is unable to start or maintain its activity without the authorisation.</p>
Complaint handling	<p>The authorization is an administrative decision that can be brought before the French administrative court.</p>
Dispute resolution process	<p>The dispute resolution process follows the French administrative law.</p>

ANALYSIS	
GDPR relevance	<p>Article 28 Article 32</p>
Benefits	<p>Free of charge: certification process affordable to SMEs</p> <p>Reliability: Certification managed by French authorities</p> <p>Market monitoring: The authorization procedure regulates the market and monitor the minimal level of security ensured by the data processors.</p>

Limits	<p>Entry barrier: The future third party certification process (see below) will be paid and might exclude SMEs (unable to afford certification) from the market.</p> <p>Limited market: Health data market remains in France a limited market. Around 100 companies have been approved, representing most of the market. It is worth spending time designing and updating requirements for only 100 companies? Why not relying on the ISO security standards already published?</p>
Evolution and Improvement	<p>Article 204. 5° c of law 2016-41 of 26 January 2016 dedicated to the modernization of healthcare system introduced the ability to set up third party certification procedures instead of the authorization procedure currently in force.</p> <p>The authorization procedure will be replaced in mid-2018 by a third-party certification scheme owned by the ASIP santé and operated by public or private third party bodies.</p> <p>The new process agreed so far is be the following one:</p> <p>The French national accreditation body (COFRAC) will accredit third-party bodies, public or private in France or in Europe, interested in issuing the certification.</p> <p>Private or public accredited certification bodies (4 years validity) will handle the full certification process under the monitoring of the ASIP santé.</p> <p>The ASIP santé will be in charge to manage the requirements and monitor the scheme.</p> <p>Even if the scheme is close to a data protection scheme, there is no plan to undergo an approval process under Article 42 GDPR or any accreditation process under Article 43. The Accreditation under Article 43 GDPR would be complicated to the extent that the ASIP requirements are based on the ISO/IEC 17021 while the GDPR requires to accredit based on ISO/IEC 17065.</p> <p>The accreditation and certification requirements are available on the ASIP Santé's website(In French only) http://esante.gouv.fr/actus/services/hebergement-des-donnees-de-sante-nouveaux-referentiels</p>

Table 2.3 CNIL - ASIP Santé - Authorization procedure dedicated to processors storing personal health data

4. CNIL Label - Safebox

<p>Label CNIL Coffre-Fort Electronique</p> <p>CNIL Label Safebox</p>	
IDENTITY	
Owner of the scheme	Commission Informatique et Libertés - CNIL (French Data Protection Commissioner)
Country	France
Creation date	2014
No. of certification issued	1
List of certified entities	Public list accessible from the CNIL's website https://www.cnil.fr/fr/labels
Licensing policy	No
Contract arrangement	<p>A CNIL's official decision (administrative act) published into the French Official Journal is issued to the certified body. This is only legal link between both parties.</p> <p>A series of customized seals (with a licence number and expiration date) is sent to the certified body along with the regulation of use.</p> <p>The seal's holder must accept and respect the regulation of use of the seal</p>
Geographical scope	National
Functional scope	Product

	<p>The scheme focuses on digital vaults</p> <p>A digital vault, states the CNIL “differs from a storage space in that the data that is stored there (documents and some meta-data) is only accessible to the holder of the vault, and to any persons whom he/she may have mandated”.</p>
Sector	Data storage
Type	Voluntary
Validity	3 years
Costs	The certification process is free of charge No license fees
Website	https://www.cnil.fr/en/what-you-should-know-about-our-standard-digital-safe-boxes
FUNCTIONING	
Foundations	Decision No. 2014-017 dated 23 January 2014 adopting a standard for the delivery of privacy seals concerning digital safe boxes.
	The requirements are accessible for free on the CNIL’s website https://www.cnil.fr/sites/default/files/atoms/files/referentiel_cfn_en.pdf
Requirements	<p>The applicant must be compliant with the 22 requirements regarding:</p> <ul style="list-style-type: none"> • Data access, • Data storage, • Users information management, • Risk management and compliance, • Cryptographic mechanisms <p>See the full requirements for details https://www.cnil.fr/sites/default/files/atoms/files/referentiel_cfn_en.pdf</p>
Assessor	Internal auditors (CNIL’s agents)
	No accreditation process


Process	Third party certification
	<p>The assessment process is based on a questionnaire compiling the requirements defined in the CNIL's standard https://www.cnil.fr/sites/default/files/atoms/files/labelsnil-cfn-demandev_0.docx</p> <p>The questionnaire must be fully completed by the applicant with relevant documents</p> <p>The questionnaire is reviewed by CNIL's agents to build the assessment report</p>
	<p>The certification process is managed by the CNIL following:</p> <ul style="list-style-type: none"> • Validation of the assessment report by the CNIL seal unit • Submission of the final decision to the CNIL's steering committee • Publication of the decision into the French Official Journal • Issuance of the certificate and customized seal to the • Update of the public list of certified bodies on CNIL's website
Renewal	On request at the end of the validity period
	Full reassessment according to the same process than the initial certification process
Monitoring	<p>No active monitoring</p> <p>Monitoring can be included the label holders into the CNIL's enforcement schedule annually updated.</p> <p>To date, no enforcement has been done on certified bodies.</p>
Suspension/Withdrawal	<p>The CNIL is entitled to withdraw the seal in case of persisting non conformity</p> <p>Justification and remedial must be provided within a month after the certified body has been informed of its noncompliance.</p> <p>Without any response within this delay, a report is drafted to the labeling board and submitted for decision during a CNIL's plenary session. The plenary session decides to withdraw or not the certification granted.</p> <p>The certified bodies is then no more allowed to use and display the seal on its product and documentation.</p> <p>So far, no withdrawal has been requested by the labelling board.</p>

Guarantees	No
Complaint handling	No dedicated complaint handling process has been set for the CNIL label However, anybody is entitled to lodge a complaint online from the webform available on the CNIL's website (In French) https://www.cnil.fr/fr/plaintes
Dispute resolution process	All disputes are internally managed. However, in case of persisting disagreement, the case could be brought before the French administrative court.

ANALYSIS	
GDPR relevance	Article 28 Article 32
Benefits	Free of charge: Beneficial for SMEs Legitimacy of the issuer: The certification is managed by the French Data Protection Authority Marketing advantage: The seal offers to promote certified vaults not certified in the market
Limits	limited adoption: The requirements appears to stringent, especially concerning the security requirements Very limited market: The digital vault market in France is very limited and the low adoption rate questions the relevance to spend time for designing requirements for a single type of product.
Evolution and Improvement	The CNIL has already updated two standards (Governance and Training sessions) and plans to update the two last (audits and digital safe) during the 1st half of 2018. The CNIL is going to delegate the scheme management to accredited private bodies and keep the drafting or/and approval process of the requirements and plan to contribute to the accreditation process.

Table 3.4 CNIL Label – Safebox

5. Datenschutzaudit beim ULD

<p>Datenschutzaudit beim ULD</p>	
<p>IDENTITY</p>	
<p>Owner</p>	<p>Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (Independent State Center for Data Protection Schleswig-Holstein, abbreviation: ULD)</p>
<p>Country</p>	<p>Germany</p>
<p>Creation date</p>	<p>2000</p>
<p>Licensing</p>	<p>No</p>
<p>Contract arrangement</p>	<p>A public contract referring to Article 43 of the data protection law of the German Federal State of Schleswig-Holstein is concluded between ULD and the public body audited. It Includes:</p> <ul style="list-style-type: none"> • Target of evaluation (scope of certification), • Process, • Price • Planning
<p>No. of certification issued</p>	<p>35</p>
<p>List of certified entities</p>	<p>See https://www.datenschutzzentrum.de/audit/register/ This register starts in 2007 and has the most recent audit in 2017.</p>
<p>Geographical coverage</p>	<p>Regional (German Federal State of Schleswig-Holstein)</p>
<p>Scope</p>	<p>Data processing and personal information management system</p>
	<p>The subject of the Data Protection Authority audits may be:</p> <ul style="list-style-type: none"> - Individual automated or non-automated procedures in - The entire processing of personal data

	- Delimited part of a data processing
Sector	Public bodies
Type	Voluntary
Validity	3 years
Costs	<ul style="list-style-type: none"> • The certification process is charged on a case by case basis. (An audit expert is charged around €80 per hour). • The total certification cost depends on the complexity of the case. • No license fees are charged • For details on costs, see the documentation online. (In German only) https://www.datenschutzzentrum.de/audit/faq/ ('Wie hoch sind die Kosten')
Website	In German only https://www.datenschutzzentrum.de/audit/
FUNCTIONING	
Foundations	<p>The scheme is directly based on the Schleswig-Holstein 's data protection law (LDSG - Landesdatenschutzgesetz) and organized according to Article 43 Abs. 2 LDSG establishing the Independent State Center for Data Protection Schleswig-Holstein in charge of the certification process.</p> <p>The data protection law of Schleswig-Holstein (LDSG - Landesdatenschutzgesetz) is available in German at this address: http://www.gesetze-rechtsprechung.sh.juris.de/jportal/?quelle=jlink&query=DSG+SH&psml=bsshoprod.psml&max=true&aiz=true</p>
Requirements	<p>The applicant must be compliant with all the provisions of the Schleswig-Holstein data protection law:</p> <ul style="list-style-type: none"> • General principles <ul style="list-style-type: none"> • data avoidance and data economy, data protection Audit • general measures for data Security • special measures for data security with the use of automated procedures • List of procedures, notification • common procedures and call-off Procedures • preliminary inspection

	<ul style="list-style-type: none"> • Official Data Protection Officer • Admissibility of data Processing <ul style="list-style-type: none"> • admissibility of data Processing • form of consent • Survey, binding purpose • data transmission to other public bodies • data transmission to non-public bodies • data transmission to foreign countries • Special forms of data processing <ul style="list-style-type: none"> • processing of personal data in order • mobile personal computing Systems • automated individual decisions • video surveillance and recording • publication of data on the Internet • Special purposes of data processing <ul style="list-style-type: none"> • data processing for scientific purposes • data processing in service and employment Relationships • public awards • Rights of data subjects <ul style="list-style-type: none"> • Information, notification • information affected • information obligation in case of unlawful knowledge of data • correction, deletion, blocking • objection to the processing • damages • non-discrimination
<p>Assessor</p>	<p>ULD Internal auditors</p>
	<p>No accreditation process. ULD’s auditors are public servants</p>
<p>Process</p>	<p>The process is split into two phases: a pre-phase and the real audit. During the pre-phase the following issues are covered:</p> <ul style="list-style-type: none"> • Delineation of the audit scope (Target of Evaluation or ToE), • Determination of objectives for data protection, • Collection of documentation related to the audit scope, • Inventory of technical and organizational processes, • Preparation project plan, • Issue solving, • Establishment of a data protection management system, • Creation of the data protection concept, • Preparation of the documentation required for the data protection authorities audit as well as final review of the fulfillment of all tasks defined and to be performed during the pre-audit.

	<p>The real audit phase itself captures the following steps:</p> <ul style="list-style-type: none"> • Checking the delineation of the audit scope, • Analysis of the documentation regarding the data protection management system (Datenschutzkonzept), • Assessment of the operation of the data protection management system, • Assessment of the achievement of specified data protection objectives, • Highlighting recommendable and privacy-friendly data processing processes, • Random verification of the implementation of the security measures defined in the data protection concept, • Verification of compliance with data protection and sector-specific regulations with regard to the scope of the audit • Preparation of the audit report,
	<ul style="list-style-type: none"> • The certification is issued by the ULD following a review of the audit report. • A seal is awarded to the body certified. • The information about the certified body along with its audit report are published on the ULD's website.
Renewal	The certification is renewable on request at the end of the validity period.
	Partial reassessment in case of minor changes, full reassessment in the other cases
Monitoring	<p>The ULD ensures two types of monitoring:</p> <ul style="list-style-type: none"> • An optional conformity review is offered 12 and 24 month after a successful certification (Included in initial contract) • A random checking can be done to the extent ULD is a data protection authority
Suspension/Withdrawal	<p>The certification can be withdrawn:</p> <ul style="list-style-type: none"> • When ULD observes that circumstances have changed and lead to the need to reconsider the process, • A certified organization indicates itself that circumstances of data processing and the management of the data processing have changed such that the declaration is not valid anymore. • No detailed process is defined in the status of the State Center for Data Protection organizing the suspension and withdrawal process.
Guarantees	No

Complaint handling	<p>Complaint handling is managed in two steps</p> <ul style="list-style-type: none"> • Certified bodies and third parties can lodge a complaint in writing to the ULD, • The ULD receives and internally manages the complaints, • In case of persisting disagreement, the complainant is entitled to bring the case before the administrative court
Dispute resolution process	The dispute will be resolved by the normal procedures in place for disputing a claim under the Schleswig-Holstein' administrative law ("Landesverwaltungsgesetz")

ANALYSIS	
GDPR relevance	Article 24
Benefits	<p>Free of charge: The certification process is affordable to SMEs</p> <p>Reliability: The certification is managed by the German Lander Data Protection Authority</p> <p>Focus on public processing: The scheme intends to address the processing managed by public authorities that some can potentially challenge citizen fundamental rights.</p>
Limits	<p>Regional scope: The geographical scope of the scheme is limited to the German Lander of Schleswig-Holstein.</p> <p>Direct reference to the law: The scheme directly refers to the provisions of the law. The assessment of legal provisions can be sometime difficult to interpret and audit.</p>
Evolution and Improvement	<p>European-wide scheme: It could be interesting to leverage the ULD's experience to set up a European-Wide scheme focusing on public processing.</p> <p>Standard based scheme: The translation of the legal provisions into auditable requirements could ease the certification process and its preparation by candidates. It seems (to be verified) this is the direction taken by the ULD in the requirements revision process currently in progress. See draft below (in German only) (https://www.datenschutzzentrum.de/uploads/guetesiegel/guetesiegel-anforderungskatalog.pdf).</p>

Table 3.5 Datenschutzaudit beim ULD

6. ePrivacyApp

<p>ePrivacyApp</p>	
IDENTITY	
Owner	ePrivacy GmbH
Country	Germany
Creation date	2012
Licensing	No
Contract Arrangement	<p>Assessment service contract The assessment process can be carried out under a separate agreement when done by an external auditor approved by ePrivacy GmbH.</p> <p>Certification licensing agreement The certification is also subject to a licensing agreement signed between the certified organization and ePrivacy GmbH.</p>
No. of certification issued	45
List of certified entities	The list is available on ePrivacy website https://www.eprivacy.eu/en/customers/awarded-seals/
Geographical coverage	International
Scope	Products
	ePrivacyApp certifies any online mobile applications

Sector	Mobile Apps
Type	Voluntary
Validity	Unlimited validity period until any changes are made on the app
Costs	The conformity assessment is charged to the applicant on the basis of a fixed price. An annual license fees is also charged to the certified body
Website	https://www.eprivacy.eu/en/privacy-seals/eprivacyapp/
FUNCTIONING	
Foundations	The ePrivacyApp criteria are based on the German Data Protection law, the GDPR, the IAB Europe OBA Framework (governing self-regulation of by the digital advertising industry) and ePrivacy GmbH security criteria.
	The ePrivacyApp criteria are accessible for free on the ePrivacy GmbH website https://www.eprivacy.eu/fileadmin/Redakteur/PDF/Kriterienkataloge/ePrivacyApp_criteria_catalog_2018.pdf
Requirements	<p>The ePrivacyApp criteria encompasses 150 criteria assessing the following topics:</p> <ul style="list-style-type: none"> • Data protection <ul style="list-style-type: none"> • privacy notice/ T&Cs • selection of data protection settings by users • use of the data via the app • access to personal information or details of contacts or users • dissemination of data to third parties • compliance with data protection legislation (BDSG, TMG) • Data security <ul style="list-style-type: none"> • examination of data packages • analysis of incoming and outgoing data traffic • encoding of data traffic • secure saving of data • data testing by means of white-hat hacking (???) • authentication of data recipients (WHOIS) • Online behavioral advertising (OBA)


	<ul style="list-style-type: none"> • use of the app for the creation of user profiles • opt-out possibility • possibility of contacting operators <p>See ePrivacyApp criteria on ePrivacy’s website for details https://www.eprivacy.eu/fileadmin/Redakteur/PDF/Kriterienkataloge/ePrivacyApp_criteria_catalog_2018.pdf</p>
Assessor	Internal and external auditors
	<ul style="list-style-type: none"> • Training process for external auditors based on certification experience with ePrivacy internal auditors • To get an ePrivacy <i>accreditation (note: not to be confused with art. 43 accreditation)</i>, it is necessary to have collaborated on a couple of certification processes with experienced ePrivacy auditors. After that, applicant auditors can ask the management for an official accreditation • Auditors have to prove their technical or legal expertise to the ePrivacy board. • There is no technical or legal exam or renewal process due to the small size of the team.
Process	Third party certification
	<p>The conformity assessment is performed according to the following steps:</p> <ul style="list-style-type: none"> • App testing on different devices according to the ePrivacyApp Criteria Catalog • Technical workshop (2-3 hours) with the applicant's team and our technical experts if necessary • Issuance of the technical evaluation report
	<p>The ePrivacy board reviews the technical evaluation and, if positive, sends the evaluation with the official certificate and seal to the client.</p> <p>Every certificate issued is also published on the ePrivacy website https://www.eprivacy.eu/en/customers/awarded-seals/</p>
Renewal	On request after major changes to the app Full reassessment
	Full assessment according to the same process than the initial certification process

Monitoring	No active monitoring
Suspension/Withdrawal	ePrivacy reminds the certified body via email and/or telephone of the non-conformity (ies) that must be redressed in case of persisting non-conformity, the seal could withdrawn (not occurred so far)
Guarantees	No
Complaint handling	A complaint can be lodged on ePrivacy GmbH website https://www.eprivacy.eu/en/contact/ The complaint is managed internally. ePrivacy GmbH also may contact other external experts or authorities if necessary.
Dispute resolution process	No formal processes defined and described into the scheme documentation The dispute process is internally managed contact other experts or the authorities if necessary.

ANALYSIS	
GDPR relevance	Article 24 Article 32 Article 28
Benefits	Dedicated scheme: Scope relevant to apps Technical assessment: The scheme ensures in depth technical analysis of the app
Limits	Readiness: Process needs to be updated to meet GDPR's requirements
Evolution and Improvement	-

Table 3.6 ePrivacyApp

7. European Privacy Seal - EuroPriSe

<p>European Privacy Seal EuroPriSe</p>	
IDENTITY	
Owner	EuroPriSe GmbH
Country	Germany
Creation date	2007
Licensing	No
Contract Arrangement	<p>Assessment service contract A service contract (“evaluation agreement”) is signed between the applicant and the external auditor. “This agreement is directly negotiated between the seal applicant and the chosen experts, without any interference by EuroPriSe”.</p> <p>Certification agreement The certification agreement is signed between EuroPriSe and the applicant before the conformity assessment. It defines:</p> <ul style="list-style-type: none"> • The certification scope (“target of evaluation”), • The fees on the part of the certification body, • The rights and duties of the contractual partners regarding topics such as confidentiality, duty of the seal applicant to cooperate”
No. of certification issued	43
List of certified entities	Public list available on EuroPriSe’s website https://www.european-privacy-seal.eu/EP-S-en/awarded-seals
Geographical coverage	International
Scope	Products and services

	<p>EuroPriSe offers to certify:</p> <ul style="list-style-type: none"> • Hardware and software IT products. EuroPriSe certifies the product itself is certified but not its use, • IT-based services when service providers is processors. The service offered is certified but not its concrete use, • IT-based services with service providers as controllers. The service offered is certified but not the concrete use, • Publicly accessible parts of websites with a focus on interaction between website and browser of a visitor excluding webshops, restricted areas and
Sector	Any
Type	Voluntary
Validity	2 years
Costs	<p>Website certification: 10 000 € (price including expert and certification body cost)</p> <p>Other certification services: The price can range from 3 500 € up to 24 000 € (price excluding expert cost) depending on the complexity of the request. The upper range is for projects of particularly large complexity.</p> <p>When certification is renewed and no revisions in the product or service to be certified are present, costs are about half of the above price.</p>
Website	https://www.european-privacy-seal.eu
FUNCTIONING	
Foundations	<p>The EuroPriSe criteria are an open 'standard' based upon all the GDPR provisions also including ePrivacy Directive requirements (Directive 2009/136/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation).</p> <p>The Data subject rights are one of the main focal points of the certification procedure.</p>

	<p>The EuroPriSe criteria are accessible for free on Europrise’s website https://www.european-privacy-seal.eu/EPS-en/Criteria</p>
Requirements	<p>The applicant must be in conformity with all the following requirements defined in the EuroPriSe criteria:</p> <ul style="list-style-type: none"> • 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 <p>See the EuroPriSe criteria for details: https://www.european-privacy-seal.eu/AppFile/GetFile/e5ed7122-74b1-4f75-a5af-fb0c317bd20b</p>
Auditors	<p>External accredited (<i>note: not to be confused with art. 43 accreditation</i>) organisations or individuals</p> <ul style="list-style-type: none"> • Mandatory accreditation (<i>note: not to be confused with art. 43 accreditation</i>) 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.
Process	<p>Third party certification</p> <p>The assessment process follows a 3 steps process:</p> <ol style="list-style-type: none"> 1. Target of evaluation Definition of the certification scope (the “Target of Evaluation (ToE)”) with the applicant. 2. Technical and legal evaluation of the ToE. The “evaluation methods may include, but are not necessarily limited to on-site visits, interviews with relevant staff of the seal applicant, the use of demo versions of an IT product and of test accounts for an IT-based service as well as the review of web portals, source code and relevant documentation”. 3. Evaluation report Once drafted by the expert in charge of the evaluation, “a signed copy of the evaluation report must be submitted to the certification body”


	<p>The EuroPriSe board issues the certification after having</p> <ul style="list-style-type: none"> Validated the evaluation report Drafted the validation report <p>A seal is then issued along with the public report published on EuroPriSe website</p> <p>EuroPriSe publishes online the service or product name and type, the version of certification criteria used during the process, the certification, the validity period, the monitoring audit dates and the core findings of the evaluation in a short public report.</p>
Renewal	On request at the end of the validity period. Early recertification can be required in case of important technical or legal changes.
	Partial assessment in case of minor changes or full reassessment
Monitoring	<p>The assessor performed two monitoring audits 8 and 16 months after a successful certification or recertification to check the maintenance of the conformity.</p> <p>If clear deviations are observed, this will be notified to the certified party and If necessary, will be brought to the attention of the EuroPriSe certification board through the monitoring report.</p>
Suspension/Withdrawal	<p>The certification can be withdrawn if one of the following situation occurs:</p> <ul style="list-style-type: none"> Observed non-compliance, Non-respect of the contractual obligations, Commonly agreed contract termination, Final decision of a dispute concluding to the non-conformity
Guarantees	No
Complaint handling	<p>Two steps in the complaint handling</p> <ul style="list-style-type: none"> First, the complainants are required to submit their complaints to the respective seal holder. Second, If the complaint has not been resolved between the complainant and the seal holder, an external complaints can be lodged with the EuroPriSe board by means of a dedicated complaint form available on EuroPriSe's website. https://www.european-privacy-seal.eu/EPS-en/Dispute-Resolution-Complaint-Form.

Dispute resolution process	<ul style="list-style-type: none"> • The complainant and the EuroPriSe seal holder try to resolve the dispute through an internal dispute resolution process. • If the above process did not lead to a solution, because the dispute is not solved or the complainant is able to show probable cause that the internal dispute resolution is not acceptable, then, the external procedure with the EuroPriSe board is started. • The complainant is informed whether or not its complaint is admissible within 5-10 working days. The investigation and evaluation of the facts are done within a 6 weeks time frame at the end of which the complainants is informed of the result.
-----------------------------------	---

ANALYSIS	
GDPR relevance	Article 24 Article 28
Benefits	<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 The scheme aligned its requirements with the GDPR and is already accredited (<i>note: not to be confused with art. 43 accreditation</i>). Possesse auditors in 19 countries even in certain countries outside EU. The scheme is well-suited, once approved and accredited, to become one of the first European-wide data protection scheme.</p>
Limits	Scalability The capacity of EuroPriSe to manage the scalability of the scheme is still to be demonstrated.
Evolution and Improvement	Licensing EuroPriSe could license the scheme requirements, seal and processes to other certification bodies.

Table 3.7 European Privacy Seal – EuroPriSe

8. iKeepSafe COPPA

iKeepSafe COPPA	
IDENTITY	
Owner	iKeepSafe, (501(3)(c) non-profit organization)
Country	USA
Licensing	No
Creation date	2014
Contract Arrangement	<p>The contract defines:</p> <ul style="list-style-type: none"> • The license granted to the certified body to display the seal, • The rule of fair use of the seal without which the seal can be withdrawn, • The contract signature is also the starting point of the certification process ensuring its confidentiality.
No. of certification issued	23
List of certified entities	The list of certified bodies is available on iKeepSafe's website https://ikeepsafe.org/products/
Geographical coverage	National
Scope	Products and processes
	iKeepSafe COPPA Safe Harbor Certification ensures that practices surrounding collection, use, maintenance and disclosure of personal information from children are consistent with principles and requirements of the Children's Online. Privacy Protection Act (COPPA).

Sector	Any, although the scheme primarily focuses on educational environments
Type	Voluntary
Validity	1 year
Costs	The initial certification process costs US \$6400 The renewal is available at 20% off the initial fee. No license fees
Website	https://ikeepSAFE.org/certification/coppa/
FUNCTIONING	
Foundations	<p>The scheme is based on an internal standard (Program Guidelines) derived from the US children’s Online Privacy Protection Act (COPPA).</p> <p>COPPA includes a provision enabling industry groups or others to submit to Federal Trade Commission (FTC) for approval self-regulatory guidelines that implement the protections of the Commission’s final Rule.</p>
	<p>The Program Guidelines are in restricted access to IkeepSafe’s customers.</p> <p>However, basic documents including COPPA Safe Harbor program guidelines and COPPA 101 for EdTech Companies are available at no charge on the FTC’s website.</p> <p>https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule</p>
Requirements	<p>The applicant must be compliant with all the content of the Children’s Online Privacy Protection rules.</p> <ul style="list-style-type: none"> • Regulation of unfair or deceptive acts. • Regulation of practices about the collection, use, and/or disclosure of personal information from and about children on the Internet. • Notice. • Parental consent. • Right of parent to review personal information provided


	<p>by a child.</p> <ul style="list-style-type: none"> • Prohibition against conditioning a child's participation on collection of personal information. • Confidentiality, security, and integrity of personal information collected from children. • Enforcement. • Data retention and deletion requirements. • Safe harbor programs. • Voluntary Commission Approval Processes. • Severability. <p>See for details on FTC's website https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5</p>
<p>Assessor</p>	<p>Internal auditors</p>
	<p>iKeepSafe has been approved as Safe Harbor organization by the FTC.</p> <p>The assessment processes can be randomly checked by FTC officials.</p> <p>Every year, IkeepSAFE undergoes a case examination with FTC officials and must send its activity report.</p>
<p>Process</p>	<p>Third party certification</p>
	<p>The assessment process is performed according to the following steps:</p> <ul style="list-style-type: none"> • Non-disclosure agreement is signed to ensure the process confidentiality • Live presentation of the product or service • Documentation review from technical and legal documents disclosed by the applicant • Technical tests • Security check
	<p>iKeepSafe awards the certification after they find the client is in full compliance with all the requirements</p> <p>The certified body receives a seal to display on its site and marketing materials.</p> <p>They are referred to as a 'Member Company' and a few information about the company and the product are published on the website.</p>

Renewal	<p>On request at the end of the validity period</p> <hr/> <p>Full reassessment with a 20% discount offer</p>
Monitoring	<p>iKeepSafe can use full or partial random check without notice</p> <p>If iKeepSafe determines certified bodies previously compliant are no longer in compliance, iKeepSafe submits a notice to the certified body detailing the non-compliance and specifying required changes (the "Notice of Concern").</p> <p>Non-compliant certified body has 5 business days to respond in writing to attest that the required changes will be made in a specific and timely fashion.</p> <p>Once done, the certified body must submit a signed certification form attesting to completion of the required changes.</p>
Suspension/Withdrawal	<p>iKeepSafe can revoke the certification at any time during the validity period if any of the following occur:</p> <ul style="list-style-type: none"> • Member Company has failed within a reasonable period to cure material non-compliance with Program Guidelines after notification from iKeepSafe. • Member Company's breach of its obligations. • Intentional misstatements by the certified body in any communications related to the online services, the COPPA Safe Harbor Program, iKeepSafe, or the seal. <p>A certified body can also notify iKeepSafe at any point that it no longer wishes to use the seal:</p> <ul style="list-style-type: none"> • Member Company must then cease all use of the seal.
Guarantees	No
Complaint handling	<p>Third party can lodge complaints related to IkeepSafe certified bodies by email</p> <p>iKeepSafe responds to the questions and/or investigate the complaint.</p>
Dispute resolution process	In case of persisting disagreement, the case can be brought before the Court.

ANALYSIS	
GDPR relevance	Recital 38 Article 8 (children data protection)
Benefits	<p>Scope The COPPA framework offers an interesting example of what could be done to protect children data.</p> <p>Pricing policy The pricing policy applied by the scheme offering a 20% discount for renewing its certification. It could represent an interesting incentive for SMEs to maintain their conformity over time.</p>
Limits	<p>National coverage The scheme is closely related to the US regulation and is inapplicable as such in Europe.</p> <p>Sustainability The pricing policy applied by the scheme is only sustainable, confirmed the owner, because the management structure of the scheme remains very light. Applying such a policy on a wider scale could compromise the financial sustainability of the schemes.</p>
Evolution and Improvement	-

Table 3.8 iKeepSafe COPPA

9. ISDP©10003 Data Protection Certification

<p>ISDP©10003 Data Protection Certification</p>	 <p>The image shows two logos. On the left is a circular seal for 'DATA PROTECTION CERTIFIED' with 'ISDP 10003:2015' at the bottom and a map of Europe in the center. On the right is the ACCREDIA logo, which includes the text 'ACCREDIA', 'L'ENTE ITALIANO DI ACCREDITAMENTO', 'PRD N° 189 B', 'Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC', and 'Signatory of EA, IAF and ILAC Mutual Recognition Agreements'.</p>
IDENTITY	
Owner	Inveo srl
Country	Italy
Creation date	2015
Licensing	The scheme can be licensed. It has been licensed to 3 other certification bodies.
Contract arrangement	<p>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.</p> <p>Assessment service contract The assessment process can be carried out under a separate agreement when done by an external auditor accredited by Inveo.</p> <p>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;</p> <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
No. of certification issued	31

List of certified entities	The list of certified bodies is available on Inveo's website https://www.in-veo.com/en/registri/albo-certificazioni/aziende
Geographical coverage	International
Scope	Processes
	Certification of processes for the protection of the physical person regarding personal data and the free circulation of said data.
Sector	Any
Type	Voluntary
Validity	3 years
Costs	Certification process is charged to the applicant on a case by case basis based on rules defined in ISO 27006 Annex B and IAF MD05 about audit times required by company size.
Website	https://www.in-veo.com/en/certification/isdp-10003-2015-data-protection
FUNCTIONING	
Foundations	The ISDP©10003 standard is based on the General Data Protection Regulation, and a series of standards used to ensure the methodology relevance and consistency. For instance, the ISO 9001, ISO 19011 ISO 17021-1 (Audit methodology), ISO 2859-10 (Sampling methodology), ISO 25012 and ISO 25024 (data quality model) and ISO 31000 (Risk Management), Annex SL (drafting guide) , ISO 27001 (security)
	The ISDP standard is in paying access (180€ in November 2017)
Assessor	Internal and external bodies and individuals
	Accreditation (<i>note: not to be confused with art. 43 accreditation</i>) of external require: <ul style="list-style-type: none"> • Following 5 training modules ended with a final examination (written and use case exam) • Annual upgrade training required

<p>Requirements</p>	<p>The applicant is required to be compliant with all the requirements cover the following topics:</p> <ul style="list-style-type: none"> • General obligations and Awareness of the holder Objective: Establish a correct perception and formal application of the concept of general responsibility of the seal holder. • Organizational measures for the protection of personal data Objective: Determine whether the holder has adopted all internal policies to ensure the application of data protection principles. • Technical Measures for the Protection of Personal Data Objective: Ensure the correct application of technical measures to verify and assess whether the policies adopted in the process guarantees the security. • Assessment of the rights and freedoms of subjects Objective: Enhance compliance of data processes that may pose high risks to fundamental rights and freedoms of natural persons • Seal holder Objective: Ensure that the rules in force are respected • Co-responsible Objective: To establish and ensure the correct distribution of responsibilities • Data controller Objective: Ensure compliance with the holder's prescriptions • Responsibility Objective: Ensure the correct application of the principles of data processing and quality • Security of the process Objective: Ensure the safe handling of personal data • Principles of voluntary processing of personal data: Consent Objective: Assess adequacy and accuracy of information available to the person concerned in expressing his consent to the treatment • Information Objective: Evaluate the correct information disclosure procedures to the data subjects • Rights of the data subjects Objective: Evaluate the correctness of the exercise of the rights of data subjects • Opposition to profiling activities Objective: Ensure proper profiling management
----------------------------	--


	<ul style="list-style-type: none"> Transfer of personal data to third countries Objective: Evaluate the compliance of the procedures adopted to transfer data outside the EU (if any)
Process	Third party certification
	<p>The assessment activity encompasses two phases:</p> <ul style="list-style-type: none"> Document review: This phase evaluates the completeness and compliance of company's documentation (manual, procedures, operating instructions) On-site inspection: This phase analyses the current state of implementation of the data protection system, through interviews, objective evidence, procedures and operational processes set by the organization in its business with reference to personal data being processed.
	<p>Inveo's Technical Approval Committee reviews the audit report produced by the auditors and decide of the certification issuance</p> <p>In case the audit report is conclusive, the certification is issued and information about the certified body published on Inveo's website</p>
Renewal	On request at the end of the validity period
	Full reassessment according to the same condition than the initial certification
Monitoring	<p>The monitoring is done is based on an annual review of processes certified</p> <p>The monitoring aims at reviewing the full set of processes certified twice during the validity period.</p> <p>The monitoring is performed by Inveo with direct clients (or licensed certification bodies with their own customers according to the same process)</p>
Suspension/Withdrawal	<p>Suspension decision may be taken in case:</p> <ul style="list-style-type: none"> Persisting non compliance, Failure to take corrective action following a review, Opposition to a periodical on site inspection, Non payment of the fees <p>Non compliant companies have 4 months to remediate. Without remediation within this period, Inveo (or licensed certification bodies) are then authorised:</p>

	<ul style="list-style-type: none"> • To withdraw the certification • To reduce the scope of certification
Guarantees	No
Complaint handling	<p>Complaints can be lodged in writing to Inveo Srl Inveo (or licensed certification bodies) by every companies or individuals.</p> <p>Inveo (or licensed certification bodies) directly handle the complaints and answer to the plaintiff within 2 months period.</p>
Dispute resolution process	In case of failure of the internal resolution process, a persisting dispute can be brought before the Data Protection Authority or accreditation body (Regulation EC 765/2008)

ANALYSIS	
GDPR relevance	Article 24
Benefits	<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>
Limits	<p>Paying access: The standard is accessible with a fee</p>
Evolution and Improvement	<p>EU-wide scheme: The scheme can be managed under license and could be licensed to other and larger certification bodies once approved by the European authorities.</p>

Table 3.9 ISDP©10003 Data Protection Certification

10. JIPDEC PrivacyMark System

<p>JIPDEC PrivacyMark System</p>	
IDENTITY	
Owner	JIPDEC
Country	Japan
Creation date	1998
No. of certification issued	15 613
List of certified entities	<p>The public list is available on JIPDEC's website (In Japanese) https://robins.jipdec.or.jp/robins/reference_ImportSearchAction.do?groupCode=003</p>
Licensing Policy	No
Contract Arrangement	<p>The Privacy Mark Grant Agreement signed between JIPDEC and the certified body defines:</p> <ul style="list-style-type: none"> • The mark's rule of use, • The renewal conditions, • The dispute resolution process • The withdrawal conditions and consequences.
Geographical coverage	National
Scope	Management system

	<p>The scheme assesses whether or not the applicant’s Personal Information Protection Management System (PMS) adequately manage risks on handling personal information.</p> <p>Personal Information Protection Management System” includes paper-based information as well as electronic information while Personal data management system only covers electronic information.</p>
Sector	Any private entities
Type	Voluntary
Validity	2 years
Costs	<p>Application fees: 380 € (51 000 JPY - Nov 2017) The application fees are covering the consistency review made by JIPDEC on the application documents</p> <p>Initial Assessment fees: From 1 500€ to 7 500€ (from 205 000 JPY to 977 000 JPY) The initial assessment fees are covering the full assessment process. The amount of the fees depends of the company size which is appreciated based on the number of employees and amount of capital etc. as specified in the Japan’s Small and Medium-sized Enterprise Basic Act.</p> <p>Small companies</p> <ul style="list-style-type: none"> • Up to 5 employees (wholesalers, retailers and services) • Up to 20 employees for the others <p>Medium</p> <ul style="list-style-type: none"> • Up to 3,7 M€ turnover (50 M JPY) for retailers and services • Up to 7,5 M€ turnover (100 M JPY) for wholesalers • Up to 22 M€ turn over (300 M JPY) for manufacturers and others <p>Renewal fees: From 930 € to 1 500€ (from 123 000 JPY to 205 000 JPY) The renewal assessment fees covers the full assessment process. The fees amount is similarly related of the company size.</p> <p>Use fees: From 450 € to 1 500€ (From 51 000 JPY to 205 000 JPY) The use fee represents the royalty to be paid for a two-year use of the mark.</p>
Website	https://privacymark.org/

FUNCTIONING	
Foundations	<p>The PrivacyMark System is based on the Japanese Industrial Standards JIS Q 15001:2006 - Personal Information Protection Management System - Requirements- standard issued in 2006</p> <p>The high-level content of the JIS Q 15001:2006 standard is accessible for free on JIPDEC’s website: https://privacymark.org/ou0ioa000000013f-att/ThePrivacyMarkSystem.pdf</p> <p>The access to the JIS Q 15001 standard is accessible for a fee</p>
Requirements	<p>JIS Q 15001 defines the following requirements;</p> <ul style="list-style-type: none"> • Personal Information Protection Policy • Plan <ul style="list-style-type: none"> • Specification of Personal Information; • Laws, regulations and other codes stipulated by the state; • Recognition, analysis and measures of risks; • Resources - roles - responsibilities -authorities; • Internal Regulations; • Planning documents; • Preparation for stage of emergency; • Implementation and Operation <ul style="list-style-type: none"> • Operation procedures; • Principles on acquisition • use and provision • Appropriate Control; • Rights of the person concerning personal information; • Education • Personal Information Protection Management System Documents <ul style="list-style-type: none"> • Range of documents • Document control • Record control • Response to complaints and consultations • Inspection <ul style="list-style-type: none"> • Confirmation of operations • Audits • Corrective and preventive actions • Review by the representative of the business entity
Assessor	External bodies or individuals

	<p>All Assessors must be registered with the PrivacyMark Assessor Registration Section. 1 246 assessors have been registered up to now.</p> <p>External auditors make contracts with the Assessment Section of JIPDEC or with certified assessment Bodies registered by JIPDEC.</p> <p>There are three types of assessors.</p> <p>1. Provisional Assessor, To become Provisional Assessor, the applicants must follow a 5-day training session and pass the exam ending the training</p> <p>2. Assessor, To get promoted to Assessor, Provisional Assessors must complete five on-site assessments together with assessor and lead assessor to build skills for auditing and receive recommendations of two or more Lead Assessors.</p> <p>3. Lead Assessor To get promoted to Lead Assessor, Assessor must complete ten or more assessments and receive recommendation of two or more Lead Assessors.</p>
<p>Process</p>	<p>Third party certification</p> <hr/> <p>The candidate submits its application to one of the 12 industry specific bodies to which its activity belongs. In case no industry specific body is available, the candidate is entitled to submit its application to one of the 6 regional bodies or, directly, to JIPDEC.</p> <p>The assessment process encompasses two steps.</p> <p>1. Documentation review</p> <ul style="list-style-type: none"> • Verifies the content of the privacy policy • verifies the content of the Personal Information Management System (PMS) • Verifies the procedure implementing the PMS <p>2. Onsite assessment</p> <ul style="list-style-type: none"> • Verifies the consistent implementation of the PMS • Verifies the risk mitigation measures • Verifies the monitoring procedures set up <hr/> <p>The privacyMark System committee reviews the assessment report.</p> <p>When the report is conclusive, the privacyMark System committee grants the mark to the applicant.</p> <p>It publishes the certified information on the directory available on its website.</p>

Renewal	On request at the end of the validity period
	Full reassessment according to the same conditions than the initial certification.
Monitoring	<ul style="list-style-type: none"> • No random control • Complaint handling • Renewal assessment process at the end of the validity period
Suspension/Withdrawal	<p>The PrivacyMark System Committee can proceed to the withdrawal or the suspension of the PrivacyMark.</p> <p>The sanction level is evaluated with the PrivacyMark Penalty Rules applying a scoring system to the different possible infringements. See details on p10 and p11 https://privacymark.org/ou0ioa00000013f-att/ThePrivacyMarkSystem.pdf</p> <p>JIPDEC evaluates disqualification matters and decides about dismissal of application, suspension of use of the Mark, etc.</p>
Guarantees	<p>Some Japanese authorities require companies to be certified with the PrivacyMark</p> <p>Some Insurance companies offer a discount to companies PrivacyMark’s certified</p>
Complaint handling	<p>The complaint from assessor, applicant or third party can be lodged with the industry specific bodies or with the 6 regional bodies (3275 complaints received in 2016 in the 18 bodies).</p> <p>JIPDEC deals with petitions of objection from certified entities and applicants.</p> <p>The PrivacyMark consumer contact committees in the bodies handle the complaints with their own full-time counselors.</p>
Dispute resolution process	<p>A Protest Assessment Committee (ad hoc) is created to deal with the complaint.</p> <ul style="list-style-type: none"> • JIPDEC receives a written petition of objection from a certified entity or applicant. • The Protest Assessment Committee whose members are composed of external experts is temporarily set up. • Based on the Protest Assessment Committee report, JIPDEC makes a judgement to the petition of objection and sends a written notice of result to the certified entity or the applicant.

ANALYSIS	
GDPR relevance	Article 24
Benefits	<p>One size fits all solution: The JIPDEC's PrivacyMark System is covering all facets of the data protection compliance in one single scheme.</p> <p>Management system approach: The management system certification could be less dependent of quick technological evolutions than process and product certification and thus, be more affordable to SMEs.</p> <p>Widespread adoption: The JIPDEC's PrivacyMark System is one on the pioneer of data protection certification with the ULD in Germany. As underlined by the scheme owner, widespread adoption of the scheme is partly linked to its anteriority and to the fact the scheme was, until the enactment of the data protection law in 2006, the only way for Japanese companies to demonstrate their commitment in data protection.</p> <p>Pricing policy The JIPDEC's PrivacyMark System is offering an original and interesting pricing policy depending on the applicant's size and type of activity.</p>
Limits	<p>National coverage The scheme is closely related to the content of the Japanese Industrial Standards JIS Q 15001:2006 that is not aligned with the GDPR.</p> <p>Out of GDPR's scope: The scheme certifies management systems that is out of Article 42's scope.</p> <p>Paying access: The standard is accessible with a fee.</p>
Evolution and Improvement	<p>Accreditation Assessors of JIPDEC could collaborate and be trained to certify EU approved criteria for data transfers to controllers or processors in Japan.</p>

Table 3.10 JIPDEC PrivacyMark System

11. Privacy by Design Certification

<p>Privacy by Design Certification</p>	
<p>IDENTITY</p>	
<p>Owner</p>	<p>Privacy by Design Centre of Excellence at Ryerson University</p>
<p>Country</p>	<p>Canada</p>
<p>Creation date</p>	<p>2015</p>
<p>Licensing</p>	<p>No</p>
<p>Contract Arrangement</p>	<p>The assessment process is carried out under a separate agreement between the auditor (Deloitte) and the organization applying for the certification.</p> <p>The certification is subject to a licensing agreement between the organization and Ryerson. The Usage Agreement signed between the Privacy by Design Centre of Excellence and the certified body defines;</p> <ul style="list-style-type: none"> • The user obligations, • Authorized and unauthorized use, • Termination conditions, • Liabilities. <p>See for details the usage agreement https://www.ryerson.ca/content/dam/pbdce/certification/Privacy-by-Design-Usage-Agreement.pdf</p>
<p>No. of certification issued</p>	<p>7</p>
<p>List of certified entities</p>	<p>The list is available on Ryerson’s website http://www.ryerson.ca/pbdce/certification/certifications-granted/</p>
<p>Geographical coverage</p>	<p>International</p>

Scope	Products and processes
	The scope of the Privacy by Design assessment may involve an organization's product, service, process or system against privacy by design principles and related privacy control framework using risk scorecard technique (see below for details).
Sector	Any
Type	Voluntary
Validity	3 years
Costs	<p>Three types of costs:</p> <ul style="list-style-type: none"> • Assessment and reassessment fee: variable depending on the size of the applicant • Certification issuance fee: 3 300€ (5 000 CAN \$ in November 2017) • Annual maintenance/licence fee: 850 € (1 250 \$ CAN)
Website	http://www.ryerson.ca/pbdce/certification/
FUNCTIONING	
Foundations	<p>The Ryerson's Privacy by Design Certification Program is based the 7 Foundational Principles of Privacy by Design principles elaborated by Dr. A. Cavoukian during the 1990s.</p> <p>See a full presentation of the Privacy by Design principles on Ryerson's website https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/</p> <p>Deloitte Canada has partnered with Ryerson University to launch Privacy by Design Certification Program by serving as the assessment body to Ryerson leveraging the 7 Foundational Principles of Privacy by Design as the framework for the assessment, which in turn is mapped to 30 measurable data protection/privacy criteria and 95 illustrative privacy controls for assessment purposes where organizations can demonstrate how they comply.</p> <p>The privacy by design assessment framework drafted by Deloitte claims to be aligned with the GDPR and other international legal requirements, industry best practices and data protection</p>

	<p>standards (e.g. the Generally Accepted Privacy Principles, ISO/IEC 29100, ISO/IEC 27001), including regulatory guidance issued by the FTC and Canadian regulators.</p> <hr/> <p><i>Some examples of the privacy by design assessment framework are available on Ryerson’s website:</i> http://www.ryerson.ca/content/dam/pbdce/certification/Privacy-by-Design-Certification-Program-Assessment-Methodology.pdf</p> <p>The full assessment framework is in restricted access to the scheme customers.</p>
<p>Requirements</p>	<p>The applicant must be compliant with all the 30 following criteria;</p> <ul style="list-style-type: none"> • Privacy Governance- Responsibility and Accountability for Policies and Procedures • Privacy Impact Assessments or Privacy Risk Reviews • Privacy Incident and Breach Management • Compliance, Monitoring and Enforcement • Consistency of Privacy Policies and Procedures with Laws and Regulations • Privacy Training • Third Party Protection of Personal Information • Privacy Settings by Default • Data Minimization: Collection Limited to Identified Purpose • Use of Personal Information • Consideration of Privacy in Design Documentation • Privacy in Operational Procedures and Processes • Privacy in Change Management • Positive Sum (the organization can articulate and demonstrate the “positive sum” (e.g. no trade-offs; win/win) characteristics of the solution, product or service.) • Security in Privacy Policies • Safeguarding of Personal Information • Logical Access to Personal Information • Physical Access Controls • Environmental Safeguards • Transmitted Personal Information • Retention and Storage of Personal Information • Disposal, Destruction and Redaction of Personal Information • Testing Security Safeguards • Policies and Commitment • Openness • Purpose of Collection • Notice • Consent and Notice • Access to and Correction by Individuals of Their Personal Information • Right to deletion (“right to be forgotten”) and right to object • Accuracy

	<p>The framework also defines 95 control points for demonstrating the compliance with the criteria. Some examples are available in the presentation of the privacy by design assessment framework.</p> <p>http://www.ryerson.ca/content/dam/pbdce/certification/Privacy-by-Design-Certification-Program-Assessment-Methodology.pdf</p>
Assessor	<p>External auditors (partnership with Deloitte Canada)</p>
	<p>No accreditation process of Deloitte's auditors by the Privacy by Design Centre of Excellence Ryerson.</p> <p>However, Deloitte's auditors are already accredited depending their speciality by the American or Canadian Institute of Chartered Public Accountants; by the Law Society of Upper Canada; by ISO based certification as Certified Information Systems Security Professionals (CISSPs). All of them have also received a certification from the International Association of Privacy Professionals (IAPP).</p>
Process	<p>Third Party Certification</p>
	<p>The assessment process is performed according the following steps:</p> <ol style="list-style-type: none"> 1. The applicant submits its application to the Privacy by Design Centre of Excellence, 2. The Centre of Excellence submits the application to Deloitte Canada that is contracting with the applicant to organize the assessment process. 3. Deloitte's auditors scrutinize the product(s), services(s), conduct interviews, and examine operational processes through technical tests if needed.. 4. Deloitte issues a report to the applicant organization <p>See p 21 of the framework presentation for details https://www.ryerson.ca/content/dam/pbdce/certification/Privacy-by-Design-Certification-Program-Assessment-Methodology.pdf</p> <p>The assessment process is based on:</p> <ul style="list-style-type: none"> • A documentation review during which Deloitte's auditors analyze technology and related architecture, data flows, supporting policy and governance documents, corroborated by interviews. • An on-site inspection evaluating whether the privacy or security control(s) exist and are designed properly through technical tests if needed. <p>The assessment is based on Deloitte's scorecard technique:</p> <ul style="list-style-type: none"> • It provides an overall assessment rating of either "satisfactory", or "unsatisfactory" for each criteria evaluated.

	<ul style="list-style-type: none"> • The overall rating not only reflects the rating of controls being assessed (i.e., “effective” or “ineffective”), but also considers their relevant measurement of significance in achieving the corresponding Privacy by Design criterion or principle (“risk weighting”). • The applicant organization is responsible for closing any gaps identified and must receive a “satisfactory” rating for each criteria to be certified by Privacy by Design Centre of Excellence. <p>See p19 of the framework presentation for details on the rating methodology: https://www.ryerson.ca/content/dam/pbdce/certification/Privacy-by-Design-Certification-Program-Assessment-Methodology.pdf</p> <p>The certification issuance is done according to the following process:</p> <ul style="list-style-type: none"> • The Privacy by Design Centre of Excellence receives and reviews the audit report (the “Privacy by Design Assessment Report”) issued by Deloitte. • The Centre of Excellence issues a decision as to whether certification will be granted. • A seal (the “PbyD Certification Shield”) is then issued to the certified body that is entitled to display the shield on its products and documentation. • The name, certification and validity date are published on Ryerson’s website.
Renewal	<p>On request at the end of the validity period</p> <p>Full reassessment according to the same conditions than the initial certification process</p>
Monitoring	<p>No active monitoring. The Privacy by Design Centre of Excellence relies:</p> <ul style="list-style-type: none"> • On the certified body commitment to annually attest to the maintenance of compliant practices • As well as a public complaint mechanism accessible from its website (see below)
Suspension/Withdrawal	<p>The certification can be suspended during the validity period if any of the following occur:</p> <ul style="list-style-type: none"> • Material breach of usage agreement, • Usage of the seal in a manner inconsistent with permission granted under the agreement, • Failure to keep processes aligned with Privacy by Design principles/Program Requirements, • Failure to report material changes in its practices calling

	<p>into question the certification granted.</p> <p>Temporary withdrawal: The company is temporarily enjoined from using Privacy by Design Certification or the Privacy by Design Certification Shield (seal).</p> <p>The suspension continues until either the certification is terminated as part of the complaint process or until the complaint process is completed and the organization's certification is retained.</p> <p>No time limit is set to remedy to the non-compliance. The timing is linked to the investigation of the complaint and the certified organization's response to it.</p> <p>However, and without adequate response from the certified body within 30 business days, the certification is terminated.</p> <p>On termination, the certified must cease all use and display of the seal. Either the complainant or the subject of a complaint may appeal a decision by Ryerson made within the complaints process. Appeals will be considered by the Privacy by Design Certification Advisory Board.</p>
Guarantees	No
Complaint handling	<p>A complaint can be lodged by a certified body, a third party body or individual from a dedicated webform available on Ryerson's website http://www.ryerson.ca/pbdce/certification/complaints/</p> <p>The complaint management process is fully described in the license agreement (Usage Agreement) signed by the certified and the Centre of Excellence. The process follows these steps:</p> <ol style="list-style-type: none"> 1. Receive complaint 2. Confirm complaint process with complainant 3. Review Complaint (within 5 business days) 4. Decide whether or not the complaint require suspension of certification pending complaint process 5. Submit complaint to organization for response 6. Receive and review response 7. Write report on response 8. Send report to organization and complainant (within 15 days following the response from the certified body) 9. Follow-up <p>See Schedule D of the usage agreement https://www.ryerson.ca/content/dam/pbdce/certification/Privacy-by-Design-Usage-Agreement.pdf</p>
Dispute resolution process	<p>The Usage Agreement also details the dispute resolution process:</p> <ul style="list-style-type: none"> • The dispute resolution process is internally managed by Privacy by Design Centre of Excellence, • Either the complainant or the subject of a complaint may

	<p>appeal a decision by Ryerson,</p> <ul style="list-style-type: none"> The dispute is managed by a dedicated board (“Privacy by Design Certification Advisory Board”) that is voting, based on the report issued by one its member, to sustain or not the appeal.
--	---

ANALYSIS	
GDPR relevance	<p>Article 25 Article 24</p>
Benefits	<p>One size fits all solution: The Privacy by Design Certification is covering all facets of data protection in one single scheme.</p> <p>Management system approach: The scheme offers a similar approach to a management system certification scheme. It requires a privacy by design approach for each criteria rather than a simple regulatory compliance. Thus, the scheme can be seen as a special type of management system certification. This approach could be less dependent of swift technological evolutions than process and product certification and thus, be more affordable to SMEs.</p> <p>GDPR readiness The scheme is active and the requirements have already been updated to be in line with the GDPR</p>
Limits	<p>Non-EU scheme This Canadian scheme also raises the question of the accreditation of non-EU certification bodies.</p> <p>Out of GDPR’s scope: The scheme certifies management systems that do not enter into Article 42’s scope.</p> <p>Scalability 7 certifications have been issued since 2015. This does demonstrate whether or not the process is quickly scalable.</p>
Evolution and Improvement	-

Table 3.11 Privacy by Design Certification

12. Privacy Seal MYOBI Mind Your Own Business Information⁶

<p>Privacy Seal MYOBI Mind Your Own Business Information</p>	
IDENTITY	
Owner	MYOBI B.V.
Country	The Netherlands
Creation date	Not clear from website
Licensing	<p>No information available online regarding the Privacy Seal. Certain forms of licensing, probably regarding other products and services that can be licensed via TTP Associates. http://www.ttp.associates/bedrijfsinformatie</p>
No. of certification issued	58 (by the second half of 2017)
List of certified entities	https://www.myobi.eu/?page=0#block-organizationoverviewblock
Contract Arrangement	Not clear from website
Geographical coverage	National (The Netherlands)
Scope	<p>Mind Your Own Business Information (MYOBI) is an independent third party which facilitates partners in a network with assurances regarding the reliability of company information. https://www.myobi.eu/en</p> <ul style="list-style-type: none"> • The applicant company and its processes are evaluated as a whole for accountability and responsibility. • MYOBI facilitates:

⁶ This template is based on publicly available information collected online during the second half of 2017.

	<ul style="list-style-type: none"> ○ The application of network-driven resilient data processing agreements ○ Doing business and exchanging information in an effective and cost efficient manner <p>Within the MYOBI network of participating companies (TTP), Duthler Associates functions as independent moderator, and TTP Associates as provider of operational services, interoperability services between MYOBI and other TTPs; developer and administrator of taxonomies for attributes and sticky policies for data processing; developer and administrator for cross-certification schemes. http://www.ttp.associates/</p> <p>“MYOBI can grant the Privacy Seal, which is a dynamic way to express, through certification, the level of data protection and privacy security that exists within an organisation. In that way an organisation is transparent towards data subjects, watchdogs and other parties. This level is referred to as a 'maturity level'.” The dynamic character of the Privacy Seal implies, among others, that if displayed online, the Seal is clickable - by clicking the Seal, information is revealed about the results of the privacy assessment on the basis of which the Seal had been granted, the name and contact information of the responsible data protection officer, the link to information in the Data Protection Officer Register held by Duthler Associates. https://www.myobi.eu/en</p>
	<ul style="list-style-type: none"> • The project aims at certifying the compliance of products and procedures in relation to GDPR and other relevant e Dutch lawLaw <p>This Privacy Seal also comes with 7 (1 being the lowest and 7 being the highest) maturity levels designed to express, through certification, the level of data protection and privacy security that exists within an organisation. The system includes as well a level of maturity 0 indicating that the assessment process is ongoing. Each maturity level is colour-coded differently. http://www.ttp.associates/sites/default/files/1603018%20vs1_4%20Privacy%20Seal%20Policy_school.pdf</p>
Sector	Any
Type	Voluntary
Validity	<p>The Privacy Seal is valid for a period of 1 (one) year.</p> <p>The contract regarding the use of the Privacy Seal is signed for a period of 5 years (renewed tacitly for 1 additional year at the expiration of the initial 5 years).</p>

Costs	Not specified on the website
Website	https://www.myobi.eu/ https://www.ttp.associates. http://www.ttp.associates/sites/default/files/1603018%20vs1_4%20Privacy%20Seal%20Policy_schoon.pdf https://www.myobi.eu/sites/default/files/160303%20vs2%20Privacy%20Seal%20Algemene%20Voorwaarden_schoon.pdf
FUNCTIONING	
Foundations	<p>Based on the Dutch Data Protection Law (Wet Bescherming Persoonsgegevens) and General Conditions (attached) as well as GDPR</p> <ul style="list-style-type: none"> • relevant law; official texts available online • According to the business model, a designated company privacy officer is required to attend privacy training at the Duthler Academy.
Requirements	<p>The right to use the Privacy Seal is granted to an organization (or organizational unit) by MYOBI if the following conditions are met:</p> <ul style="list-style-type: none"> • There has been at least one maturity scan and a consultation with the management; and • The company employs a privacy officer (in training) who attends privacy training with Duthler Academy, or • The company employs a Duthler Academy trained and registered privacy officer <p>http://www.ttp.associates/sites/default/files/1603018%20vs1_4%20Privacy%20Seal%20Policy_schoon.pdf</p>
Auditors accreditation	Not clear from website
Process	<p>The following process is necessary in order to obtain the Privacy Seal:</p> <ol style="list-style-type: none"> 1. Maturity scan → short assessment of the state of data protection and information security in the organization 2. Management Consultation led by a Duthler Associates professional with the data protection officer of the assessed organization and the member of the Board of Directors of that organization responsible for data protection. Based on the consultation, the maturity level is assessed as well as the organization's ambitions and aspirations regarding data protection. The so-called legal entity framework is also determined. For determining the legal entity framework, Duthler Associates make use of the proprietary software called SBC Management system. 3. Issuing of the Privacy Seal 4. Technical and operational issues - this step consists of

	<p>the inclusion of the privacy officer in the Privacy Officer Register of the Duthler Academy →</p> <p>5. Counselling is an additional step in the process of renewal of the Privacy Seal, similar to the management consultation, during which the data protection situation and maturity levels are reassessed and adjusted as necessary.</p>
	Assessment: Done by external/third party Duthler Associates
	Certificate issuance: Done by MYOBI
Renewal	<p>The Privacy Seal has a validity of one year. At least 14 days before expiration, a new so-called management consultation can take place to determine if:</p> <ul style="list-style-type: none"> • the use of the Privacy Seal can be renewed for another year and • if the maturity level has to be adjusted (to a lower/higher level). <p>http://www.ttp.associates/sites/default/files/1603018%20vs1_4%20Privacy%20Seal%20Policy_schoon.pdf</p> <p>The contract regarding the use of the Privacy Seal is signed for a period of 5 years after which it is tacitly and automatically prolonged for a year at a time. http://www.ttp.associates/sites/default/files/1603018%20vs1_4%20Privacy%20Seal%20Policy_schoon.pdf</p> <p>MYOBI membership has a minimum duration of three years, after which it is automatically renewed for one year, until the agreement is terminated in accordance with the terms of the connection agreement, the TTP policy. The client may terminate the connection agreement in writing at the end of the duration of the agreement, taking into account a two-month notice period. https://www.myobi.eu/en/general-conditions</p>
Monitoring	<ul style="list-style-type: none"> • Either the company has to nominate a privacy officer who then receives training from Duthler Academy or Duthler Academy supplies the company with a qualified privacy officer. • It is part of the privacy officer's duty to continuously monitor the company's compliance. The management consultation takes place once every year. <p>http://www.ttp.associates/sites/default/files/1603018%20vs1_4%20Privacy%20Seal%20Policy_schoon.pdf</p>
Suspension/Withdrawal	<p>The Privacy Seal can be revoked when:</p> <ul style="list-style-type: none"> • The appointed privacy officer recommends revocation on the ground that management fails to adhere to privacy rules;


	<ul style="list-style-type: none"> The company's privacy policy is not implemented; The company no longer complies with the general terms and conditions relating to the award of the Privacy Seal
Guarantees	<p>No guarantees</p> <p>The Privacy Seal provides no guarantees as to the company's compliance with legal requirements re data protection. Nor does the Privacy Seal guarantee that the organization has adopted measures, tasks, responsibilities in accordance with certain relevant legal requirements.</p> <p>The Privacy Seal is only a transparency measure meant to indicate the level of privacy and data protection that can be expected from the company displaying it. http://www.ttp.associates/sites/default/files/1603018%20vs1_4%20Privacy%20Seal%20Policy_schoon.pdf</p>
Complaint handling	Not clear from website
Dispute resolution process	<p>Section 9.2 of the general conditions of the scheme suggests</p> <ul style="list-style-type: none"> - using arbitration in front of a body specializing in the resolution of ICT disputes, Stichting Geschillenoplossing Automatisering (SGOA) in The Hague - or have the case brought to a Dutch Court. <p>see also clause 7 of https://www.myobi.eu/en/general-conditions</p>

ANALYSIS	
GDPR relevance	Article 24
Benefits	<p>One-size-fits-all solution: Privacy Seal MYOBI is covering all facets of data protection in one single scheme.</p> <p>Innovative approach Privacy Seal MYOBI suggests certifying companies where MYOBI has trained an internal privacy officer or provide an external one.</p> <p>Alternative to the DPO certification The approach suggested by MYOBI offers to certify the privacy officer's activity rather than his competencies. It valorizes and recognizes privacy officer's activity for maintaining compliance and its certification</p>
Limits	<p>National coverage</p> <p>Out of GDPR's scope: The scheme certifies a management system and thus falls outside the scope of Article 42 GDPR.</p>

Evolution and Improvement	

Table 3.12 Privacy Seal MYOBI Mind Your Own Business Information

13. Privacy Audit Proof certification & seal⁷

<p>Privacy Audit Proof certification & seal</p>	
<p>IDENTITY</p>	
<p>Owner</p>	<p>NIVRA (the Royal Netherlands Institute for Registered Accountants) and NOREA (the Netherlands Organization of Registered IT Auditors) are joint owners of the Privacy Audit Proof. The corresponding privacy seal is issued by NOREA. https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/addendum-norea-privacy-audit-2016.pdf</p>
<p>Country</p>	<p>The Netherlands</p>
<p>Creation date</p>	<p>After 2001 (the date when the Dutch Data Protection Act came into force).</p>
<p>Licensing</p>	<p>In accordance with the NOREA Privacy Audit Standard 3600, external assessments and certification can be conducted/issued by certified accountants and certified IT auditors with expertise in the areas of data protection (law) and IT. https://www.privacy-audit-proof.nl/</p> <p>For Standard 3600, see https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/richtlijn_3600_privacyaudit.pdf</p> <p>For the updated (2017) version of the standard, namely 3600n, see https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/addendum-norea-privacy-audit-2016.pdf</p>
<p>No. of certificates issued</p>	<p>At the time when this template was last updated (15 Nov 2017), the online register was listing as certified 6 data processing activities conducted by 4 organizations, namely: Liander Infostroom (smart meter data); the Netherlands Credit Bureau; the system of social-statistical data of the Netherlands Central</p>

⁷ This template is based on publicly available information collected online during the second half of 2017.

	Bureau for Statistics; other data processing activities of the Netherlands Central Bureau for Statistics; the Vehicle Registration Plate Register of the Netherlands Road Traffic Agency; and the Parking Register of the same Netherlands Road Traffic Agency.
List of certified entities	The Directory of certified NOREA clients is public and searchable online at: https://www.privacy-audit-proof.nl
Geographical coverage	National (The Netherlands)
Scope	Data Processing
	A full-scope audit on the manner in which and the extent to which an organization complies with the requirements of the Dutch data protection act (Wbp). (Please note that this item was last updated in November 2017.) Decisions are taken in accordance with / based on the Privacy Audit Directive 3600. The purpose of this directive is to establish a basis and provide guidance for conducting assurance in the area of data protection. https://www.privacy-audit-proof.nl/
Sector	Any
Type	Voluntary
Validity	1 year
Costs	Yearly registration fees related to the privacy seal were EUR 300 in 2006. Current rate to be confirmed by scheme owner. https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/gebruiksvoorwaarden_keurmerk.pdf
Website	https://www.privacy-audit-proof.nl/ https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/gebruiksvoorwaarden_keurmerk.pdf
FUNCTIONING	

<p>Foundations</p>	<p>Prompted by the adoption and entry into force of the Dutch data protection act.</p> <p>Further informed by various documents, such as the Privacy Audit Framework published in 2001 and the accompanying guidance issued by the Dutch Data Protection Authority.</p> <p>Other relevant sources used to derive assessment criteria might include sectoral codes of conduct, case law, etc.</p> <p>The assessment leading to granting the privacy certificate & seal is based on the NOREA Privacy Audit Standard 3600, now updated to version 3600n.</p> <p>The NOREA Standard 3600 was updated following the introduction of a data breach reporting duty in 2016 and the publication of the guidance on securing personal data issued by the Dutch Data Protection Authority. The latest version of the Privacy Audit Standard 3600, renumbered 3600n, is dated 2017.</p> <p>The text of the updated standard mentions that existing assessment criteria are in need of constant changing/updating so as to account for changes in legislation, technological developments, etc.</p> <p>https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/addendum-norea-privacy-audit-2016.pdf</p> <p>Various types of information accessible online at:</p> <ul style="list-style-type: none"> • https://www.privacy-audit-proof.nl/ • https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/richtlijn_3600_privacyaudit.pdf • https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/addendum-norea-privacy-audit-2016.pdf • https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf
<p>Requirements</p>	<p>The text of the updated standard 3600n mentions that existing assessment criteria are in need of constant changing/updating so as to account for changes in legislation, technological developments, etc. To compensate for the fact that a standard cannot be updated with every such change, NOREA instruct assessors applying the standard to mention relevant said changes in their privacy assessment reports.</p> <p>See section “foundations” above for the sources of assessment criteria as defined in standard 3600n.</p> <p>https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/addendum-norea-privacy-audit-2016.pdf https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/raamwerk_privacyaudit.pdf</p>

	<p>Assessment criteria include but are not limited to issues related to:</p> <ul style="list-style-type: none"> • plan-do-check-act activities • risk assessment • information security • confidentiality • monitoring and enforcement • various other issues to do with data processing • data breach reporting • use of PETs (privacy enhancing technologies) and encryption
Assessor	<p>This scheme allows also for external assessors under explicit conditions.</p> <p>In accordance with the NOREA Privacy Audit Standard 3600, external assessments and certification can be conducted/issued by certified accountants and certified IT auditors with expertise in the areas of data protection (law) and IT. Third parties can provide additional knowledge data protection and/or IT if and where necessary.</p> <p>https://www.privacy-audit-proof.nl/ For Standard 3600, see https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/richtlijn_3600_privacyaudit.pdf For the updated (2017) version of the standard, namely 3600n, see https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/addendum-norea-privacy-audit-2016.pdf</p>
Process	<p>Certification by scheme owner and by external experts</p> <hr/> <p>The object of assessment falls in two main categories:</p> <ul style="list-style-type: none"> • the totality of measures and procedures adopted for a specific form of personal data processing and • management declarations regarding the above. <p>The process is informed by:</p> <ul style="list-style-type: none"> • professional norms and codes of conduct • the Privacy Audit Framework and accompanying guidance issued by the Dutch Data Protection Authority and • the specific remit as outlined in the contract between assessor and his client. <p>https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/richtlijn_3600_privacyaudit.pdf</p> <hr/> <p>A positive assurance report and additional requirements regarding good functioning entitle the client to being issued the privacy seal. The right is issued jointly by NIVRA and NOREA in writing. The seal can be used on the client's correspondence and publicity material and on the public pages of his website. If the seal is displayed on the client's website, it must include a hyperlink to the NOREA public register.</p>


Renewal	<p>The certificate/privacy seal can be renewed within three months calculated from the expiration date. All requirements of the original assessment must be met for the certificate/privacy seal to be renewed. Also, the object of certification must remain the same as the original one.</p> <p>Full reassessment</p>
Monitoring	Monitoring is a condition for issuing a client with the privacy seal and is conducted over the period of validity of the seal (i.e. 12 months).
Suspension/Withdrawal	<p>As part of the certification process, the certified party is informed about the possible changes of the certification.</p> <p>NIVRA and NOREA retain the right to suspend or end certified clients, permanently or temporarily if the client does not comply with his obligations. A grace period of three months is allowed for the client to remedy faults. https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/gebruiksvoorwaarden_keurmerk.pdf</p>
Guarantees	No
Complaint handling	No information available.
Dispute resolution process	No information available.

ANALYSIS	
GDPR relevance	Article 24
Benefits	<p>One-size-fits-all solution: NOREA is covering all facets of data protection in one single scheme.</p> <p>Innovative approach The scheme assesses the existence and relevance of a permanent quality control plan (Plan-Do-Check-Act or PDCA) applied to data protection compliance. This approach could be helpful to closely monitor the compliance over time.</p>

Limits	National coverage The scheme is based on Dutch law and nothing on the owner’s website says whether or not the scheme intends to comply with the GDPR Out of GDPR’s scope: The scheme certifies a management system and thus falls outside the scope of Article 42 GDPR.
Evolution and Improvement	

Table 3.13 Privacy Audit Proof certification & seal

14. TRUSTArc APEC CBPR

<p style="text-align: center;">TRUSTe APEC CBPR</p>	
IDENTITY	
Owner	TrustArc Inc. (TRUSTe LLC is a subsidiary of TrustArc Inc.)
Country	USA
Creation date	2013
No. of certification issued	21
List of certified entities	Public list available on TrustArc website https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list
Licensing	No
Contract	<p>The agreement signed with the client ("TRUSTe Technology Terms of Service") defines:</p> <ul style="list-style-type: none"> • The contractual process, • Pricing and payment conditions, • Obligations for parties • Termination conditions and process, • Intellectual property, • Confidentiality, • Indemnification conditions, • Limits of liabilities
Geographical coverage	Regional
Scope	Processes
	Cross-border data transfers from TRUSTe-certified companies to

	<p>any companies within the APEC area.</p> <p>Online and offline data collection and processing practices of businesses as being in compliance with the requirements of the CBPR system.</p> <p>To be eligible for TRUSTArc APEC certification, businesses must have their primary location in the United States and be subject to the jurisdiction of the Federal Trade Commission.</p>
Sector	All sectors subject to Federal Trade Commission Jurisdiction
Type	Voluntary
Validity	1 year
Costs	<p>The conformity assessment is charged to the applicant on a case by case basis depending on the evaluation scope.</p> <p>No license fees</p>
Website	https://www.trustarc.com/products/apec-certification/
FUNCTIONING	
Foundations	TRUSTe APEC Privacy Certification Standard is based on the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) Program Requirements.
	<p>TRUSTe APEC Privacy Certification Standard is accessible for free on the TRUSTArc website</p> <p>https://download.trustarc.com/?f=LH7RIJRS-627</p>

Requirements	<p>The TRUSTe standard includes the APEC CBPR programme requirements slightly rephrased in order to make them easily auditable. The requirements can be categorized as follows:</p> <ul style="list-style-type: none"> • Collection Limitation • Use of Personal Information • Choice • Collection and Use of Third Party Personal Information • User Public Profiles • Access • Promotional and Newsletter Media Communications • Material Changes • Data Security • Data Quality and Integrity • Data Retention • Third Party Data Sources • Service Providers • Training • User Complaints and Feedback • Data Breach • Accountability and Cooperation with TRUSTArc <p>For details, see TRUSTe APEC Privacy Certification Standard https://download.trustarc.com/?f=LH7RIJRS-627</p>
Assessor	<p>Internal auditors</p> <p>TRUSTe is accredited as Accountability Agent by the APEC CBPR system Joint Oversight Panel (JOP) for a renewable period of 2 years.</p> <p>The applicant must demonstrate:</p> <ul style="list-style-type: none"> • The processes in place to ensure its independence, • The organization of the certification process, • The monitoring and compliance review processes, • The renewal process, • The dispute resolution process, • The mechanisms in place for enforcing the CBPR program requirements <p>For details, see Accountability Agent Recognition Criteria https://cbprs.blob.core.windows.net/files/Accountability%20Agent%20Recognition%20Criteria.pdf</p>
Process	<p>Third party certification</p> <p>TRUSTe performs an initial assessment of applicant’s compliance through a document review and technical assessment (web crawling)</p> <p>TRUSTe then provides a comprehensive report to the applicant’s outlining findings regarding compliance with TRUSTe’s Privacy</p>

	<p>Certification Program Requirements</p> <p>TRUSTe then verifies that any required changes as outlined in the findings report have been properly implemented; and</p> <p>Upon successful conclusion of the above-listed steps, TRUSTe certifies that the applicant is in compliance with their program requirements.</p> <p>TRUSTe posts CBPR-certified company online on its website</p> <hr/> <p>The privacy certification seal is issued by TRUSTe.</p> <p>The electronic seal remains hosted on TRUSTe’s web servers. It offers the capacity for TRUSTe to closely monitor the number of bodies which are displaying the seal and opportunity for end-users to quickly check the veracity of the certification on TRUSTe’s website.</p>
Renewal	<p>On request at the end of the validity period</p> <hr/> <p>Full reassessment according to the same process than the initial certification process</p>
Monitoring	<ul style="list-style-type: none"> • Random auditing of certified bodies is currently in discussion at TRUSTe • Third party complaints can be lodged on TRUSTe website • Web crawling, email seeding and web traffic analysis are also used • No monitoring directly done by APEC authorities • Random enforcement performed by national authorities
Suspension/Withdrawal	<p>In the event TRUSTe reasonably believes that participant has materially violated its certification standards, the participant may be placed on suspension.</p> <p>The participant will be considered to be on suspension immediately upon receiving notice and shall last until such time as the participant has corrected the material breach or Certification Standards violation to TRUSTe satisfaction, but not for a period of greater than six months unless mutually agreed by the Parties.</p> <p>At the end of the suspension period, TRUSTe decides :</p> <ul style="list-style-type: none"> • that a participant has complied with its suspension obligations and satisfying any lingering concerns, • extend the suspension period by mutual agreement with the participant, • determine that the suspension obligations were not complied with resulting in the immediate termination of the client for cause.


Guarantees	No
Complaint handling	<p>A complaint can be lodged by a third party body or individual from from the dedicated webform (In-house Feedback and Dispute Resolution System) available on TRUSTe’s website. https://feedback-form.truste.com/watchdog/request</p> <p>Interestingly, TRUSTe requires the certified bodies to similarly provide a convenient complaint handling process on their own website and actively cooperate to the dispute resolution with TRUSTe.</p>
Dispute resolution process	<p>TRUSTe suggests a two steps process described in the document</p> <ul style="list-style-type: none"> • First contact with TRUSTe certified body to find an agreement. • In case of failure, then directly contact TRUSTe • The complaint investigation is done by TRUSTe’s internal Chief Financial Officer department • A written response is provided within 10 business days. • A written notice of complaint Resolution is sent to both complainant and participant notifying them of the final decision and closure of the complaint. • Report Complaint Statistics and Case Notes

ANALYSIS	
GDPR relevance	Article 46
Benefits	<p>Scope Certification schemes focusing on international data transfer remains rare. TRUSTe APEC CBPR scheme offers an interesting and valuable insight on cross border data flows certification.</p> <p>Monitored approach The scheme arrangement is very similar to the arrangement suggested in Article 42 GDPR in which the authorities are entitled to draft the requirements and, then, accredit private certification bodies to manage the scheme under their monitoring.</p> <p>The choice made by the CBPR board to renew the certification and accreditation process every 2 years demonstrates its wish to ensure a close monitoring on the accountability agents.</p>
Limits	<p>Regional coverage The scheme is closely related to the content of the APEC CBPR. These rules are not aligned with the GDPR requirements . Amutual recognition would require additional alignment work.</p>

Evolution and Improvement	-
----------------------------------	---

Table 3.14 TRUSTArc APEC CBPR

15. TÜV Italia - ISO/IEC 27001 certification scheme

<p>TÜV Italia Certificazione di Sistema di Gestione delle Informazioni secondo la norma ISO/IEC 27001</p> <p>TÜV Italia ISO/IEC 27001 certification scheme</p>	
IDENTITY	
Owner of the scheme	TÜV Italia
Country	Italy
Creation date	2001
Licensing	Accredia granted to TÜV Italia the accreditation for auditing and issuing ISO/IEC 27001 certificates
Contract Arrangement	<p>The contract between the applicant organization and the TÜV contains provisions reflecting ISO 17021-1:2015 requirements</p> <ul style="list-style-type: none"> • audit programme, • licensing conditions for the certified body, • suspension and withdrawal conditions, • claims, • use of information on certification
No. of certification issued	30
List of certified entities	The list is available on Accredia's website http://services.accredia.it/ppsearch/accredia_companymask_remote.jsp?
Geographical scope	Italy
Functional scope	Management system

	The ISO/IEC 27001 standard specifies the requirements, implementation and maintenance of a management system for information security.
Sector	Any
Type	Voluntary
Validity	3 years
Costs	<p>It depends on the size of the applicant (in terms of personnel and number of sites in scope) and is determined on a case by case basis.</p> <p>The ISO/IEC 27006 Annex B offers guideline for the determination of a timeframe required for each audit type</p>
Website	https://www.tuv.it/it-it/settori/telecomunicazioni-informatica/certificazioni-ict/iso-iec-27001
FUNCTIONING	
Foundations	<p>The scheme is based on the ISO/IEC 27001 standard revised in 2013</p> <p>The ISO/IEC 27001:2013 standard "specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (Hereinafter ISMS) within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization".</p> <p>The standard defines 114 specific controls, categorized under one of the 14 different "Control Goals".</p> <p>Section 15.1 applies to the compliance with legal requirements and aims at preventing breaches with regulations</p> <p>Subsection 15.1.4 specifically refers to Data protection and privacy of personal information control. It aims to ensure the compliance of IT operations with relevant legislations, regulations, and, if applicable, contractual clauses.</p>
	<p>Accessible upon payment on the ISO website https://www.iso.org/obp/ui/#iso:std:iso-iec:27013:ed-2:v1:en</p>
Requirements	<p>The ISO/IEC 27001:2013 standards defines:</p> <ul style="list-style-type: none"> • Purpose/Field of Application • References regulatory

	<ul style="list-style-type: none"> • Terms and Conditions and definitions • Background of organization • Leadership • Planning • Support • Activities • Evaluation of performance • Improvement <p>In Annex A of ISO/IEC 27001:2013, the following 14 listed "Control Goals" are identified as possible risk control mechanisms:</p> <ul style="list-style-type: none"> • Security Policies Information dealing with how information policies are written, reviews, and overhauled; • Organization of security of the information Detail how roles and responsibilities are assigned; also includes controls for mobile devices and telework; • Security of Human Resources It is about the controls before, during and after the work relationship; • Asset Management includes durable and non-durable goods, including information classification and management of social media); • Access Control covers all aspects of access, control requirements, management of user and system access and control of applications; • Encryption relates to the encryption and control of access key management; • Physical and environmental safety detail the controls applicable to security areas and equipment; • Security of Operations includes controls performed on IT security operations, such as control of operating software, malware protection, backup, recording, monitoring, technical management of vulnerabilities and audit considerations; • Communications Security includes network security controls, segregation, network services, and network security transfer of information and messages; • Acquisition, development and system maintenance devoted to controls for the security requirements of information systems and security in development and support processes; • Relations with suppliers handle controls to monitor suppliers throughout the supply chain; • Related incident management to the security of the information includes controls for alerting security events and any eventualities criticality, procedures to intervene and the collection of evidence; • Safety aspects of information in the management of operation continuity determine the necessary controls for planning a secure
--	--

	<p>business continuity, including procedures, verification practices, and a redundancy of the system;</p> <ul style="list-style-type: none"> • Conformity applies to the checks required to identify the laws and regulations in force and to conduct information security audits.
Assessor	Internal auditors
	TÜV Italia is accredited as organization against the ISO/IEC 17021
Process	Third party certification
	<p>Starting certification test Applicant organization must provide the data asked by the questionnaire form:</p> <ul style="list-style-type: none"> • Company general data (name, address(es), VAT number) • Scope of the management System • Number of persons working in scope • Info on software development • Presence of other management systems <p>Preliminary visit (pre-audit) On-demand execution consisting in a preliminary check to analyze gaps and to evaluate the compliance of the customer management system to the requirements of the standard. Results are briefly recorded by the audit team and are considered indicative (not strictly part of certification process) and the duration cannot exceed 2 days.</p> <p>1st stage audit (Initial Document Examination and Initial Visit) On-site examination (normally carried out at applicant company headquarters) by TÜV Italia technicians to verify the compliance with applicable regulatory requirements and assess suitability of the documentation of the information security management system to the requirements of the Standard (any document deficiencies must be corrected before the 2nd stage audit). The 1st stage audit assesses the degree of preparation for the 2nd stage audit and results in a special report summarizing the outcome of the initial documentation assessment.</p> <p>Verification of Stage II (2nd stage audit) Verification and closing of any non-compliance to obtain certification (which can include any subsequent audits, or post audit, for the verification of remedial actions required during the initial verification). Controlling the implementation of the management system, document analysis, field observations, staff interviews, which successfully leads when issuing a certificate.</p> <p>Sending Report and Certificate The sending of the technicians/engineer report and certificate, pending approval of the Board of Directors (Approval Committee or Certification Board), after which the annual surveillance checks are added.</p>

	<p>The certification issuance must be approved by the Board of Directors/Approvals Committee after having received and successfully tested the audit report. The documents certifying the certification consist of:</p> <ul style="list-style-type: none"> • The certificate - an identification number with corresponding revision of the certificate, the certified company's contact details, any applicable accreditations, logo of the accreditation organization, frequency of surveillance audits, and the signature of the authorized officer at TÜV Italia. • The resolution letter of the certification - stating the conditions for the renewal of certification, the date of expiry (fixed 3 years after expiry of previous certificate), time limit for next surveillance audit to be performed, and information about use of certification mark. • The inscription of the certified company's details into Accredia database.
Renewal	On request at the end of the validity period
	Full reassessment according to the same process than the initial certification process
Monitoring	<p>Surveillance audit - During the three year validity period, there are two annual surveillance audits aimed at confirming the validity of the certification. The first surveillance audit is performed 12 months after completion of the 2nd stage audit and the second surveillance audit must be performed 12 months after that.</p> <p>Special audit - TÜV Italia reserves the right to conduct an unplanned audit for a certified organization. These audits are performed in response to valid and proven reasons (at the opinion of TÜV Italia) which are communicated to the relevant organization. Three different types of audits:</p> <ul style="list-style-type: none"> • audit to lift the suspension of the certificate; • extension audit or variation of the scope; <p>Additional special audit - It can be triggered because important changes had been made to the management system of the certified company (subsequently required to notify TÜV Italia) or complaints/reports relating to the operation of the management system or information about the non-compliance of the conditions under which the certificate has been granted or improper use of the certificate or mark, the Approval Committee's request to intensify frequency of monitoring following the evaluation of dossier certification, etc.</p> <p>ISO/IEC 17021 requires that certified organizations are monitored only through onsite audits.</p>

Suspension/Withdrawal	<p>TÜV Italia has the right to reduce the scope of the certification to exclude the parts that do not respect the requirements, if the organization has failed, persistently or severely, to respect the scheme requirements.</p> <p>TÜV Italia, for reasons deemed serious and explained in writing the relevant certified organization, may suspend, for a period of not more than 6 months, the validity of the certification already granted. The organization loses the right to use the trustmark and suspension can take place for several reasons:</p> <ul style="list-style-type: none"> • non-performance of post-audits to verify the effective closure of corrective actions defined in the non-conformity report; • organization does not perform surveillance audits as scheduled; etc. <p>If conditions for the certificate re-activation are not satisfied, then the certificate is definitely withdrawn and the contract terminated.</p>
Guarantees	No
Complaint handling	<p>The General regulation of the scheme (“Regolamento Generale per la Certificazione dei Sistemi di Gestione”) defines the complaint handling process as follows:</p> <ul style="list-style-type: none"> • Complaints from third party bodies or individuals can be lodged to TÜV Italia in writing (email is also accepted). • TÜV Italia provides a response about complaint’s admissibility to the complainant within 10 working days. • The complaint is then managed by a member of TÜV Italia board, external to the initial certification process, who is dedicated to the case investigation. • The outcome is communicated to the stakeholders once a decision has been issued (No public information without stakeholder consent)
Dispute resolution process	If TÜV Italia’s decision does not satisfy one of the parties, the general regulation of the scheme entitles them to bring the case before the Court in Milan.

ANALYSIS

GDPR relevance	Art 32
-----------------------	--------

Benefits	<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.</p> <p>The ISO/IEC 27001 is progressively becoming a market standard increasingly required by IT buyers. This trend could be speed-up with the entry in force of Article 32 GDPR.</p>
Limits	<p>Access: The standard is accessible with a fee</p> <p>Out of the GDPR’s scope Refers to management systems, ou of Art. 42 `s scope</p>
Evolution and Improvement	-

Table 3.15 TÜV Italia - ISO/IEC 27001 certification scheme

Annex 4 Accreditation survey

4.1 Accreditation survey questionnaire

<p>Information about the respondent</p>	<p><u>Q1a.</u> Information about the respondent</p> <ol style="list-style-type: none"> 1. Name of the organisation: 2. Type of organisation: 1.Data Protection Authority/Information Commissioner 2.National Accreditation Body) 3. Country: 4. Contact person filling the survey and email address: <ol style="list-style-type: none"> a. <u>Q1b.</u> Do you consent to the processing of your personal data for the reasons outlined in the Introduction of the survey? [Please note you may withdraw your consent at any time before the publication of the Report in May 2018] <ul style="list-style-type: none"> ■ Yes, I agree ■ No, I don't agree
	<p><u>Q1c.</u> Do you agree to publish your name along with your answers in the Report?</p> <ol style="list-style-type: none"> 1. Yes, publish my name 2. No, publish only my answers and the name of the organisation
<p>For Data Protection Authorities/Information Commissioners</p>	<p><u>Q2.</u> Does the DPA plan to conduct accreditation of certification bodies in your country?</p> <ul style="list-style-type: none"> • Yes • No • I don't know yet
	<p><u>Q3.</u> What will the role of the National Accreditation Body be in relation to the GDPR certification in your country?</p> <ol style="list-style-type: none"> 1. The Accreditation Body will play no role. Only the DPA will accredit certification bodies 2. The Accreditation Body will accredit certification bodies and the DPA will provide additional requirements. 3. Other <ul style="list-style-type: none"> ○ Please elaborate: [open question] 4. No plans yet.
	<p><u>Q4a.</u> In case the DPA plans to conduct the accreditation without the National Accreditation Body. Do you plan to follow the requirements of the EN ISO/IEC 17065 standard?⁸</p>

⁸ ISO/IEC 17065:2012, Conformity assessment - Requirements for bodies certifying products, processes and services.

	<ul style="list-style-type: none"> • Yes, it is required by the GDPR • Yes, even though it is not required in the GDPR • No, it is not required • No [other reasons] <ul style="list-style-type: none"> ○ Please elaborate [open question]
	<p><u>Q4b.</u> Do you have experience with accreditation of <u>processes</u> in line with the EN ISO/IEC 17065?</p>
	<p><u>Q5.</u> In case the DPA plans to conduct the Accreditation without the National Accreditation Body, which of the following assessment techniques are likely to be applied for accreditation of certification bodies in the field of data protection <u>in your country</u>? Please rate on a scale from 1 to 3 [where 1= very likely, 2 = neutral, and 3 = least likely]</p> <ul style="list-style-type: none"> – on-site assessment – remote assessment – witnessing⁹ – document review – file review – measurement audits – validation audits – unannounced visits – interviewing – other [Please elaborate]
	<p><u>Q6.</u> In case the DPA plans to be involved in Accreditation together with the National Accreditation Body, which do you think is the scope of "<u>additional requirements</u>" of Art. 43(1)(b)?¹⁰</p> <ul style="list-style-type: none"> • Requirements related to the expertise of the certification body and its auditors in the field of data protection • Requirements related to procedural guarantees and assessment techniques related to the accreditation process (e.g. sanctions, how to deal with non-conformities, conflict of interest policy, etc.) • Both options above • Other [Please elaborate]
	<p><u>Q7.</u> Can you provide some examples of such 'additional requirements', necessary for the accreditation of certification bodies in the data protection field? [free field]</p>

⁹ "Observation by the accreditation body of a conformity assessment body carrying out conformity assessment activities within its scope of accreditation" ISO/IEC 17011.

¹⁰ Art.43(1)(b) GDPR: "the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56."

	<p><u>Q8.</u> Do you think that the DPAs should recognise accreditation granted in other EU Member States?</p> <ul style="list-style-type: none"> • Yes • Yes, but only when they are granted by DPAs (i.e. not National Accreditation Bodies) <ul style="list-style-type: none"> ○ [Please elaborate] • No <ul style="list-style-type: none"> ○ [Please elaborate] • I don't know
	<p><u>Q9.</u> In your view, which of these factors are relevant to assess the expertise of an auditor conducting a <u>certification process</u>? [please rate from 1 to 6, where 1=very relevant, and 6=not relevant at all]</p> <ul style="list-style-type: none"> • Educational background relevant to data protection • Proven work experience in the public sector in the field of data protection • Proven work experience in the private sector in the field of data protection • Working experience with audits and/or inspections • Certified auditors (for instance CIA or other certification)¹¹ • Certified data protection expert. • Other [Please elaborate]
	<p><u>Q10a.</u> Do you think that additional training should be provided to the auditors of the certification bodies? –Yes (<u>Q10b</u>) What kind of training and by whom? [open question]</p> <p>-No [Please elaborate]</p>
	<p><u>Q11.</u> In case of single-issue certifications (i.e. certifications covering only one aspect in the GDPR – e.g. data security or data portability), do you think that the certification body and its auditors, should:</p> <ul style="list-style-type: none"> • Primarily demonstrate general knowledge on the data protection legislation • Primarily demonstrate specific knowledge on the topic of the single-issue certification e.g. data security • Demonstrate knowledge on both the above issues. • Other [Please elaborate]
	<p><u>Q12a.</u> How do you think the independence and integrity of a certification body and its auditors can be assessed and demonstrated in the field of data protection? [please rate from 1 to 5, where 1=very relevant, 5 not likely at all]</p> <ul style="list-style-type: none"> • The certification body is already accredited by the National Accreditation Authority in other fields. • Adherence of the certification body to Codes of

¹¹ See <https://na.theiia.org/certification/CIA-Certification/Pages/CIA-Certification.aspx>

	<p>Conduct</p> <ul style="list-style-type: none"> • Reputation • Written legally binding commitments. • The certification body is a member of a European or International Association. • Other <ul style="list-style-type: none"> ○ [Please elaborate (Q12b)]
	<p>Q13. Do you plan to conduct <u>certification</u> of organisations (controllers/processors)?</p> <ul style="list-style-type: none"> • No, accredited certification bodies will conduct the certification • Yes, the national DPA will conduct the certification • Yes, both, the national DPA and accredited certification bodies will conduct • Other <ul style="list-style-type: none"> ○ [Please elaborate]
	<p>Q14. Do you plan to charge a fee for the accreditation process?</p> <ul style="list-style-type: none"> • Yes [Could you provide a range of applicable fees?] • No • Not applicable, the DPA will not conduct the accreditation process
	<p>Q15. Would you like to add something on the topic? [open field]</p>
For National Accreditation Bodies	<p>Q2. Does the National Accreditation Body plan to conduct accreditation of certification bodies based on the General Data Protection Regulation (Art. 43) <u>in your country</u>?</p> <ul style="list-style-type: none"> • No, the Accreditation Body will play no role. Only the Data Protection Authority/Information Commissioner will accredit certification bodies • Yes, the Accreditation Body will accredit certification bodies and the DPA will provide additional requirements • Yes, other <ul style="list-style-type: none"> ○ [Please elaborate] • No plans yet.
	<p>Q3. Against which conformity assessment standard does the National Accreditation Body accredit? [Open field]</p>
	<p>Q4. Do you have experience with accreditation of <u>processes</u> in line with the EN ISO/IEC 17065?</p>
	<p>Q5. Please name the stages of the accreditation process you follow in case of accreditation of certification bodies (e.g. pre-assessment, initial assessment). Provide links to documents, where available. [Open question]</p>

	<p><u>Q6.</u> Which of the following assessment techniques are likely to be applied for accreditation of certification bodies in the field of data protection <u>in your country</u>? Please rate on a scale from 1 to 3 [where 1= very likely, 2= neutral, and 3 = least likely]</p> <ul style="list-style-type: none"> – on-site assessment – remote assessment – witnessing¹² – document review – file review – measurement audits – validation audits – unannounced visits – interviewing – other [Please elaborate]
	<p><u>Q7.</u> Does the national law on accreditation in your country, include requirements, procedures, or safeguards for accreditation of certification bodies, in addition to those of the Regulation 765/2008?</p> <ul style="list-style-type: none"> • Yes [please provide link to the national law, and briefly explain the requirements, procedures, or safeguards] • No • I don't know
	<p><u>Q8a.</u> The General Protection Regulation provides the option to Member States to select a model of accreditation, in which the National Accreditation Body conducts the accreditation based on the ISO/IEC 17065 and the Regulation 765/2008, and receives a set of "additional requirements" from the national Data Protection Authority.</p> <p>Are you aware of any other areas in your country, where the National Accreditation Body collaborates with a competent public authority in another field?</p> <p>-No -Yes [open field (<u>Q8b</u>)]</p>
	<p><u>Q9a.</u> The General Protection Regulation provides the option to Member States to select a model of accreditation, in which the National Accreditation Body conducts the accreditation based on the ISO/IEC 17065 and the Regulation 765/2008, and receives a set of "additional requirements" from the national Data Protection Authority (Art. 43(1)(b) GDPR).¹³</p>

¹² "Observation by the accreditation body of a conformity assessment body carrying out conformity assessment activities within its scope of accreditation" ISO/IEC 17011.

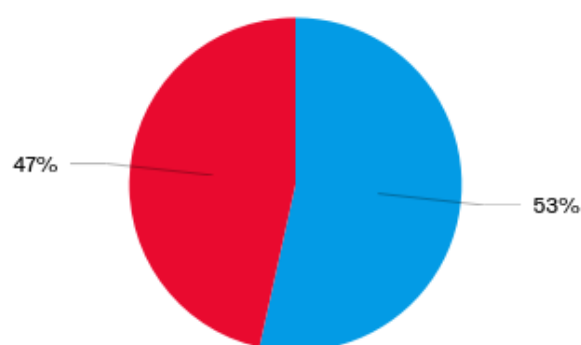
¹³ Art.43(1)(b) GDPR: "the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56."

	<p>In your experience, to what topics should those “additional requirements” provided by the national Data Protection Authority/Information Commissioner relate?</p> <ul style="list-style-type: none"> • Requirements related to the expertise of the certification body and its auditors in the field of data protection • Requirements related to procedural guarantees and assessment techniques related to the accreditation process (e.g. sanctions, how to deal with non-conformities, conflict of interest policy, etc.) • Both of the above • Other [Please elaborate (Q9b)]
Only for accreditation bodies that replied <u>yes</u> in Q2	<p><u>Q10.</u> Does the National Accreditation Body <u>in your country</u> have personnel with expertise in data protection?</p> <ul style="list-style-type: none"> • Yes • No, but we are planning to hire • No, we will collaborate with assessors on an ad hoc basis, every time there is a relevant application. • I don’t know • Other [Please elaborate]
	<p><u>Q11.</u> In your view, which are the necessary qualifications for assessors for the accreditation of certification bodies in the field of data protection?</p> <ul style="list-style-type: none"> • Primarily educational background and/or working experience in information security • Primarily educational background and/or in data protection legislation • Both • Other [Please elaborate]
	<p><u>Q12.</u> In case of single-issue certifications (i.e. certifications covering only one aspect in the GDPR – e.g. data security or data portability), do you think that the certification body and its auditors, should:</p> <ul style="list-style-type: none"> • Primarily demonstrate general knowledge on the data protection legislation • Primarily demonstrate specific knowledge on the topic of the single-issue certification e.g. data security • Demonstrate knowledge on both the above issues. • I don’t know • Other [Please elaborate]
	<p><u>Q13a.</u> Do you plan to recognise accreditation certificates granted by national Data Protection Authorities in other EU Member States?</p> <ul style="list-style-type: none"> • Yes • Yes, under conditions [Please elaborate (Q13b)] • No [Please elaborate (Q13b)] • I don’t know

	<p><u>Q14a.</u> How do you think the independence and integrity of a certification body and its auditors can be assessed and demonstrated in the field of data protection? [please rate from 1 to 5, where 1 very relevant]</p> <ul style="list-style-type: none"> • The certification body is already accredited by the National Accreditation Authority in other fields • Adherence of the certification body to Codes of Conduct • Reputation • Written legally binding commitments • The certification body is a member of a European or International Association • Other [Please elaborate (<u>Q14b</u>)]
	<p><u>Q15.</u> Do you plan to charge a fee for the accreditation process?</p> <ul style="list-style-type: none"> • Yes [Could you provide a range of applicable fees?] • No • Not applicable, the National Accreditation Body will not conduct accreditation process
	<p><u>Q16.</u> Would you like to add something on the topic? [open field]</p>

4.2 Accreditation survey results

4.2.1 Overview of respondents



■ Data Protection Authority / Information Commissioner ■ National Accreditation Body

Source: Online survey on accreditation. N=43.

Figure 4.1 Type of organisation

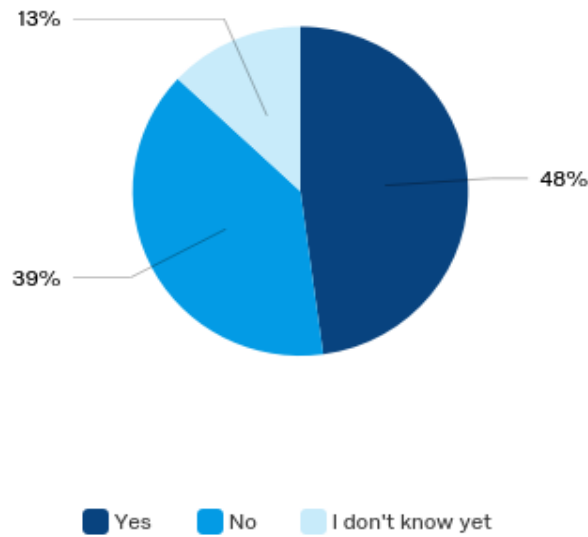
Country	Number of respondents	%
Belgium	1	2%
Bulgaria	2	5%
Czech Republic	2	5%
Denmark	1	2%
Estonia	1	2%
Finland	1	2%
France	1	2%
Germany	7	16%
Greece	2	5%
Hungary	2	5%
Ireland	1	2%
Italy	2	5%
Latvia	1	2%
Lithuania	1	2%
Luxembourg	2	5%
Netherlands	2	5%
Poland	1	2%
Portugal	2	5%
Romania	1	2%
Slovakia	2	5%
Slovenia	2	5%
Spain	1	2%
Sweden	2	5%
United Kingdom	2	5%
EU-level	1	2%
Total	43	100%

Source: Online survey on accreditation. N=43.

Table 4.3 Number and percentage of respondents in different countries

4.2.2 Results of the survey section addressed to data protection authorities and information commissioners

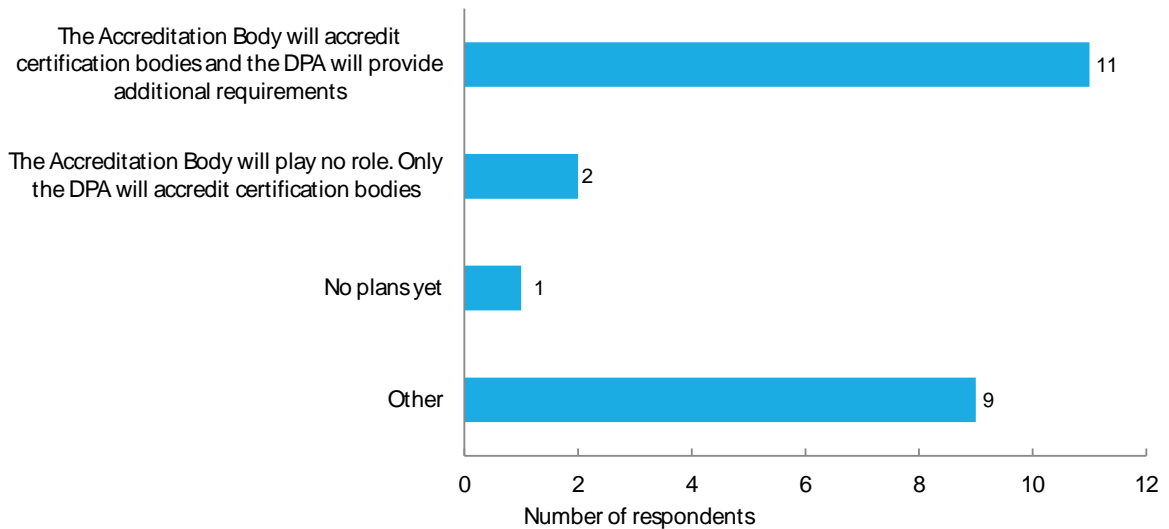
Question (Q2): Does the DPA plan to conduct accreditation of certification bodies in your country?



Source: Online survey on accreditation. N=23.

Figure 4.2 Percentage of DPAs planning to conduct accreditation of certification bodies

Question (Q3): What will the role of the National Accreditation Body be in relation to the GDPR certification in your country?



Source: Online survey on accreditation.
 Note: Bars denote total response count. N=23.

Figure 4.3 Role of the National Accreditation Body in relation to the GDPR certification

Question (Q4a): In case the DPA plans to conduct the accreditation without the National Accreditation Body, do you plan to follow the requirements of the EN ISO/IEC 17065 standard?

- One respondent indicated: “yes, even though it is not required in the GDPR”

- One respondent answered: “no”
- Other respondents did not provide a response to this question.

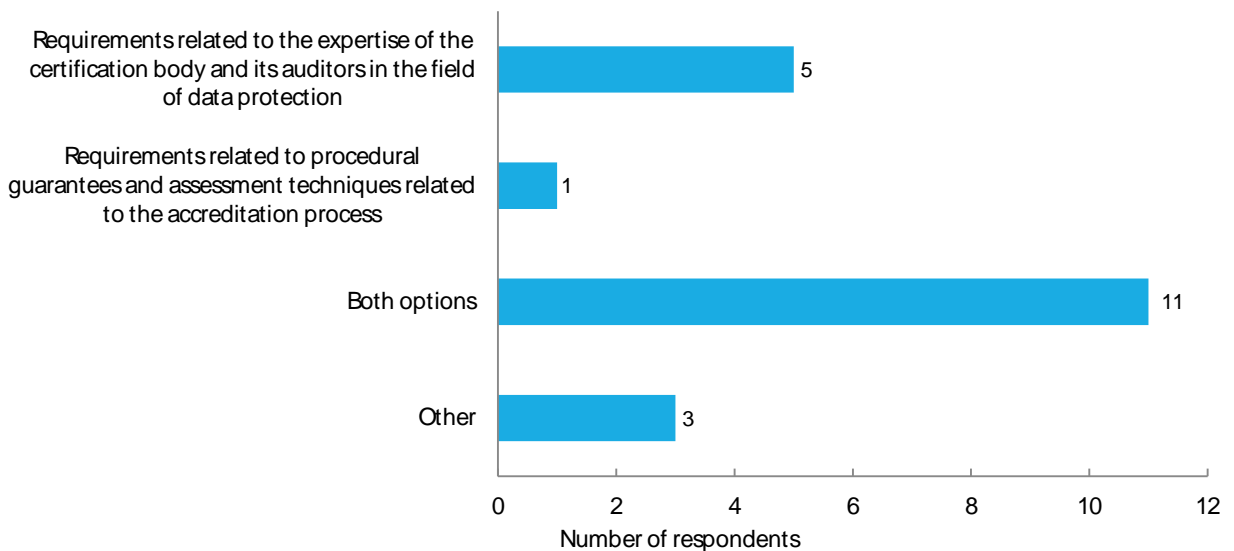
Question (Q4b): Do you have experience with accreditation of processes in line with the EN ISO/IEC 17065?

- Two respondents indicated “no” and did not provide further elaboration
- Other respondents did not provide a response to this question.

Question (Q5): In case the DPA plans to conduct the Accreditation without the National Accreditation Body, which of the following assessment techniques are likely to be applied for accreditation of certification bodies in the field of data protection in your country?

- One respondent provided the following assessment: “remote assessment”, “document review” and “file review” were rated as 1 (very likely), “witnessing”, “measurement audits”, “validation audits” and “interviewing” were rated as 2 (neutral), and “on-site assessment” and “unannounced visits” were rated as 3 (least likely).
- Other respondents did not provide any assessments.

Question (Q6): In case the DPA plans to be involved in Accreditation together with the National Accreditation Body, which do you think is the scope of “additional requirements” of Art. 43(1)(b)?



Source: Online survey on accreditation.

Note: Bars denote total response count. N=20.

Figure 4.4 Scope of ‘additional requirements’ of Art. 43(1)(b)

Question (Q7): Can you provide some examples of 'additional requirements' of Art. 43(1)(b) necessary for the accreditation of certification bodies in the data protection field?

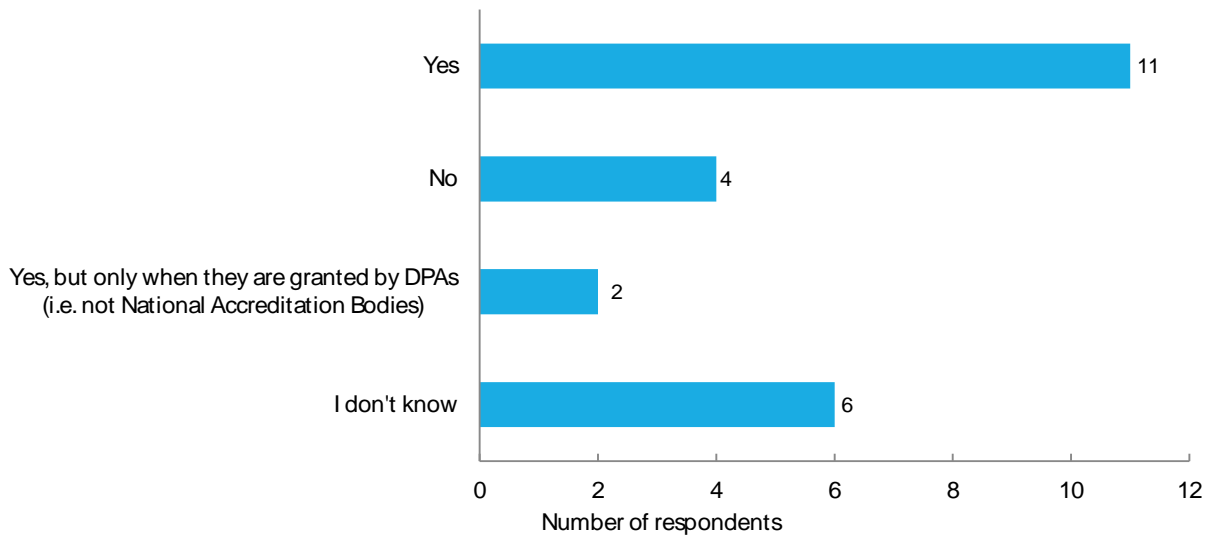
Comment
Work experience
Practice in the field of auditing or IS management at least 5 years and evidence of at least 10 fully completed audits (it concerns staff of certification bodies)
By assuming a data protection certification, seal or mark should finally be admitted in a study on a data protection case resp. data protection investigation there are many additional requirements. A certification body must control and audit the tested data protection and data security goals for each product, process or system that are certified. So, the DPA has the possibility to check during an investigation of [a] data protection case the guarantees which are given by a certification, seal or mark at any time. As a consequence an integrated data protection management and the corresponding system should be established for all parties who are [involved]. (This one-line text field doesn't enable the DPA to give further details.)
Qualification, publishing audit results etc. [Note: three separate respondents provided the same comment]
Knowledge of ePrivacy regulation, DPIA, anonymisation
Expertise in all data protection and information security aspects according to GDPR. For instance, specific assessment criteria of DPIAs, specific evaluation framework and tools relating to technical and organisational security measures, knowledge and expertise in business logic or processes related to several activity sectors, etc.
The additional requirements will complement ISO 17065 point by point. For example the expertise of the certification body will be checked by a desk review where certain qualification[s] and practice will be required
NAB and DPA will ensure adequate and relevant resourcing for accreditation of DP certification mechanisms; AB shall not advise the SA on the nature of the data protection requirements required for accreditation or on the effectiveness or otherwise of the criteria approved for certification pursuant to 42(5) AB shall inform DPA of all accreditation awards and withdrawals AB shall take account of decisions relevant to the accreditation of where it believes the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body that infringe the requirements of the GDPR; CBs should be able to demonstrate their agreement with organisation is independent, intervenable, is transparent about its certification; CB has expert staff; auditors have experience in DP; CB withdraws where conditions are no longer met
Competence required for the auditors (possibly certified)
Additional requirements should be established to ensure the independence of [the] accreditation body (sufficient resources and expertise of the accreditation body). For example, requirements in regard [to] experience of employees of the accreditation body could be considered
Experience in data protection, maybe legal experience
For example knowledge and expertise related to data protection and privacy
Still under discussion
a) Demonstrate in writing that he has at least 5 years of professional experience in the field of auditing of information systems; b) Demonstrate in writing that he has at least 5 years of professional experience in the field of personal data protection; c) Did not provide a consultation or other service to the controller or processor within a

Comment
period of 3 years prior to the date on which the audit was initiated by the auditor, which could constitute a risk of impartiality or a conflict of interest if he performed a personal data audit to the controller or processor
Unfortunately not yet
A.43(2) & data protection (DP) competence & suitability in the information rights context

Source: Online survey on accreditation. N=18.

Table 4 Examples of 'additional requirements' of Art. 43(1)(b)

Question (Q8): Do you think that the DPAs should recognise accreditation granted in other EU Member States?

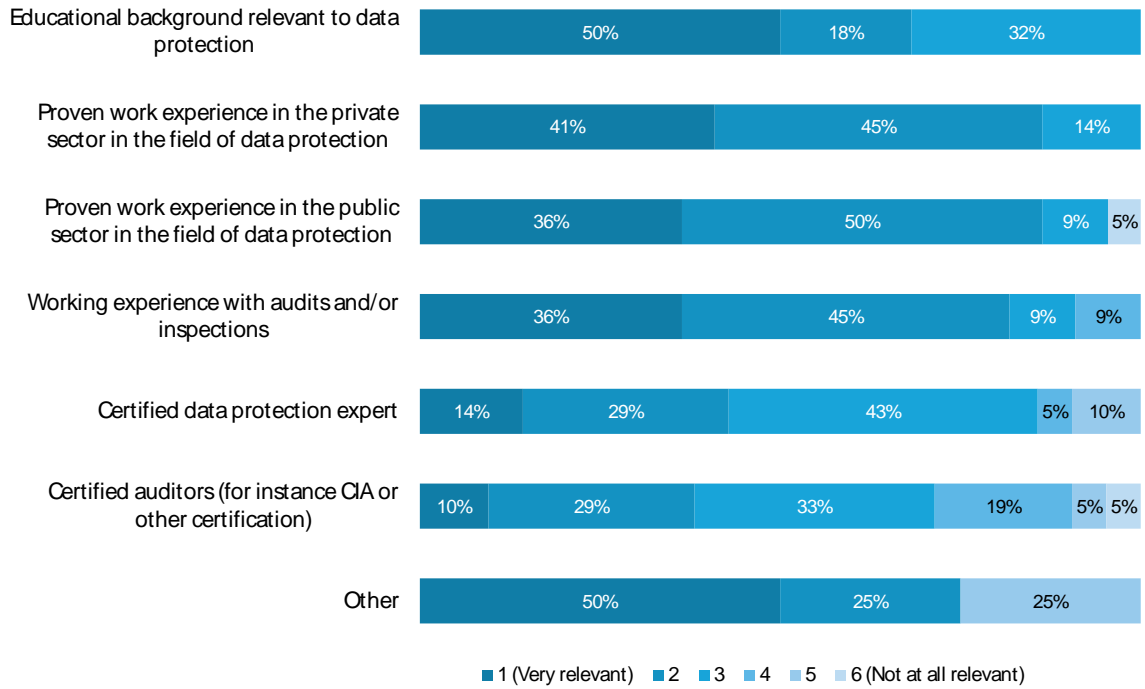


Source: Online survey on accreditation.

Note: Bars denote total response count. N=23.

Figure 4.5 Recognition of accreditation granted in other EU Member States

Question (Q9): In your view, which of these factors are relevant to assess the expertise of an auditor conducting a certification process? Please rate from 1 to 6 (where 1=very relevant, 6=not relevant at all)

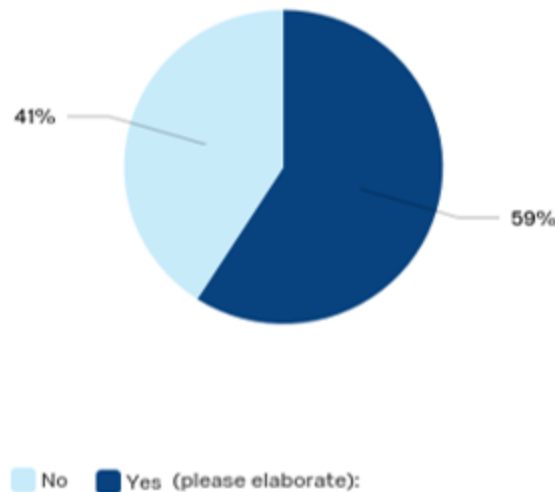


Source: Online survey on accreditation.

Note: From top to bottom, N=22, 22, 22, 22, 21, 21, 4.

Figure 4.6 Factors relevant to assess the expertise of an auditor conducting a certification process

Question (Q10a): Do you think that additional training should be provided to the auditors of the certification bodies?



Source: Online survey on accreditation. N=22.

Figure 4.7 Need for additional training to the auditors of the certification bodies

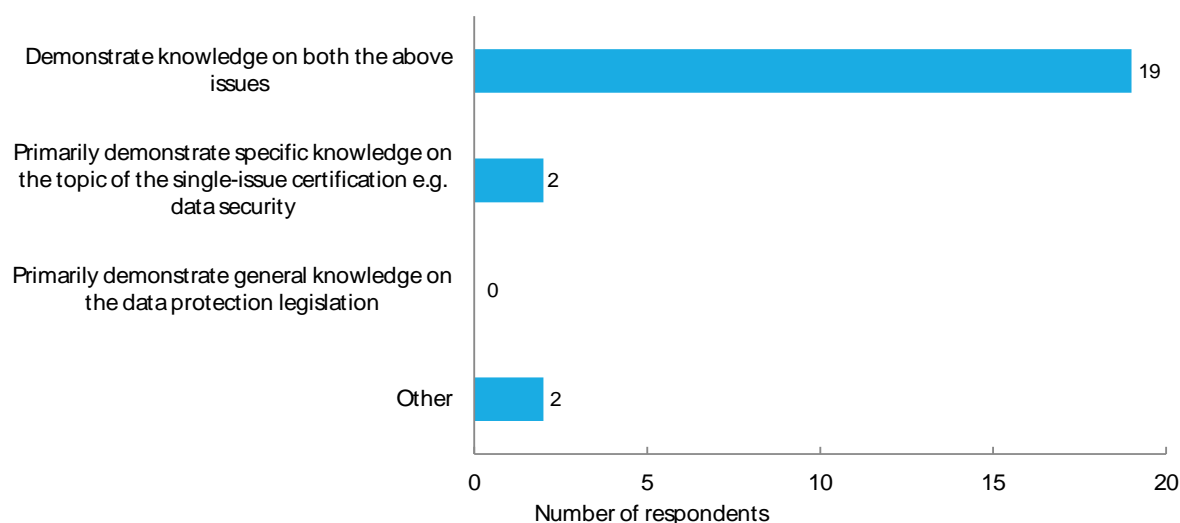
Question (Q10b): (If 'yes' to the previous question) What kind of training and by whom? The table below provides an overview of the most relevant answers.

Comment
Short-term, in personal data protection
Accreditation body and DPA
The training should include the legal, organisational and technical aspects related to the GDPR as well as the accreditation and certification processes [at] the National level. Such training can [be] realized by the accreditation body and/or the DPAs
Training in data protection practices (e.g. DPIA techniques, technical and organisational measures to ensure adequate data protection)
Relevant domain DP policy, compliance, and practice matters along with general and specific data protection training
Evaluation on case by case basis. Data protection requirements training may be provided by the DPA
On accreditation of certification bodies, certification process
Data protection in the field in which they perform their audits (ex: DP in health sector, DP for fintechs)
On data protection; by certified bodies (e.g. PECB Europe)
On GDPR by the DPA
DP specific training in the context of certification mechanisms and relevant for single issue certifications. Different training models are likely to evolve, e.g. learning from DPA good practice audits. Responsibility for training auditors lies with the certification body

Source: Online survey on accreditation. N=13.

Table 5 Suggestions concerning additional training to the auditors of the certification bodies

Question (Q11): In case of single-issue certifications (i.e. certifications covering only one aspect in the GDPR – e.g. data security or data portability), what do you think that the certification body and its auditors should do?



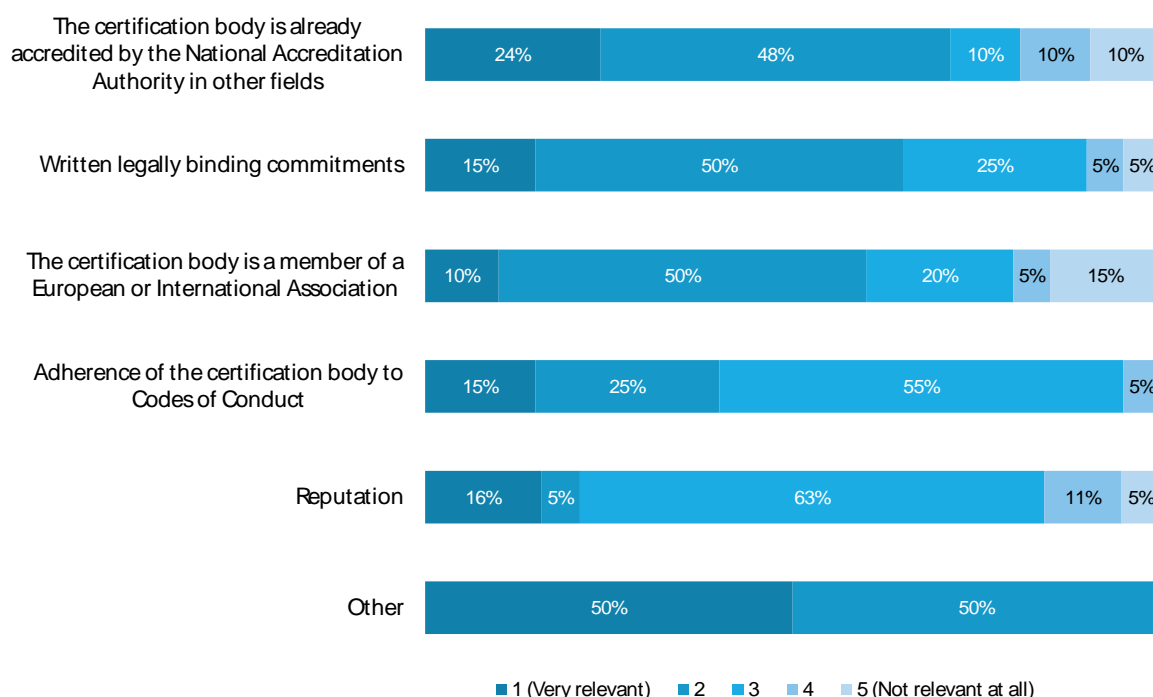
Source: Online survey on accreditation.

Note: Bars denote total response count. N=23.

Figure 4.8 Demonstration of knowledge in case of single-issue certifications

With respect to the above question, the two respondents who indicated “other” both commented that further details could not be provided.

Question (Q12a): *How do you think the independence and integrity of a certification body and its auditors can be assessed and demonstrated in the field of data protection? Please rate from 1 to 5 (where 1=very relevant, 5=not relevant at all)*



Source: Online survey on accreditation.

Note: Bars denote average scores. From top to bottom, N=21, 20, 20, 20, 19, 4.

Figure 4.9 Assessment of independence and integrity of a certification body and its auditors

The respondents who provided an assessment for “Other” were asked to elaborate. Their comments are presented in the table below.

Question (Q12b): *How do you think the independence and integrity of a certification body and its auditors can be assessed and demonstrated in the field of data protection? – “Other” The table below provides an overview of the most relevant answers.*

Comment
Economically independent
Accreditation is based on ISO 17065 which covers all aspects of demonstrating independence and integrity

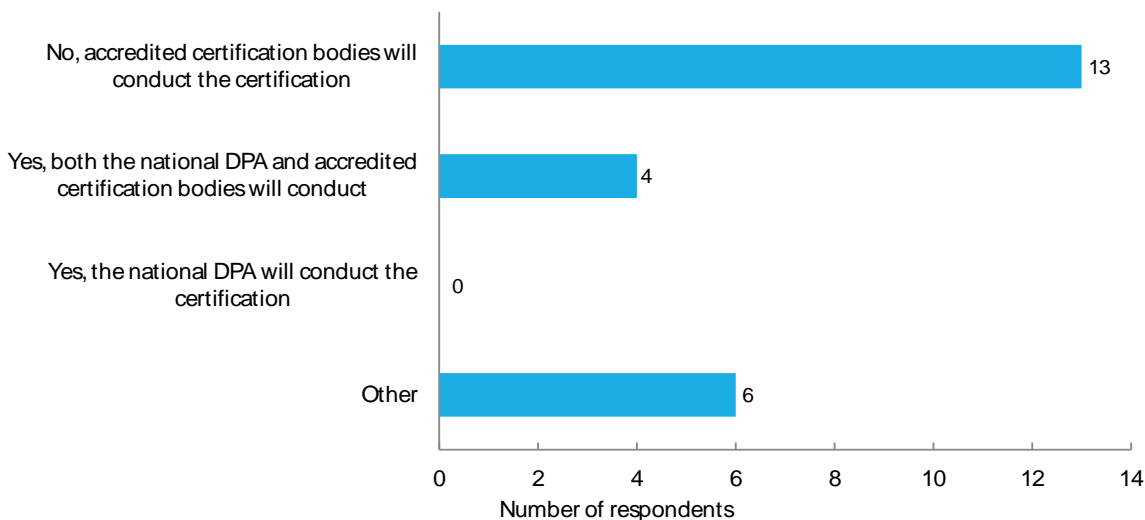
Comment
Still under discussion

Source: Online survey on accreditation.

Note: N=4.

Table 4.6 Assessment of independence and integrity of a certification body and its auditors – further comments

Question (Q13): Do you plan to conduct certification of organisations (controllers/processors)?

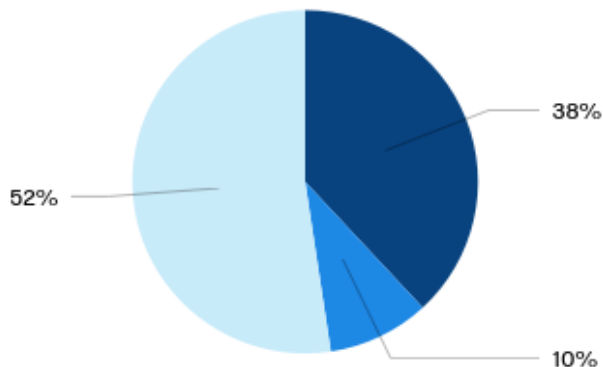


Source: Online survey on accreditation.

Note: Bars denote total response count. N=23.

Figure 4.10 Plans for conducting certification of organisations

Question (Q14): Do you plan to charge a fee for the accreditation process?



■ Yes
 ■ No
 ■ Not applicable, the DPA will not conduct the accreditation process

Source: Online survey on accreditation.

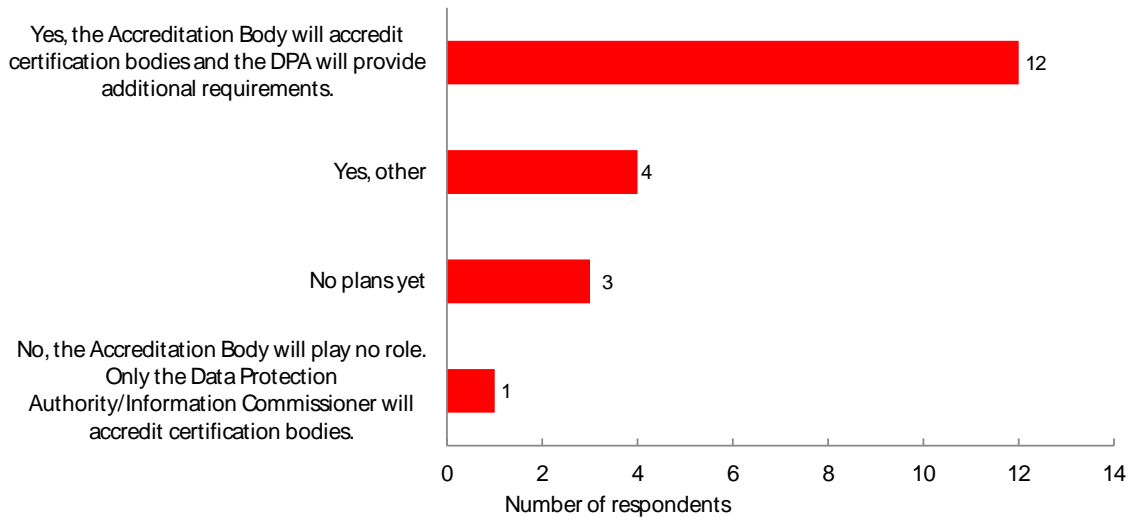
Note: N=21.

Figure 4.11 Plans to charge a fee for the accreditation process

When those who answered “yes” to the above question were asked to provide a range of applicable fees, one respondent indicated EUR 7 000.

4.2.3 Results of the survey section addressed to national accreditation bodies

Question (Q2): Does the National Accreditation Body plan to conduct accreditation of certification bodies based on the General Data Protection Regulation (Art. 43) in your country?



Source: Online survey on accreditation.

Note: Bars denote total response count. N=20.

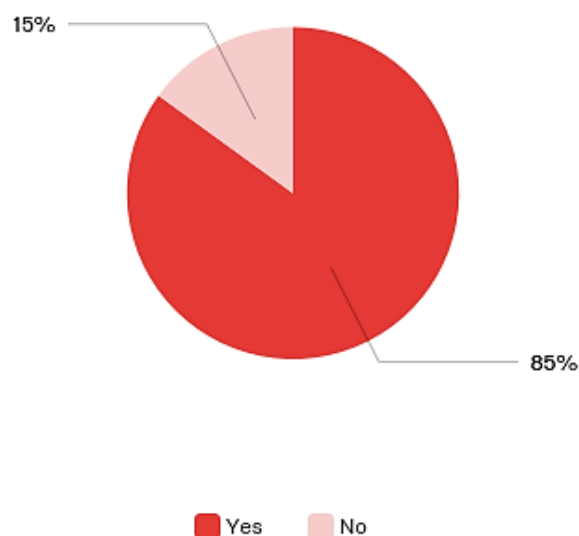
Figure 4.12 Plans to conduct accreditation of certification bodies

The respondents who ticked "Yes, other" were asked to elaborate.

Question (Q3): Against which conformity assessment standard does the National Accreditation Body accredit?

The majority of the respondents replied the ISO/IEC 17065 standard. Additional standards were: EN ISO/IEC 17025, 17020, 17021-1, 17024, 17043; EN ISO 14065, 17034, 17589.

Question (Q4): Do you have experience with accreditation of processes in line with the EN IS/IEC 17065?



Source: Online survey on accreditation.

Note: N=20.

Figure 4.13 Experience with accreditation of processes in line with the EN IS/IEC 17065

Question (Q5): *Could you please name the stages of the accreditation process you follow in case of accreditation of certification bodies (e.g. pre-assessment, initial assessment)? Provide links to documents, where available. The table below provides an overview of the most relevant answers.*

Country	Comment
Belgium	Pre-assessment, initial assessment, 1st surveillance assessment, 2nd surveillance assessment, re-assessment, 1st surveillance assessment, 2nd surveillance assessment, 3rd surveillance assessment, re-assessment. From here on the cycle with 3 surveillance assessments is repeated
Bulgaria	http://nab-bas.bg/en/documentslib
Czech Republic	Application review, initial assessment, on-site assessment + WA, decision making and surveillance visits
Finland	Document review, pre-assessment for new clients, initial assessment covering onsite assessment and witnessing, see assessment process from www.finas.fi
France	Process of accreditation includes application of the CB, review of application, onsite assessment, accreditation decision. After the accreditation is delivered, the CBs is monitored through regular (surveillance and renewal) onsite assessments. See http://www.cofrac.fr/documentation/CERT-REF-05
Germany	https://drive.google.com/file/d/1yHbevQ_n9TI8hpX-ynPcUgbNK6F1YEJK/view
Greece	Assessment procedure according to ESYD Procedures
Hungary	See our website: http://nah.gov.hu/process-of-accreditation
Italy	Steps required by ISO 17011. https://www.accredia.it/documento/rg-01-rev-04-regolamento-per-

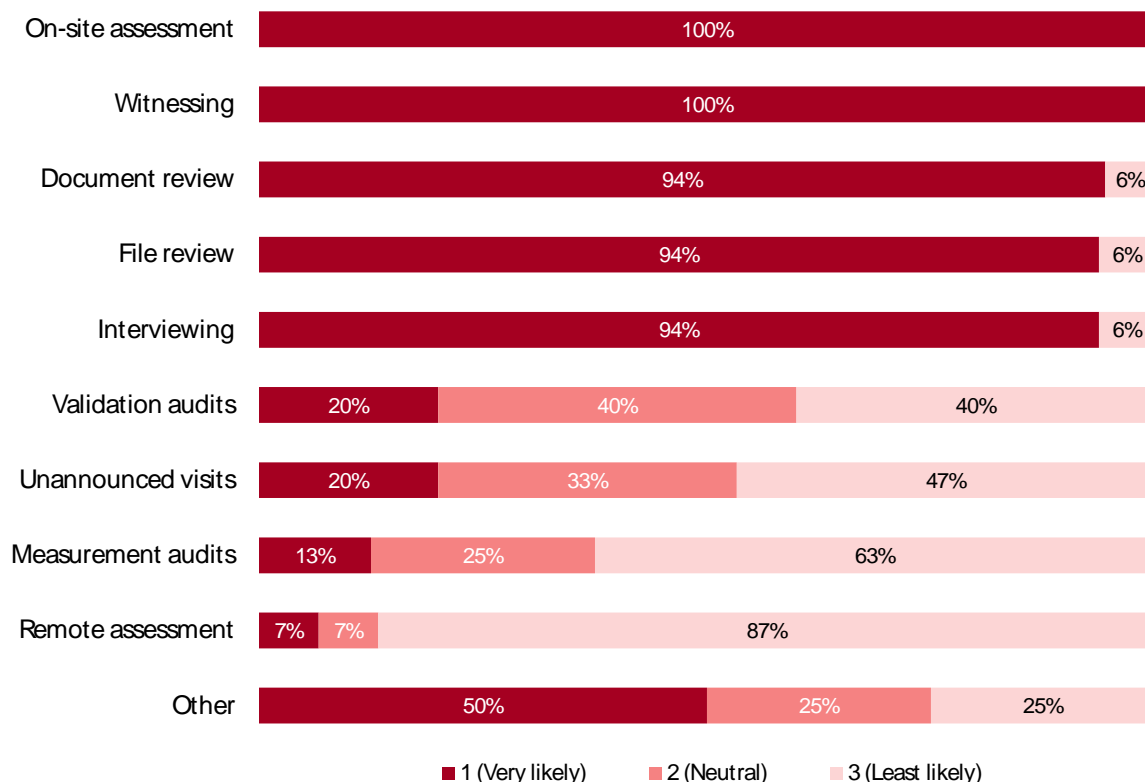
Country	Comment
	laccreditamento-degli-organismi-di-certificazione-ispezione-verifica-e-convalida-parte-generale/ and https://www.accredia.it/documento/rg-01-03-rev-01-regolamento-per-laccreditamento-degli-organismi-di-certificazione-del-prodotto-servizio/
Luxembourg	https://portail-qualite.public.lu/content/dam/qualite/fr/documentations/accreditation-notification/accreditation-olas/procedures/p002-realisation-audit-v27/p002-realisation-audit-en.pdf
Netherlands	Pre-assessment, initial assessment, witness, follow up on correct actions, surveillance, re-assessment, see document BR002 on the RvA website https://www.rva.nl/en/documents/rules-and-decisions
Poland	Pre-assessment, initial assessment, reassessment, Document DA-01: http://www.pca.gov.pl/download/data/rep-files/userfiles/_public/dokumenty_pca/dokumenty_ogolne/da-01_9.pdf
Portugal	1. Application; 2. Documental Review; 3. Initial Assessment 4. Closing of Findings 5. Decision http://www.ipac.pt/docs/publicdocs/regulamentos/DRC001_General_Regulation_v311217_En.pdf
Slovakia	All document[s] are available on http://www.snas.sk/index.php?l=sk&p=6&ps=14
Slovenia	http://www.slo-akreditacija.si/wp-content/uploads/2016/06/S03-izdaja-24-ANGL.pdf
Spain	See PAC-ENAC-EC in our website www.enac.es
Sweden	Document review, initial assessment, witness assessment https://www.swedac.se/services/accreditation/how-accreditation-works/?lang=en
United Kingdom	Application, application review, pre-assessment visit (optional but recommended)

Source: Online survey on accreditation.

Note: N=18.

Table 4.7 Stages of the accreditation process

Question (Q6): Which of the following assessment techniques are likely to be applied for accreditation of certification bodies in the field of data protection in your country? Please rate on a scale from 1 to 3 (where 1=very likely, 2=neutral, and 3=least likely)

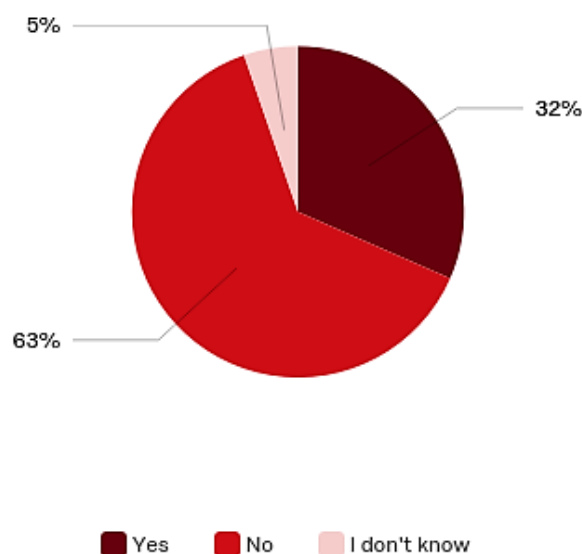


Source: Online survey on accreditation.

Note: Bars denote average scores. From top to bottom, N=18, 18, 18, 16, 16, 15, 15, 16, 15, 4.

Figure 4.14 Assessment techniques likely to be applied for accreditation of certification bodies in the field of data protection

Question (Q7): Does the national law on accreditation in your country include requirements, procedures, or safeguards for accreditation of certification bodies in addition to those of the Regulation 765/2008?

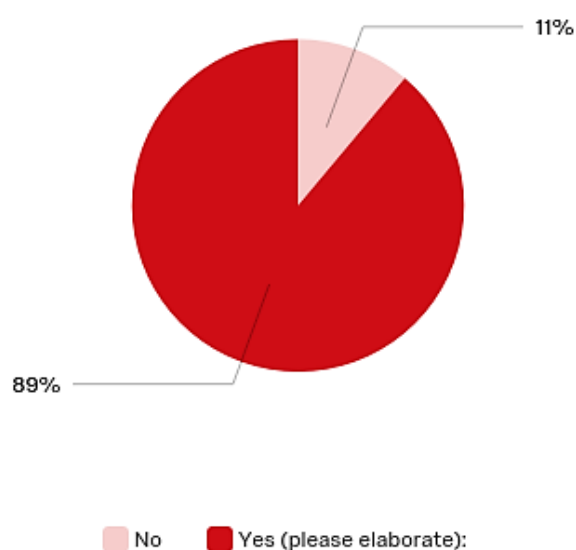


Source: Online survey on accreditation.

Note: N=19.

Figure 4.15 Additional requirements, procedures, or safeguards for accreditation of certification bodies

Question (Q8a): *Are you aware of any other areas in your country where the National Accreditation Body collaborates with a competent public authority in another field?*



Source: Online survey on accreditation.

Note: N=18.

Figure 4.16 Collaboration of National Accreditation Body with a competent public authority in another field

Question (Q8b): *(If 'yes' to the previous question) please elaborate.*

Country	Comment
Belgium	Cybersecurity
Bulgaria	Organic farming Regulation 834/2007; Verification bodies Regulation 600/2012; EMAS Regulation 1221/2009
Czech Republic	eIDAS
Finland	Nuclear safety, information security, GHG verification, notified bodies
France	There are many areas where the NAB cooperates with the competent authority. After are some, non-exhaustive examples: European directives and regulations for CE marking (construction products: EC 305/2011), Organic production (EC 834/2007), GHG (EC 600/2012)e-IDAS (EC 910/2014), Energy (2010/31/UE directive)
Germany	Deutschland vgl. § 4 AkkStelleG, z.B. im Sektor Medizinprodukte
Italy	Security, CE Directives, organic, civil infrastructure
Luxembourg	Electronic archiving of documents

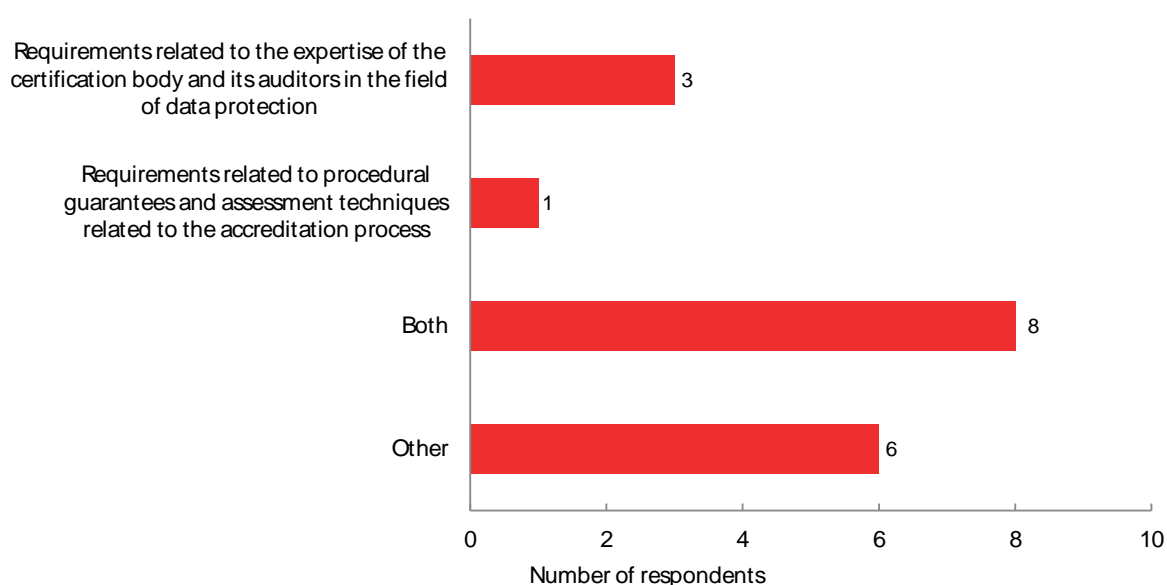
Country	Comment
Netherlands	It is quite common that the competent authority uses private schemes in which additional requirements for certification bodies are set. The ministry mentions the scheme in national regulation, therefore the scheme becomes mandatory including the additional requirements.
Poland	Organic regulation (EC) 834/2017, accreditation for notification purposes
Portugal	Agricultural and food sector; notification; environmental sector; industrial sector; etc.
Slovakia	Authorization for notification purpose in scope of new approach directives, law on air pollution, regulation on construction product, eIDAS
Slovenia	EMAS; certification of organic production and processing; GHG, notified bodies
Spain	Product safety (CE marking), legal metrology, national security scheme (cybersecurity), recurrent inspection of vehicles, protected designation of origin (food products), trust services (eidas Regulation), and more
Sweden	Many areas e.g. motor vehicles, building and houses, work environment, environmental, taxes
EU-level	Notification

Source: Online survey on accreditation.

Note: N=16.

Table 4.8 Collaboration of National Accreditation Body with a competent public authority in another field – further comments

Question (Q9a): *In your experience, to what topics should those "additional requirements" provided by the national Data Protection Authority/ Information Commissioner relate?*



Source: Online survey on accreditation.

Note: Bars denote total response count. N=18.

Figure 4.17 Topics the ‘additional requirements’ provided by the national Data Protection Authority/ Information Commissioner should relate to

The respondents who ticked “Other” were asked to elaborate. Their comments are presented in the table below.

Question (Q9b): *In your experience, to what topics should those “additional requirements” provided by the national Data Protection Authority/ Information Commissioner relate? – If “Other” please elaborate.* The table below provides an overview of the most relevant answers.

Comment
ISO 17067, certification scheme
Expertise of accreditation assessors, provisions for exchange of information with the DPA
Requirements related to the evaluation process to be followed by the CB (evaluation activities, depth of the evaluation, sampling, expected audit times, etc.)

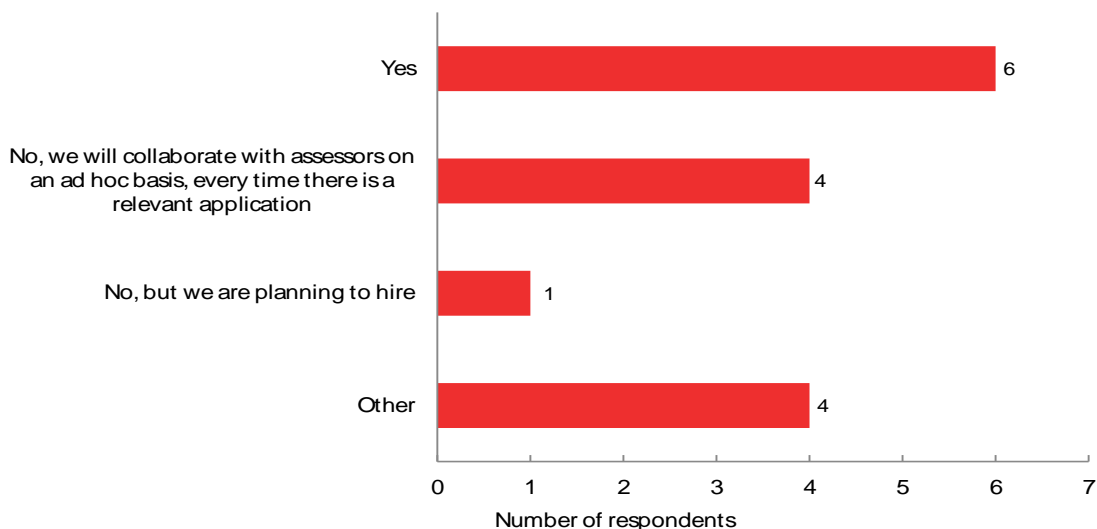
Source: Online survey on accreditation.

Note: N=4.

Table 4.9 Topics the ‘additional requirements’ provided by the national Data Protection Authority/ Information Commissioner should relate to – further comments

*Note that the following questions were asked only to accreditation bodies that answered, “yes” to Q2 “Does the National Accreditation Body plan to conduct accreditation of certification bodies based on the General Data Protection Regulation (Art. 43) in your country?”.

Question (Q10): *Does the National Accreditation Body in your country have personnel with expertise in data protection?*



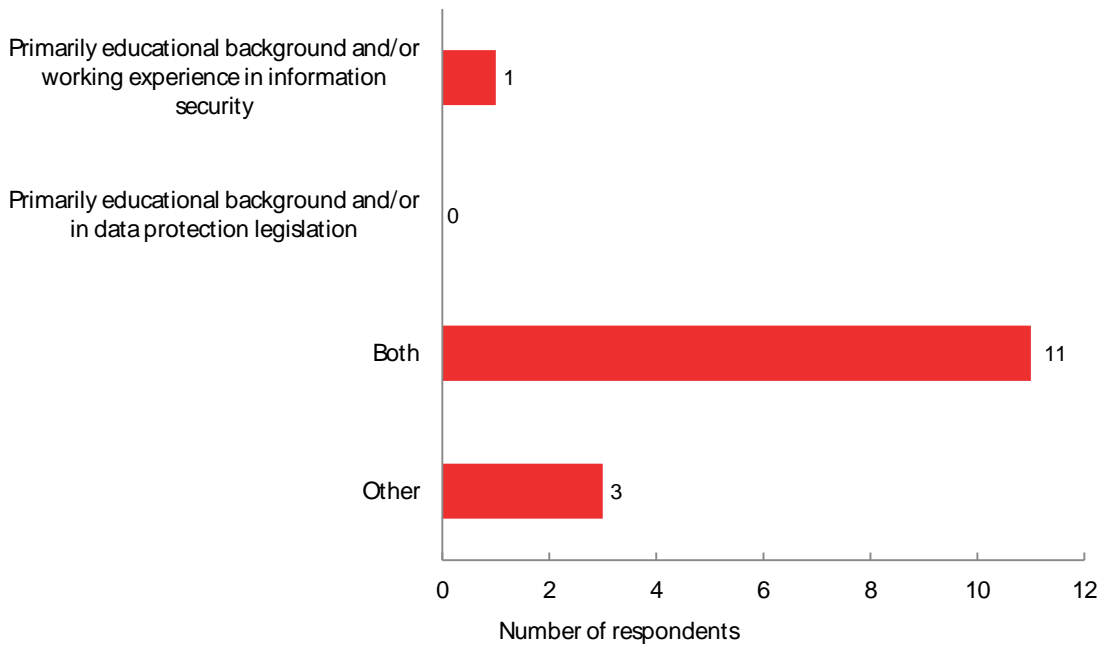
Source: Online survey on accreditation.

Note: Bars denote total response count. N=15.

Figure 4.18 Personnel with expertise in data protection

The respondents who ticked “Other” were asked to elaborate. A respondent replied that its organisation has a process for safeguarding competence in different areas, while others said they have expertise in ISO/IEC 27001 or that while they have some in-house experts, they mostly use external experts.

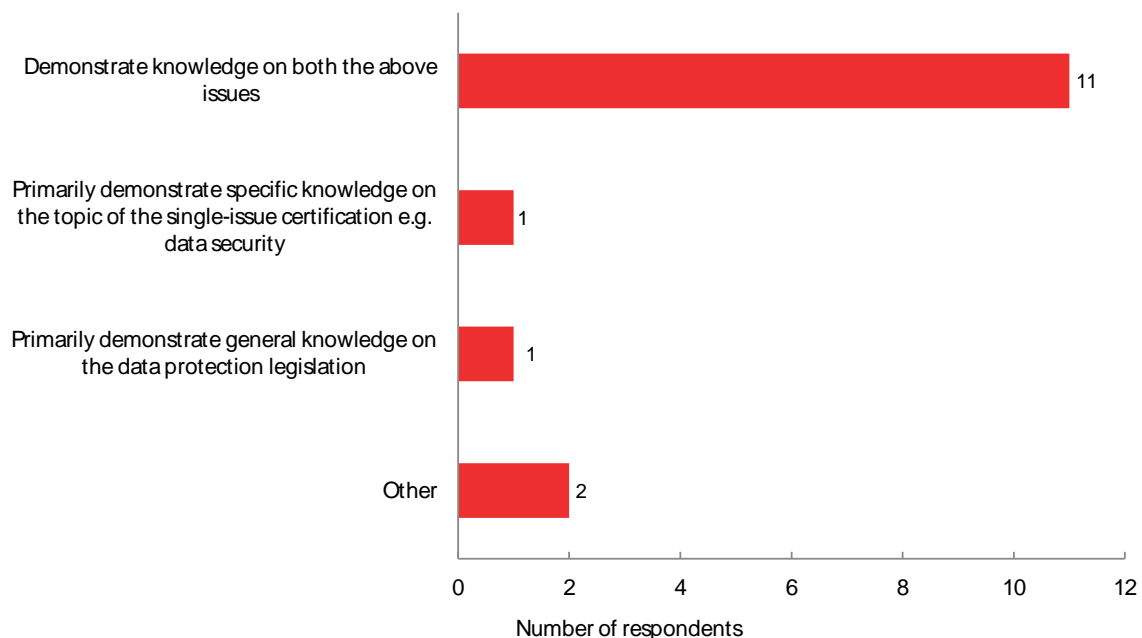
Question (Q11): In your view, which are the necessary qualifications for assessors for the accreditation of certification bodies in the field of data protection?



Source: Online survey on accreditation.
 Note: Bars denote total response count. N=15.

Figure 4.19 Necessary qualifications for assessors for the accreditation of certification bodies in the field of data protection

Question (Q12): *In case of single-issue certifications (i.e. certifications covering only one aspect in the GDPR – e.g. data security or data portability), what do you think that the certification body and its auditors should do?*

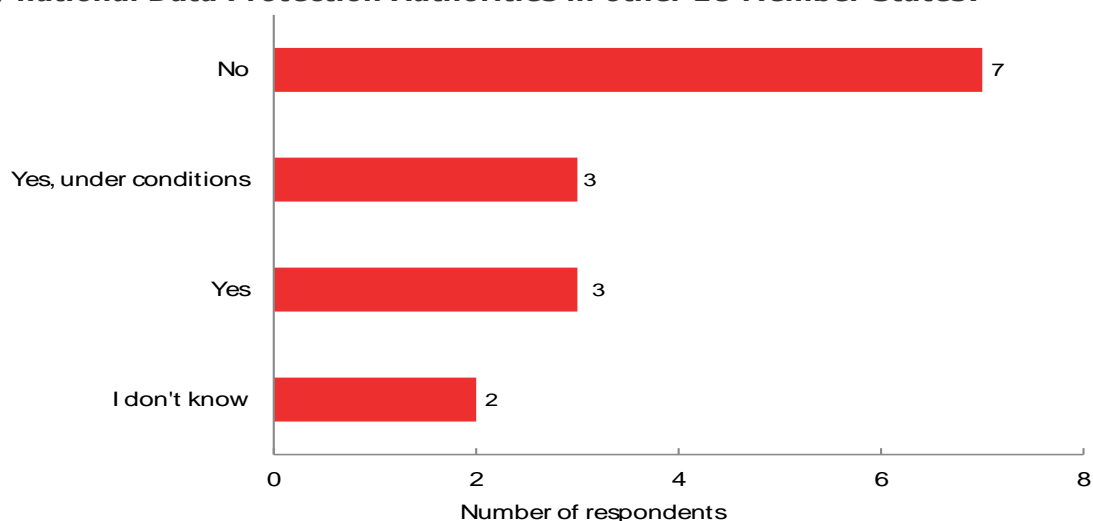


Source: Online survey on accreditation.

Note: Bars denote total response count. N=15. No comments were provided in the follow up question.

Figure 4.20 Demonstration of knowledge in case of single-issue certifications

Question (Q13a): *Do you plan to recognise accreditation certificates granted by national Data Protection Authorities in other EU Member States?*



Source: Online survey on accreditation.

Note: Bars denote total response count. N=15.

Figure 4.21 Plans to recognise accreditation certificates granted by national Data Protection Authorities

Respondents who ticked “Yes, under conditions” and respondents who ticked “No” were asked to elaborate. Their comments are presented in the table below.

Question (13b): (If ‘yes’ to the previous question) please elaborate. The table below provides an overview of the most relevant answers.

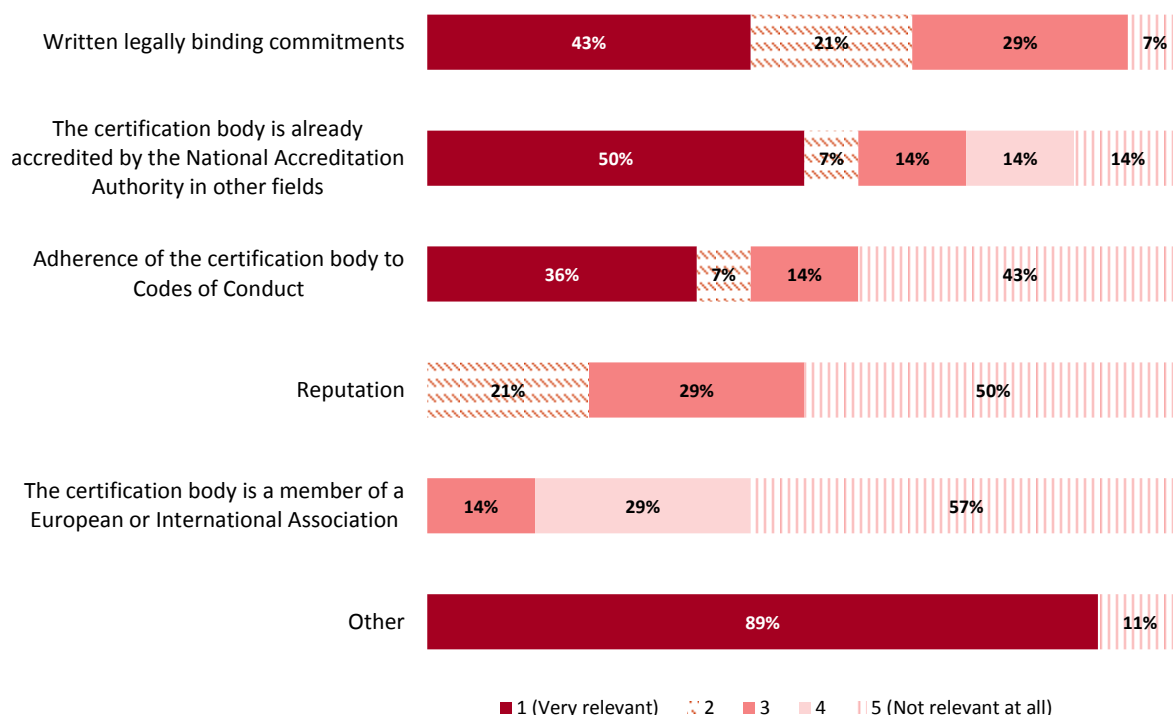
Response to question	Comment
Yes, under conditions	Yes, under conditions on which these certificates are granted in order to comply with the requirements
	Due to the fact that [the] [national] Accreditation Institute is a member of EA we are obliged to recognize all accredited certificates issued by EA members (with relevant MLA)
	Nur wenn die Akkreditierungsstelle gemäß VO (EG) Nr. 765 die Akkreditierung zusammen mit der Datenschutzaufsichtsbehörde erteilt. Die Akkreditierung darf nur über das EA-MRA und das IAF-MRA anerkannt werden.
No	NABs recognise only accreditations issued by MLA signatories
	There is no legal background to recognise accreditation by a non-accreditation-body
	NAB can recognize only certificates issued by other NABs according [to] EA MLA agreements. According Reg. 765 art. 11, it is up to the Authorities to accept certificates issued by other NABs or Authorities
	The national Data Protection Authorities in other EU MS shall not be subject to the peer evaluation referred to in Article 10 of Regulation 765/2008
	No, there is no mechanism to provide assurance on the equivalence of the accreditation processes of national DPAs and also [none] on the reliability of their operations - furthermore, the peer evaluation system in place only grants equivalence [to] certificates issued by national accreditation bodies
	According to Regulation 765 NABs must recognize the accreditation certificates granted by other NABs that have successfully passed the peer evaluation process established by EA
	We can only accept accreditations from other accreditation bodies

Source: Online survey on accreditation.

Note: N=10.

Table 4.10 Plans to recognise accreditation certificates granted by national Data Protection Authorities – further comments

Question (Q14a): How do you think the independence and integrity of a certification body and its auditors can be assessed and demonstrated in the field of data protection? Please rate from 1 to 5 (where 1=very relevant and 5=not relevant at all)



Source: Online survey on accreditation.

Note: Bars denote average scores. From top to bottom, N=14, 14, 14, 14, 14, 9.

Figure 4.22 Assessment of independence and integrity of a certification body and its auditors

Question (Q14b): *How do you think the independence and integrity of a certification body and its auditors can be assessed and demonstrated in the field of data protection? – If "Other" please elaborate.* The table below provides an overview of the most relevant answers.

Comment
Meeting the requirements of the accreditation criteria (ISO/IEC 17065)
through accreditation in the specific field
Follow ISO 17065
The risk assessment of the CAB, the mechanism to safeguard impartiality, rules and procedures of the CAB to be assessed.
A risk assessment on the existence of conflict of interests must be made and demonstrated
Demonstrated fulfilment of requirements in EN ISO 17065 regarding independence and impartiality

Source: Online survey on accreditation.

Note: N=9.

Table 4.11 Assessment of independence and integrity of a certification body and its auditors – further comments

When asked if they planned to charge a fee for the accreditation process, 15 respondents indicated "yes". The ranges of fees were provided either per hour, per day or per accreditation process and they presented significant differences. From 3000euro to 10.000 euro.

Annex 5A Stakeholder survey

5. Survey characteristics and respondents

5.1. Description of the survey

The aim of the survey was to get further insights into the reasons for organisations to adopt or not adopt European technical standards. A number of questions was also aimed at getting further insight into which standards are perceived as being relevant by the market as well as uptake factors for certifications. The underlying questionnaire was developed on the basis of relevant technical standards and uptake factors stemming from innovation literature and prior relevant studies. An overview of the questions used in the survey is set out in Section 2 of this Annex.

The survey was aimed at the following types of organisations:

- industry associations;
- certification bodies;
- standardisation bodies;
- industry (with a specific focus on SMEs).

5.2. Distribution of the survey

The questionnaire was distributed to 795 organisations that were spread across sectors in the following way:¹⁴

- Cloud Security Alliance (number: 206). Cloud Security Alliance is the world's leading organization dedicated to defining and raising awareness of best practises to help ensure a secure cloud computing environment. The stakeholder list under this section contains the executive and corporate members of the Cloud Security Alliance. The focus of the noted stakeholders falls in the field of information technology and services, cloud security, computer software, telecommunication, computer network security, banking, internet, cybersecurity as well as certification bodies.
- Certification bodies (105). This section contains the contacts of the certification bodies. This generally concern private companies that usually have been accredited by a national accreditation body for one or more certification schemes. Accreditation may also have taken place in more than one country.
- Standardisation Bodies (number: 44). This covers both the European standardisation bodies (CEN, CENELEC and ETSI) and national standardisation bodies from all the Member States (some Member States are having more than one).
- Agriculture (number: 32). The stakeholders under this section represent different professional associations on EU as well as Member State level in the field of agriculture and horticulture. It includes several European associations and councils

¹⁴ Additionally, the survey was distributed by the European Commission in its mailing list of stakeholders to an unknown number of recipients.

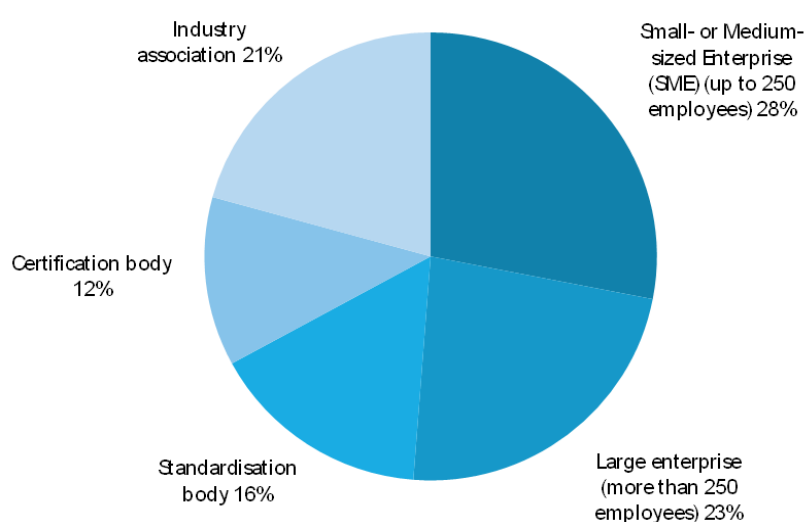
focusing of farmers and other professionals involved in agriculture. The section has also chosen representatives from the industry, such as milk suppliers, agricultural machinery and poultry producers. Representatives from research institutes targeting agricultural matters have been included as well.

- Manufacturing (number: 20). The stakeholders in this section represent different professional associations on EU as well as Member State level in the field of manufacturing including automobile manufacturing association and textile confederation as an example. Also, stakeholders from industries like pharmaceutical manufacturing, electronics, automotive and cosmetics are represented in this section.
- Energy (number: 51). This section covers several professional associations established on the European level relating to renewable energy, energy trade, smart meters, power plants, biodiesel, natural gas as well as European research institutes on the topic. The stakeholder list contains also associations on Member State level from countries such as France, Germany and Italy, focusing on topics such as electricity and consumer interests. From the side of private sector representation includes areas such as biomass fuels and smart grids companies.
- Construction (number: 16). The section regarding stakeholders in the field of construction represents many professional associations on European level such as builders' confederation, construction industry federation, contractors institute and many more. The list also includes representatives from the private sector, bringing out one of the most well-known construction companies in Europe from countries such as the Netherlands, Sweden and France.
- E-Commerce & Civic (number: 51). This section stakeholder selection provides a wide selection examples of associations and centres of consumer related focus points on EU level as well as Member State level. E-Commerce Associations from almost all of the Member States can be seen in this list. Trustmark holders from various countries dominate the section as well.
- Transportation (number: 29). The stakeholder list under this section represents different means of transportation such as aviation, railroad and ferry transport. It includes many airline companies across Europe but also package and freight delivery services. Representatives on the EU level include professional associations such as logistics, parking, rail freight, transport safety, road federation and abnormal road transport.
- Accommodation and Food Service Activities (number: 51). This section includes stakeholder from almost all of the Member States in the form of professional associations concerning hospitality industry, more specifically focusing on accommodation forms such as hotels, but also food and beverages, hotel management and hospitality employers.
- Information & Communication (number: 23). This section concerns the stakeholders from the field of information and communication includes several telecommunication companies operating in the European Union and offering their services in several countries at once. The list includes professional association representatives on European Union level focus in on telecommunication services and network operators. The association list includes also wireless infrastructure, e-identity and security.

- Financial & Insurance Activities (number: 52). This section presents stakeholders from professional associations on EU level as well as Member State level focusing on private equity, risk management, venture capitalism, financial supervision, investment, insurance intermediaries, mortgages, banking and insurance.
- Education (number: 30). This section concerns several universities across Europe as well as e-learning initiative and educational-comparison online platform. Regarding professional associations, it includes the associations targeting international education, higher education, teacher education, association of institutions and prison education association on EU level.
- Health (number: 51). This section concerns many professional associations on EU level targeting health management, public health, hospitals management etc. It contains associations from national states such as Estonia, the Netherlands and Finland. Besides the mentioned topics the stakeholders in that list also focus on insurance, alternative medicine, nurses, mental health, addictions, health IT, medical technology, logistics and transport, bio industry and research.
- Entertainment (number: 34). This section includes stakeholders from EU level such as professional associations focused on children's film, imagining and sound, festivals, amateur theatre etc., while professional associations on Member State level from countries such as Greece, Italy, Denmark, Poland and Rumania are included as well. The industry is represented by different television channels, radio stations, publishing houses, theatres and cinemas.

In total 82 respondents provided input for the survey.

5.3. The division over the types of organisations included in the survey



Source: Stakeholder survey

Note: N=82

Figure 5.23

5.4. The geographic division of the respondents

#	Answer	%	Count
1	Austria	5%	4
2	Belgium	10%	8
3	Bulgaria	2%	2
4	Croatia	1%	1
5	Cyprus	1%	1
6	Czech Republic	2%	2
7	Denmark	4%	3
8	Estonia	0%	0
9	Finland	1%	1
10	France	4%	3
11	Germany	12%	10
12	Greece	1%	1
13	Hungary	1%	1
14	Ireland	2%	2
15	Italy	2%	2
16	Latvia	0%	0
17	Lithuania	4%	3
18	Luxembourg	1%	1
19	Malta	2%	2
20	Netherlands	13%	11
21	Poland	0%	0
22	Portugal	1%	1
23	Romania	2%	2
24	Slovakia	2%	2
25	Slovenia	1%	1
26	Spain	4%	3
27	Sweden	4%	3
28	United Kingdom	5%	4
29	EU-level	10%	8
	<i>Total</i>	<i>100%</i>	<i>82</i>

Source: Stakeholder survey

Table 5.5

5.5. Stakeholder survey questionnaire

Information about the respondent

Name of the organisation:

Type of organisation:

Country:

Sector in which the organisation is active:

- Does the organisation has an in-house legal department? (Yes/No))
- Does the organisation has in-house information security expertise? (Yes/No)
- Does the organisation have a data protection officer? (Yes/No)
- Contact person filling the survey and email address:
- Do you consent to the processing of your personal data for the reasons outlined in the Introduction of the survey? [Please note you may withdraw your consent at any time before the publication of the Report in May 2018]]
- Yes, I agree
- Do you agree to publish your name along with your answers in the Report?
- Yes, publish my name
- No, publish only my answers
- Do you agree to publish the name of your organisation along with your answers?
- Yes, publish the name of my organisation
- No, publish only my answers

Please note that reference in the questionnaire to “privacy/data protection related standards” includes reference to IT-security standards, standards for assessment models and procedures, codes of practices, standards for privacy architecture frameworks etc. Reference in the questionnaire to “privacy/data protection certifications” includes reference to privacy seals and privacy marks.

Questions for standardisation bodies

(Q1) Has your organisation developed privacy/data protection related standards?

Yes. Please add name/reference numbers of the standard documents

No

What is the nature of these standards:

fundamental (terminology) standards
 management standards
 assessment standards
 informative standards (e.g. code of conduct)
 performance standard
 other:

X. Don't know

Are these standards sector specific?

No, generic standards

Yes, sector specific standards.

If so, for which sectors: [...]

(Q2) What are the reasons for updating standards in the field of privacy/data protection?:

Rate 1 (not important at all) to 5 (very important)

- Compliance with our internal regulations applicable to all our standard setting processes
- The growing societal importance of data protection

- Introduction of the EU General Data Protection per 25 May 2018
- Technological developments
- Other: ...

(Q3) What are in your view the most important factors determining the level of uptake of privacy/data protection-related standards in the market?

Rate 1 (not important at all) to 5 (very important)

- Costs of acquiring the standards
- Implementation costs
- Availability of material for training/education
- The level of endorsement of the standards by Data Protection Authorities
- The level of endorsement of standards by the European Union
- The level of endorsement of the standards by (other) government bodies
- The level of endorsement of standards by industry associations
- Positive experiences with implementing technical standards in general
- The extent to which the standards are unambiguous and clear
- The extent to which implementing the standards provides a clear business advantage
- The extent to which implementing the standards provides additional cyber security
- Other:
- X Don't know

(Q4) Is your organisation also involved in privacy/data protection related certifications?

- Yes
- No

(Q5) Are you aware of (other) certifications based on privacy/data protection related standards?
No

Yes, including:

Questions for certification bodies

(Q1) Does your organisation issue privacy/data protection certifications?

- Yes
- No

(Q2) (If yes) What is the nature/scope of these certifications?

- The scheme is certifying all types of business processes
- The scheme is certifying only specific business processes
- The scheme is aimed at a specific sector/business
- The scheme applies across all sectors/business
- The scheme applies only in a specific country
- The scheme applies in several countries
- The scheme applies in all Member States
- The scheme applies worldwide or, at least, in several non-EU countries
- The schemes is dedicated to SMEs
- The scheme helps to comply with specific GDPR provisions
- The scheme helps to comply with all GDPR provisions
- Other:

(Q3a) (If yes) Is your certification mechanism based on certain technical standards?

- No
- Yes, it concerns the following standards (Q3b):
- ISO/IEC 27001 - Information technology -- Security techniques -- Information security management systems – Requirements
- ISO/IEC 27002 - Information technology -- Security techniques -- Code of practice for

information security controls

- ISO/IEC 27003 - Information technology -- Security techniques -- Information security management systems – Guidance
 - ISO/IEC 27017:2015 Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services
 - ISO/IEC 27018:2014 - Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
 - ISO/IEC 29134:2017(en) - Information technology - Security techniques - Guidelines for privacy impact assessment
 - ISO/IEC 29101:2013 Information technology - Security techniques - Privacy architecture framework
 - ISO/IEC 29151:2017 - Information technology - Security techniques - Code of practice for personally identifiable information protection
 - ISO/IEC 29190:2015 - Information technology - Security techniques - Privacy capability assessment model
 - ISO/IEC 29191:2012 - Information technology - Security techniques - Requirements for partially anonymous, partially unlinkable authentication.
 - ISO/IEC 19941:2017 Information technology - Cloud computing - Interoperability and portability
 - BS 10012 - Personal Information Management System
- Other:

(Q4) (If not) For which reason(s):

Rate 1 (not important at all) to 5 (very important)

Market demand is too low

Business risks are too high since we might have to compete with Data Protection Authorities issuing certifications themselves

Potential customers do not see added value of certifications

Required investments exceed our financial capability

Lack of expertise in our organisation

Lack of established certification schemes which we could use as the basis for our certification process

Too complex

Other:

X Don't know

(Q5) (If not) Is your organisation considering developing a privacy/data protection certification in the near future?

Yes

No

(Q6) (If yes) What will be the nature/scope of the certification?

- The scheme will certify all types of business processes
- The scheme will certify only specific business processes
- The scheme will be aimed at a specific sector/business
- The scheme will apply across all sectors/business
- The scheme will apply only in a specific country
- The scheme will apply in several countries
- The scheme will apply in all Member States
- The scheme will apply worldwide or, at least, in several non-EU countries
- The schemes will be dedicated to SMEs
- The scheme will help to comply with specific GDPR provisions
- The scheme will help to comply with all GDPR provisions
- Other:
- X Don't know

(Q7) (If yes) Will the certification mechanism be based on certain technical standards?

- No
- Yes, it concerns the following standards:
- ISO/IEC 27001 –Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27002 –Information technology – Security techniques – Code of practice for information security controls
- ISO/IEC 27003 – Information technology – Security techniques – Information security management systems – Guidance
- ISO/IEC 27017:2015 – Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2014 –Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 29134:2017(en) – Information technology – Security techniques – Guidelines for privacy impact assessment
- ISO/IEC 29101:2013 – Information technology – Security techniques – Privacy architecture framework
- ISO/IEC 29151:2017 – Information technology – Security techniques – Code of practice for personally identifiable information protection
- ISO/IEC 29190:2015 – Information technology – Security techniques – Privacy capability assessment model
- ISO/IEC 29191:2012 – Information technology – Security techniques – Requirements for partially anonymous, partially unlinkable authentication.
- ISO/IEC 19941:2017 Information technology – Cloud computing – Interoperability and portability
- BS 10012 – Personal Information Management System
- Other:

(Q8) What are in your view the most important factors determining the level of uptake of privacy/data protection certifications in the market?

Rate 1 (not important at all) to 5 (very important)

- Costs of certifications
- The extent to which customers see the certification as being effective
- Level of enforcement of data protection legislation by the authorities
- The level of endorsement of certifications by industry associations
- The level of endorsement of certifications by the European Union
- The level of endorsement of such certifications by Data Protection Authorities
- The level of endorsement of such certifications by (other) government bodies
- The level of pressure from customers or business partners
- The extent to which competitors take out such certification
- The legal (protective) effect of certifications under the GDPR
- The recognition of certifications in other EU member states
- Other:
- X Don't know

(Q9) Is your organisation accredited in in line with ISO/IEC 17065?

- Yes
- No
- X Don't know

(Q10) Which scheme model would in your view be more efficient in the field of privacy/data protection?

- An all-encompassing scheme
- A single issue scheme
- Other:.,.....
- X Don't know

(Q11) What would be your proposal to incentive SMEs to adopt privacy/data protection certifications?

- Adapted price
- Adapted Process
- Both
- Other:
- X Don't know

Questions for industry

(Q1) Which of the following privacy/data protection related technical standards are being used in your organisation?

- ISO/IEC 27001 -Information technology -- Security techniques -- Information security management systems – Requirements
- ISO/IEC 27002 - Information technology -- Security techniques -- Code of practice for information security controls
- ISO/IEC 27003 - Information technology -- Security techniques -- Information security management systems – Guidance
- ISO/IEC 27017:2015 - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2014 -Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 29134:2017(en) - Information technology - Security techniques - Guidelines for privacy impact assessment
- ISO/IEC 29101:2013 - Information technology - Security techniques - Privacy architecture framework
- ISO/IEC 29151:2017 - Information technology - Security techniques - Code of practice for personally identifiable information protection
- ISO/IEC 29190:2015 - Information technology - Security techniques - Privacy capability assessment model
- ISO/IEC 29191:2012 - Information technology - Security techniques - Requirements for partially anonymous, partially unlinkable authentication.
- ISO/IEC 19941:2017 -Information technology - Cloud computing - Interoperability and portability
- BS 10012 - Personal Information Management System

Other:

X. Don't know

(Q2) Does your organisation have sufficient information about the availability of privacy/data protection related technical standards?

- No
- Yes
- Don't know

(Q3) Which source(s) does your organisation rely on most for obtaining information about privacy/data protection related technical standards?

Rate 1 (not important at all) to 5 (very important)

- Our own IT-department
- Our own data protection officer
- The European Union
- National governments
- Business literature
- Our industry association

- The Data Protection Authority
- Certification bodies
- Consultants
- Lawyers
- Other:
- X Don't know

(Q4) What are the most relevant factors when deciding whether to implement privacy/data protection related technical standards?

Rate 1 (not important at all) to 5 (very important)

- Costs of acquiring standards
- Costs of implementing standards
- Previous experiences with implementing other standards
- The extent to which the standards are unambiguous and clear
- The extent to which implementing the standards provides a clear business advantage
- The extent to which implementing the standards provides additional cyber security
- The extent to which implementing standards contributes to legal compliance
- The level of endorsement of the standards by Data Protection Authorities
- The level of endorsement of standards by the European Union
- The level of endorsement of the standards by (other) government bodies
- The level of endorsement of standards by industry associations
- The extent to which compliance raises trust of clients in our organisation
- Other:
- X Don't know

(Q5) In order to achieve compliance with privacy/data protection companies in our sector have to invest:

Rate 1 (minimal) through 5 (prohibitive)

- Time:
- Money/costs:
- Level of expertise:
- Other:
- X Don't know.

(Q6) On which level in your organisation is usually being decided about implementing a privacy/data protection-related standard?

- Top management
- Middle management
- Operational level
- Combination of the above
- Other:
- X. Don't know

(Q7) When considering to implement a technical standard in the field of privacy/data protection would your organisation prefer:

- National standards
- European standards:
- International standards
- X. Don't know

(Q8) What do you consider a successful standard?

- A standard that provides us with a clear business or security benefit
- A standard that exists in the market for many years
- An open standard
- A standard that is adopted by many companies
- A standard that is well-written and clear

- A standard that is both at home and abroad widely recognised
- A standard endorsed/acknowledged by the regulator
- A standard that my clients ask me to follow
- A standard that is purposeful (no unnecessary requirements)
- Other
- X. Don't know

(Q9) Has your organisation obtained any privacy/data protection related certification?

- Yes, and since when:
- No [why not]

(Q10) (If not). Does your organisation consider obtaining any privacy/data protection related certification in the near future:

- No
- Yes
- Maybe

(Q11) What are/is for your organisation the most important source(s) for obtaining information about the existence of privacy/data protection related certifications?

- Our own data protection officer
- Our own IT-department
- The European Union
- National governments
- Data Protection Authorities
- Consultancy firms
- Business magazines
- Internet websites
- Consultants
- Other:
- X. Don't know

(Q12) What are the most important factors influencing your decision whether or not to obtain any privacy/data protection related certifications?

- Costs of privacy/data protection certifications
- The extent to which the certification is effective
- The level of endorsement of certifications by industry associations
- The level of endorsement of certifications by the European Union
- The level of endorsement of such certifications by Data Protection Authorities
- The level of endorsement of such certifications by (other) government bodies
- The extent to which certification contributes to our image
- The extent to which customers or business partners value the certification
- The extent to which competitors take out such certification
- The legal (protective) effect of certifications under the GDPR
- The extent of recognition of certifications in other EU member states
- Previous experiences with certifications
- Other:
- X. Don't know

Questions for industry associations

(Q1) Which privacy/data protection related technical standards would you recommend to your members?

- ISO/IEC 27001 - Information technology -- Security techniques -- Information security management systems – Requirements
- ISO/IEC 27002 - Information technology -- Security techniques -- Code of practice for information security controls
- ISO/IEC 27003 - Information technology -- Security techniques -- Information security management systems -- Guidance
- ISO/IEC 27017:2015 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2014 -Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 29134:2017(en) -Information technology — Security techniques — Guidelines for privacy impact assessment
- ISO/IEC 29101:2013 - Information technology -- Security techniques -- Privacy architecture framework
- ISO/IEC 29151:2017 - Information technology -- Security techniques -- Code of practice for personally identifiable information protection
- ISO/IEC 29190:2015 - Information technology -- Security techniques -- Privacy capability assessment model
- ISO/IEC 29191:2012 - Information technology -- Security techniques -- Requirements for partially anonymous, partially unlinkable authentication.
- BS 10012 - Personal Information Management System
- Other:
- None
- X Don't know.

(Q2) What is your estimation about the current level of uptake of the following standards amongst your members:

- ISO/IEC 27001- Information technology -- Security techniques -- Information security management systems – Requirements
- ISO/IEC 27002- Information technology -- Security techniques -- Code of practice for information security controls
- ISO/IEC 27003 - Information technology -- Security techniques -- Information security management systems -- Guidance
- ISO/IEC 27017:2015 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2014 -Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 29134:2017(en) - Information technology — Security techniques — Guidelines for privacy impact assessment
- ISO/IEC 29101:2013 - Information technology -- Security techniques -- Privacy architecture framework
- ISO/IEC 29151:2017 - Information technology -- Security techniques -- Code of practice for personally identifiable information protection
- ISO/IEC 29190:2015 - Information technology -- Security techniques -- Privacy capability assessment model
- ISO/IEC 29191:2012 - Information technology -- Security techniques -- Requirements for partially anonymous, partially unlinkable authentication.
- BS 10012 - Personal Information Management System
- Other:
- None
- X Don't know.

(Q3) What are the most relevant factors for your organisation when deciding about promoting the implementation of privacy/data protection related technical standards by your members?

Rate 1 (not relevant at all) to 5 (very relevant)

- Costs for your members to acquire the standards
- Costs for your members to implement the standards
- The extent to which the standards are unambiguous and clear
- The extent to which implementing the standards provide a clear commercial benefit for the businesses of your members
- The extent to which implementing the standards provides additional cyber security for your members
- The level of relevant expertise in your organisation
- The level of support you can offer to support members in implementing the standards
- The extent to which implementing standards contributes to legal compliance for your members
- The level of endorsement of the standards by industry associations
- The level of endorsement of the standards by the European Union
- The level of endorsement of the standards by Data Protection Authorities
- The level of endorsement of the standards by (other) government bodies
- The extent to which compliance raises trust in your sector
- Other:
- X Don't know.

(Q4) In your view, which challenges do you think your members encounter most when it comes to implementing privacy/data protection related technical standards:

Rate 1 (not relevant at all) to 5 (very relevant)

- Negative experiences with following standards in general
- Lack of information about the existence of relevant standards
- Lack of information/knowledge about the possible benefits of complying with these standards
- Lack of information/knowledge about the costs and efforts of implementing these standards
- Lack of information/knowledge about the way in which these standards fit in their business processes
- Lack of knowledge/skills for implementing the standards
- Costs of acquiring the standards
- Costs of implementing these standards
- The standards are unclear
- The standards are only partially relevant for their business
- It is not sufficiently clear to them what would be the added value of achieving compliance with the standard
- Uncertainty about what their customers want
- Uncertainty about what their competitors will do
- Other:
- X Don't know.

(Q5) In order to achieve compliance with privacy/data protection companies in our sector have to invest:

Rate 1 (minimal) through 5 (prohibitive)

- Time:
- Money/costs:
- Level of expertise:
- Other:
- X Don't know.

(Q6) When considering endorsement of a technical standard in the field of privacy/data protection would you prefer:

Rate 1 (not preferred at all) to 5 (strongly preferred)

- National standards
- European standards:
- International standards
- X Don't know.

(Q7) Which instrument(s)/mechanism(s) would be most effective for your organisation in making the decision to promote compliance with privacy/data protection related technical standards amongst your members.

Rate 1 (not effective at all) to 5 (very effective)

- Availability of a financial incentive for your members to acquire these standards
- Availability of a financial incentive for your members to implement these standards
- Availability of training sessions for staff
- More information about availability of relevant standards
- More certainty about the legal effect of complying with such standards
- More information about what the market requires
- Other:
- X Don't know.

(Q8) Which source(s) would your organisation rely on most as regards obtaining information that could improve your awareness about the availability and effects of technical standards in the field of privacy/data protection:

Rate 1 (will not be relied on at all) to 5 (very relevant)

- Our own IT-department
- Our own data protection officer
- The European Union
- National governments
- Data protection authorities
- Consultancy firms
- Business magazines
- Internet websites
- Consultants
- Other:
- X Don't know.

(Q9) Which source(s) would your organisation rely on most as regards obtaining information that could improve your awareness about the existence of privacy/data protection related certifications?

Rate 1 (not relevant at all) to 5 (very relevant)

- Our own IT-department
- Our own data protection officer
- The European Union
- National governments
- Data protection authorities
- Consultancy firms
- Business magazines
- Internet websites
- Consultants
- Other:
- X Don't know.

(Q10) What are the most relevant factors for your organisation when deciding about promoting privacy/data protection related technical certifications?

Rate 1 (not relevant at all) to 5 (very relevant)

- Costs for our members to obtain such certification
- The extent to which it concerns an open standard

- The extent to which such a certificate has a clear business advantage for our members
- The extent to which such certification raises trust in our sector
- The extent to which such certification provides additional cyber security for our members
- The level of relevant expertise in our organisation
- The level of support we can offer to our members in obtaining such certification
- The level of support for such initiative among our members
- The extent to which such certification contributes to legal compliance for our members
- The level of endorsement of such certification by the Data Protection Authorities
- The level of endorsement of such certification by the European Union
- The level of endorsement of such certification by national government
- The level of endorsement of such certification by industry associations
- The extent of recognition of such certifications in other EU member states
- Other:
- X Don't know.

The percentage of your members that have taken out a privacy/data protection related certification:

- Low (0-20%)
- Moderate (20 - 50%)
- High (over 50%)
- X Don't know.

(Q11) What are in your view the most relevant factors influencing the decision of your members whether or not to obtain any privacy/data protection related certification?

Rate 1 (not relevant at all) to 5 (very relevant)

- Costs of privacy/data protection certifications
- The level of endorsement of certifications by industry associations
- The level of endorsement of certifications by the European Union
- The level of endorsement of such certifications by Data Protection Authorities
- The level of endorsement of such certifications by (other) government bodies
- The extent to which the certification is effective
- The extent to which certification contribute to their image
- The extent to which customers or business partners value the certification
- The extent to which competitors take out such certification
- The extent to which the certificate will protect them against GDPR related claims
- The extent of recognition of certifications in other EU member states
- Previous experiences with certifications
- Other:
- X Don't know.

5.6. Stakeholder survey results: relevant standards

5.6.1. Introduction to the Stakeholder survey results

The survey was addressed to a companies (including SME's), as well as industry associations, standardisation bodies and certification bodies. For validating the list of 12 standards drafted on the basis of studying certification mechanism (Task 2), the following approach was followed: (1a) industry associations and (1b) industry were asked to reflect on the relevance of the standards in the list and indicate which other standards were considered relevant from their perspective, (2) standardisation bodies were asked to indicate which standards were developed by their organisation and (3) certification bodies were asked to indicate on which technical standards their certification mechanism was based. The results of the survey, categorised per type of association, are as follows.

5.6.2. Survey results

5.6.3. Industry associations and industry

(a) Industry associations

As regards relevant standards, the following questions were put forward to industry associations:

Question (Q1): "Which privacy/data protection related technical standards would you recommend to your members?"¹⁵

A detailed answer to this question was unfortunately provided by only a very limited number of participants. Within that group there seems to be a significant lack of knowledge about the existence and/or value of the standards that were suggested to be relevant in the questionnaire. Next to the latter standards the following documents were each mentioned once by respondents:

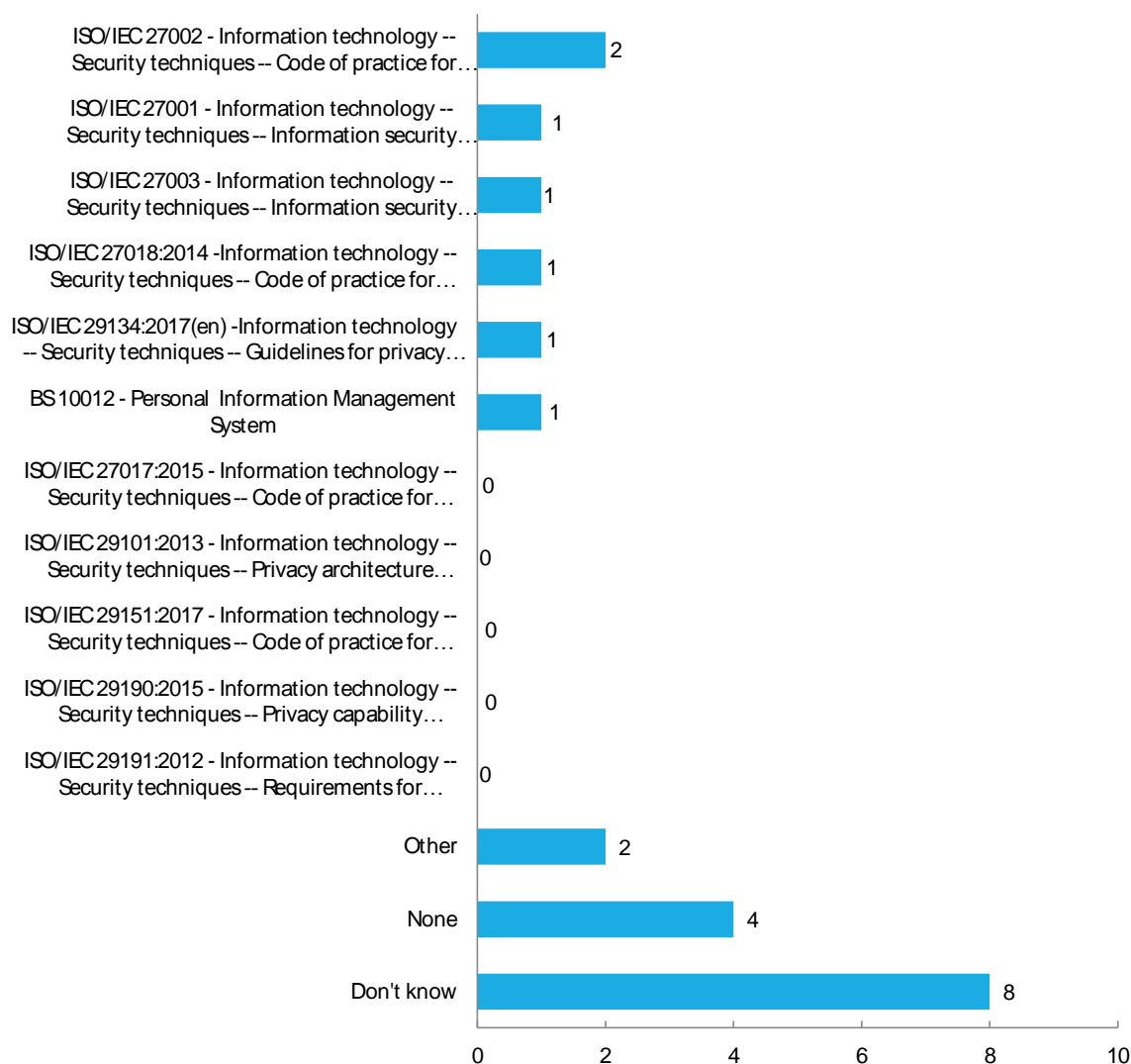
- the Cloud Security Alliance Code of Conduct for GDPR Compliance, a document aimed at specifying the application of the GDPR in the cloud environment.¹⁶
- the Cloud Security Alliance Cloud Controls Matrix (CCM), a set of measures "specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider".¹⁷
- the Cloud Computing Compliance Controls Catalogue (C5), an attestation scheme introduced by the Federal Office for Information Security (BSI) for professional cloud providers defining the minimum requirements that have to be met.¹⁸

¹⁵ Multiple answers were possible.

¹⁶ See: <https://gdpr.cloudsecurityalliance.org/news/>, accessed 17 February 2018.

¹⁷ See: https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview, accessed 17 February 2018.

¹⁸ See: https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/C5_and_Data_Protection/C5_and_Data_Protection_node.html, accessed 17 February 2018.

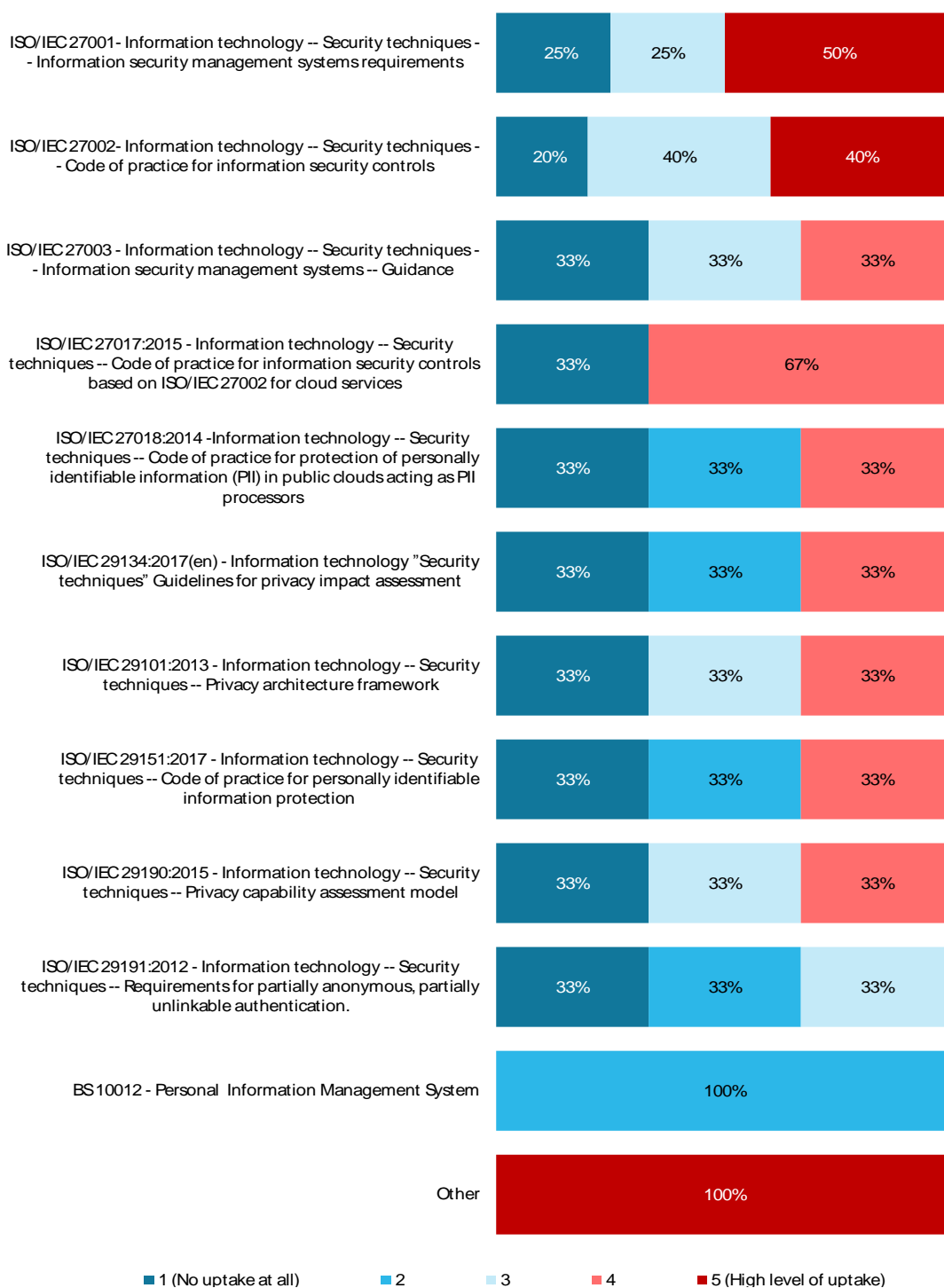


Source: Stakeholder survey

Figure 5.24

Question (Q2): "What is your estimation about the current level of uptake of the following standards amongst your members?"¹⁹

¹⁹ Multiple answers were possible. Rating from 1 (No uptake at all) to 5 (High level of uptake). If the answer is "don't know", the respondents were asked to leave the line blank.

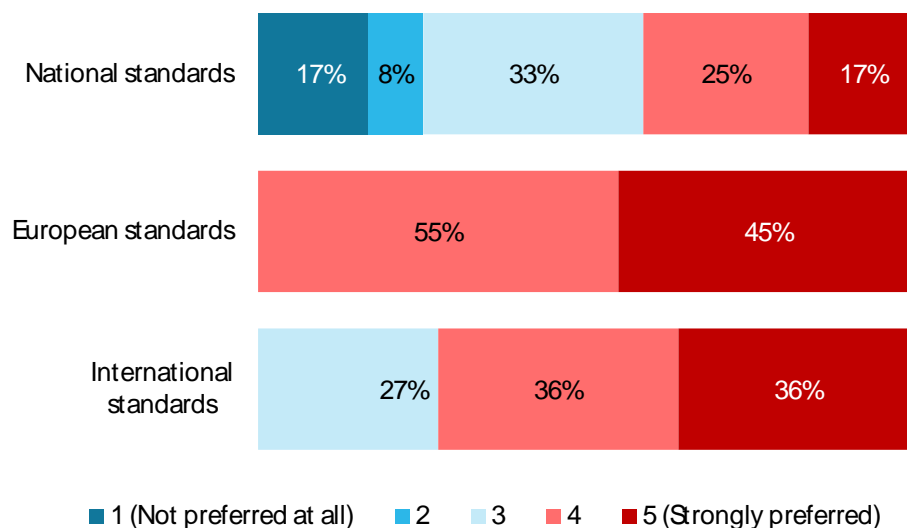


Source: Stakeholder survey

Note: From top to bottom, N=4, 5, 3, 3, 3, 3, 3, 3, 3, 3, 1, 1.

Figure 5.25

Question (Q6): "When considering implementing a technical standard in the field of privacy/data protection would your organisation prefer: Please rate from 1 (not preferred at all) to 5 (strongly preferred). If your answer is "don't know", please leave the line blank."



Source: Stakeholder survey

Note: N=12, 11, 11.

Figure 5.26

(b) Industry (SMEs and large enterprises)

As regards relevant standards, the following question was put forward to industry:

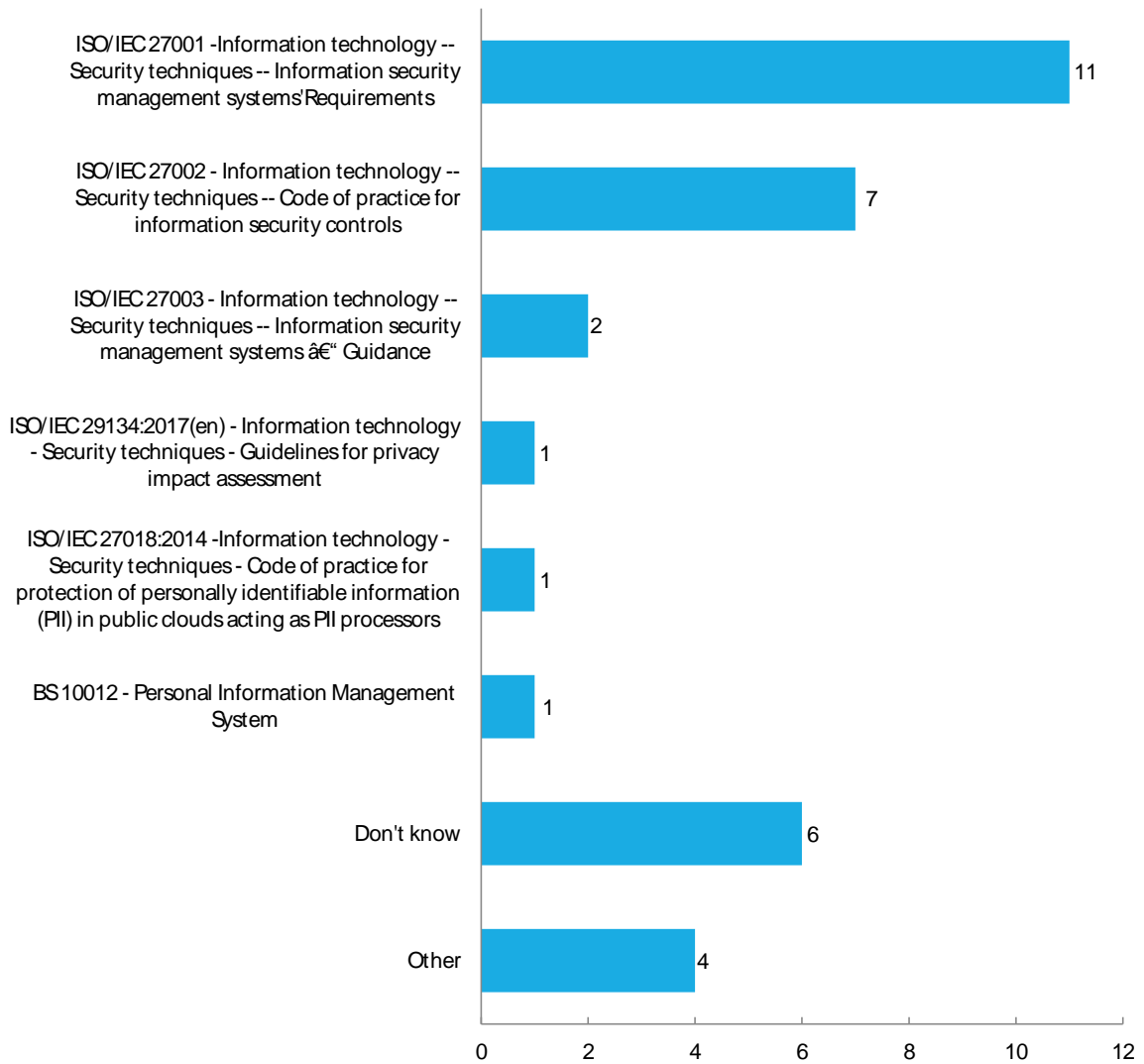
Question (Q1): "Which privacy/data protection related technical standards are being used in your organisation?"

The ISO 27001 and 27002 standards were by far most referred to. A significant portion of the respondents indicated that did not know which standards are being used in their organisation. In addition to the standards referred to in the question, a range of other standards was mentioned, including: ²⁰

- Requirements from the German BSI (Bundesamt für Sicherheit in der Informationstechnik);
- PCI DSS v3.2, EU-U.S. Privacy Shield, Swiss - U.S. Privacy Shield, HIPAA, NIST, FFIEC, PCI Forensics, NSA-CIRA, SOC 2, AV Comparatives CSA-STAR, AMTSO, and
- unspecified other guidelines, best practices and recommendations as well as regulations and regulatory standards, such as RTS of PSD2.

²⁰ Each group by one respondent only.

SMEs



Source: Stakeholder survey
 Note: multiple answers were possible.
Figure 5.27

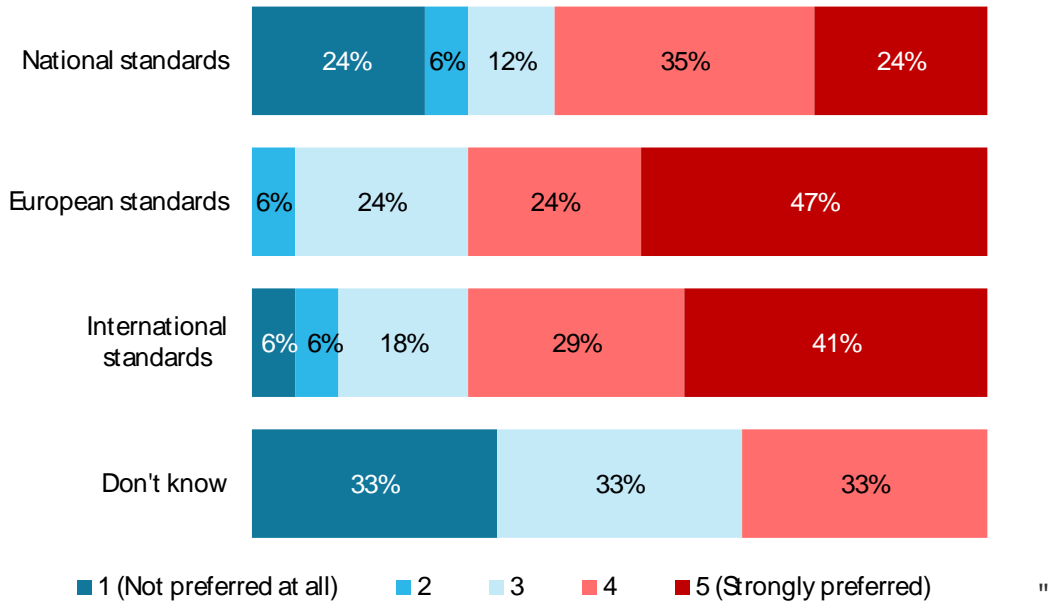
Large enterprises



Source: Stakeholder survey
 Note: multiple answers were possible.
Figure 5.28

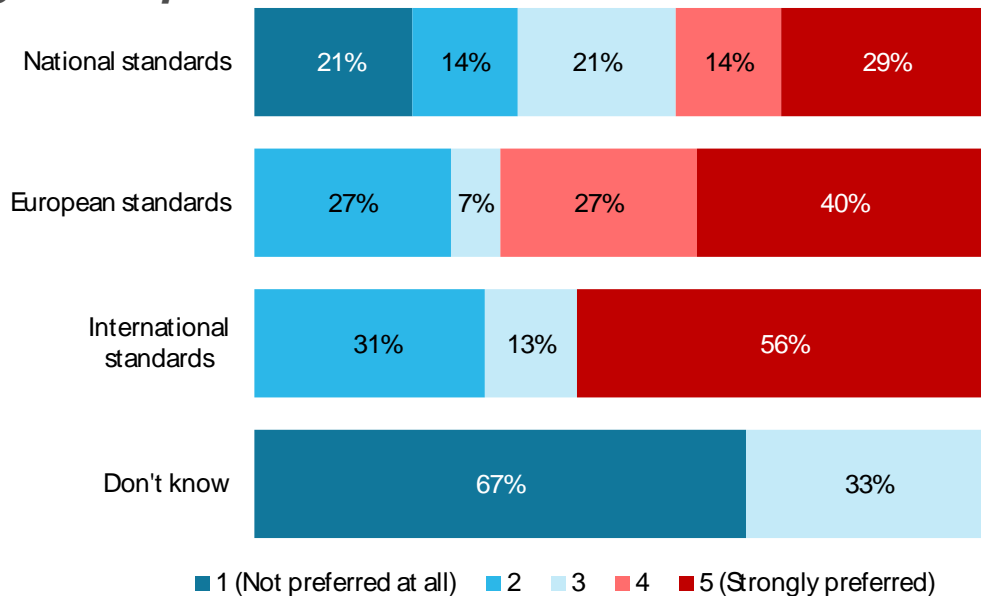
Question (Q7): "When considering implementing a technical standard in the field of privacy/data protection would your organisation prefer: Please rate from 1 (not preferred at all) to 5 (strongly preferred). If your answer is "don't know", please leave the line blank."

SMEs



Source: Stakeholder survey
 Note: N=17, 17, 17, 3.
Figure 5.29

Large enterprises

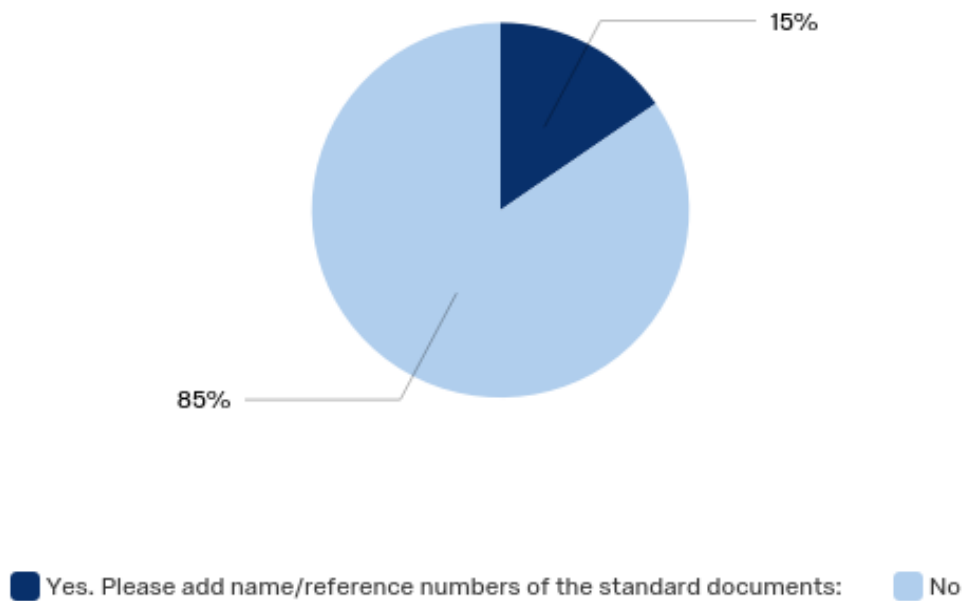


Source: Stakeholder survey
 Note: N=14, 15, 16, 3.
Figure 5.30

5.6.4. Survey results: standardisation bodies

Question (Q1): "Has your organisation developed privacy/data protection related standards?"

Only a very small number of the total respondents had developed privacy/data protection related standards. The answers provided were accordingly hence not significant.²¹



Source: Stakeholder survey

Note: N=13

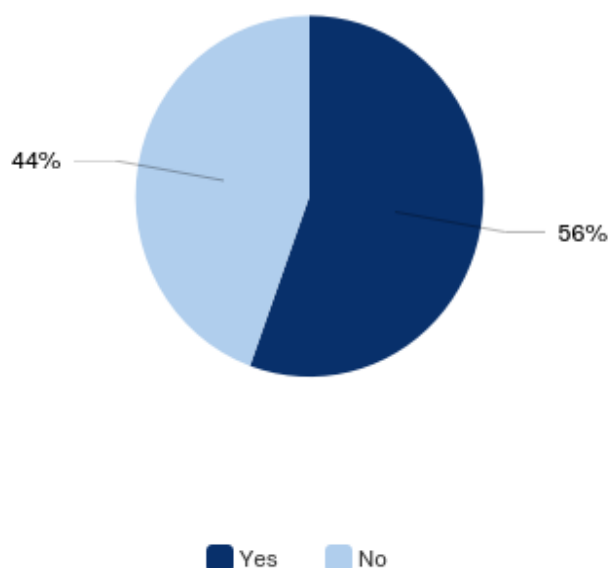
Figure 5.31

5.6.5. Survey results: certification bodies

Question (Q3a): "Is your certification mechanism based on certain technical standards?"

Interestingly, a significant number of the respondents indicated that their scheme was not based on technical standards.

²¹ The number of organisations that had developed standards was accordingly too low attach significance to the responses to questions 2 (nature of these standards), 3 (sector specific?) and 4 (reasons for updating privacy/data protection related standards).



Source: Stakeholder survey

Note: N=9

Figure 5.32

Question (Q3b): "If yes, which of the following standards does it concern?"

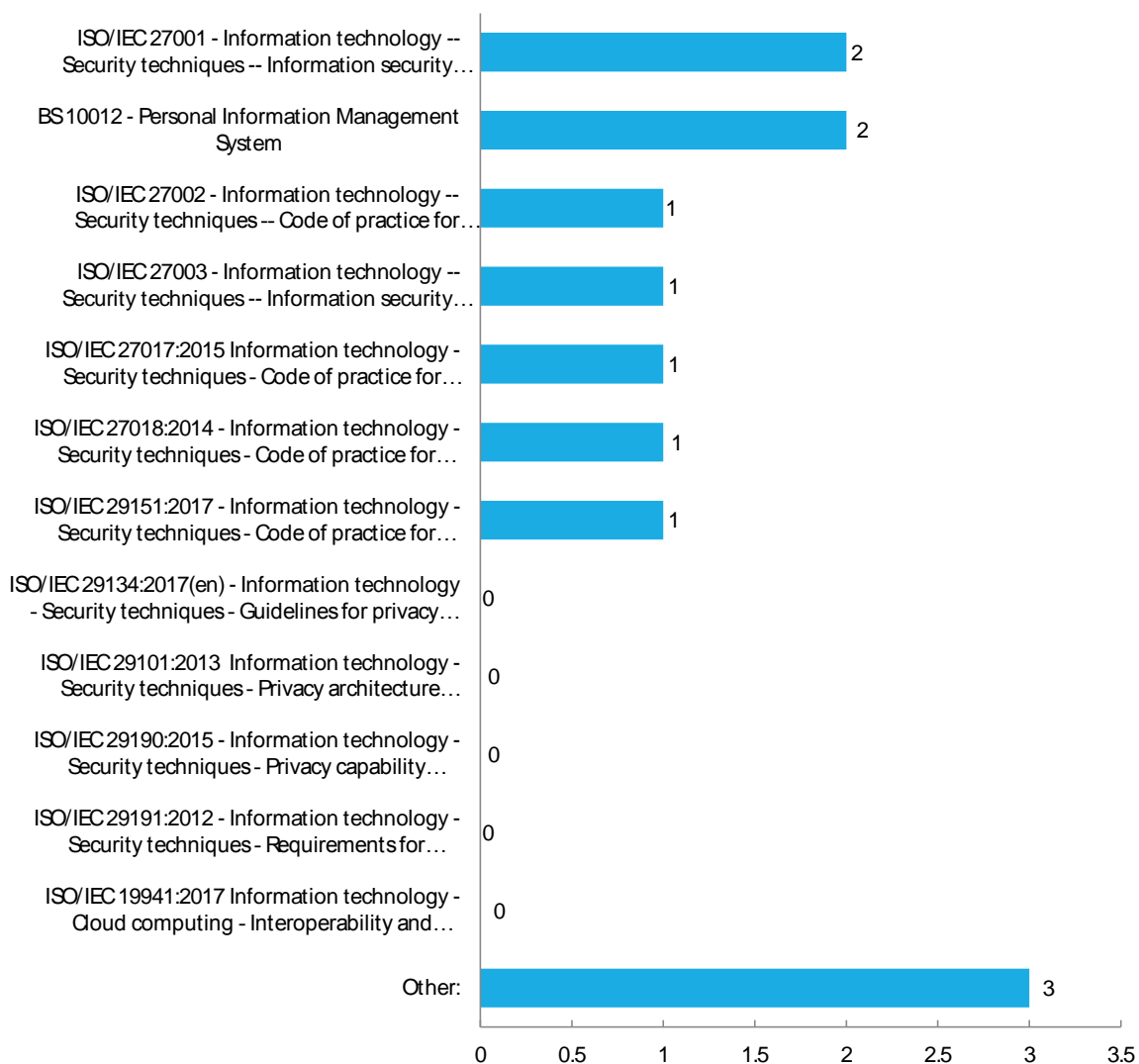
To the extent standards were underlying these schemes, it concerned mainly ISO-27000 series standards and the BS10012 standard.

Other standards referred to, in addition to the ones mentioned in the graph below, were:

- ISO 17065²² and ISO 17021 framework requirements
- Requirements from the German BSI (Bundesamt für Sicherheit in der Informationstechnik) and
- unspecified other guidelines, best practices and recommendations as well as regulations and regulatory standards, such as RTS of PSD2.²³

²² This is however an accreditation standard.

²³ No responses were provided to the follow up questions 4, 5, 6 7 and 7(b) for certification bodies.



Source: Stakeholder survey

Figure 5.33

5.7. Stakeholder survey results: uptake factors (including other mechanisms to promote and recognise)

5.7.1. Introduction to the Stakeholder survey results

In the survey several questions were related, directly or indirectly to uptake factors as well as to other mechanisms to promote or recognise standards or certifications. Relevant questions and results are described below for standards and for certifications.

5.7.2. Uptake factors for standards

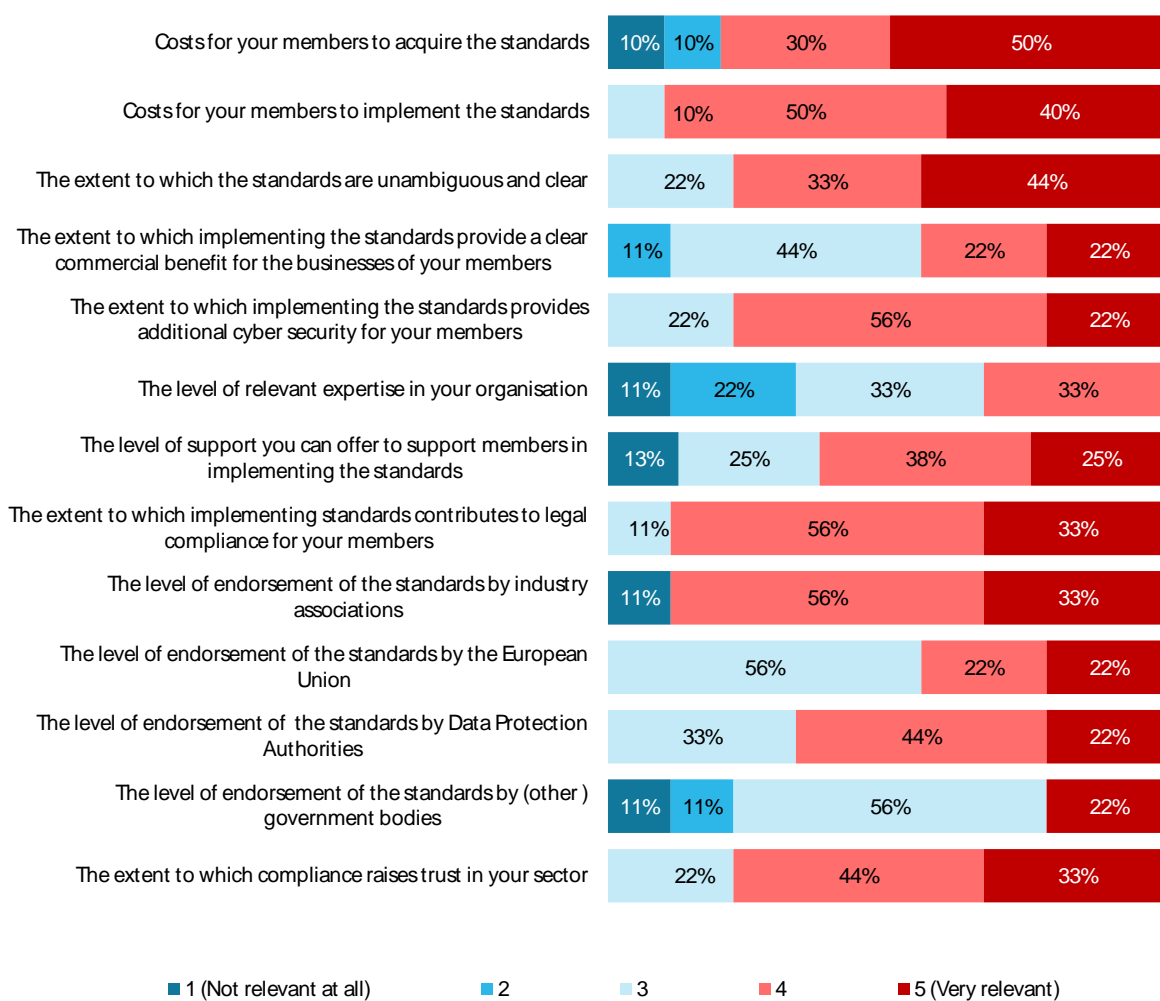
5.7.2.1. Responses from industry associations

Question (Q3): "What are the most relevant factors for your organisation when deciding about promoting the implementation of privacy/data protection related technical standards by your members?"²⁴

Industry associations considered a whole range of factors to be significant or very significant in deciding about promoting standards, and in particular:

- the costs for acquiring and implementing a standard;
- the quality of the standard;
- the extent to which implementing the standard contributes to legal compliance;
- the level of endorsement of the standard by industry associations;
- the extent to which compliance with the standard raises trust in their sector.

²⁴ Multiple answers were possible. Rating from 1 (No uptake at all) to 5 (High level of uptake). If the answer is "don't know", the respondents were asked to leave the line blank.



Source: Stakeholder survey

Note: From top to bottom, N=10, 10, 9, 9, 9, 9, 8, 9, 9, 9, 9, 9, 9.

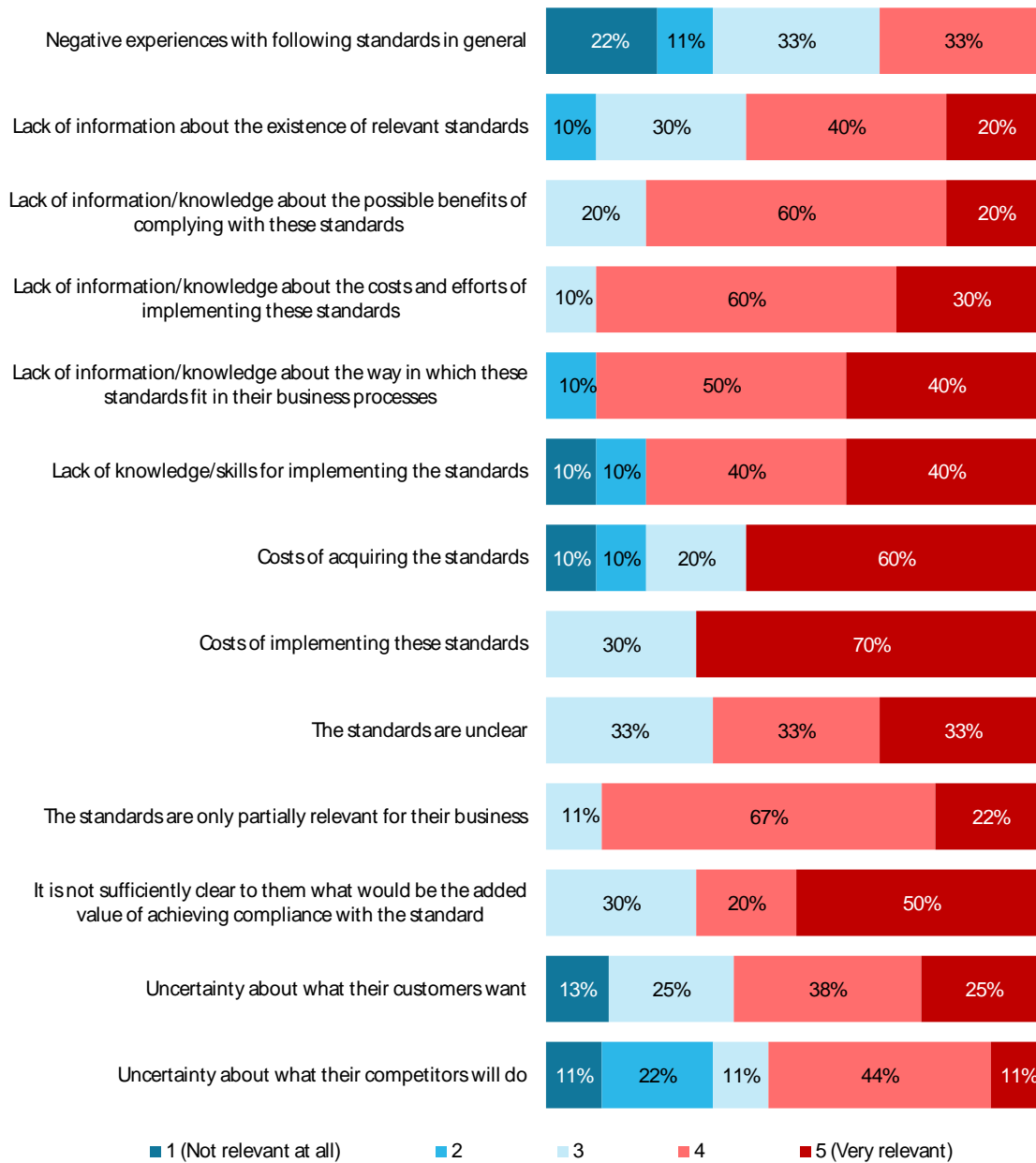
Figure 5.34

Question (Q4): "In your view, which challenges do you think your members encounter most when it comes to implementing privacy/data protection related technical standards?"²⁵

Industry associations considered a whole range of challenges to be significant or very significant in this context, and in particular:

- the costs for acquiring and implementing a standard;
- the quality of the standard;
- the lack of information/knowledge about the way in which the standard fits in their business processes;
- the lack of knowledge/skills for implementing the standard;
- the lack of clarity as regards the added value of the standard.

²⁵ Multiple answers were possible. Rating from 1 (No uptake at all) to 5 (High level of uptake). If the answer is "don't know", the respondents were asked to leave the line blank.

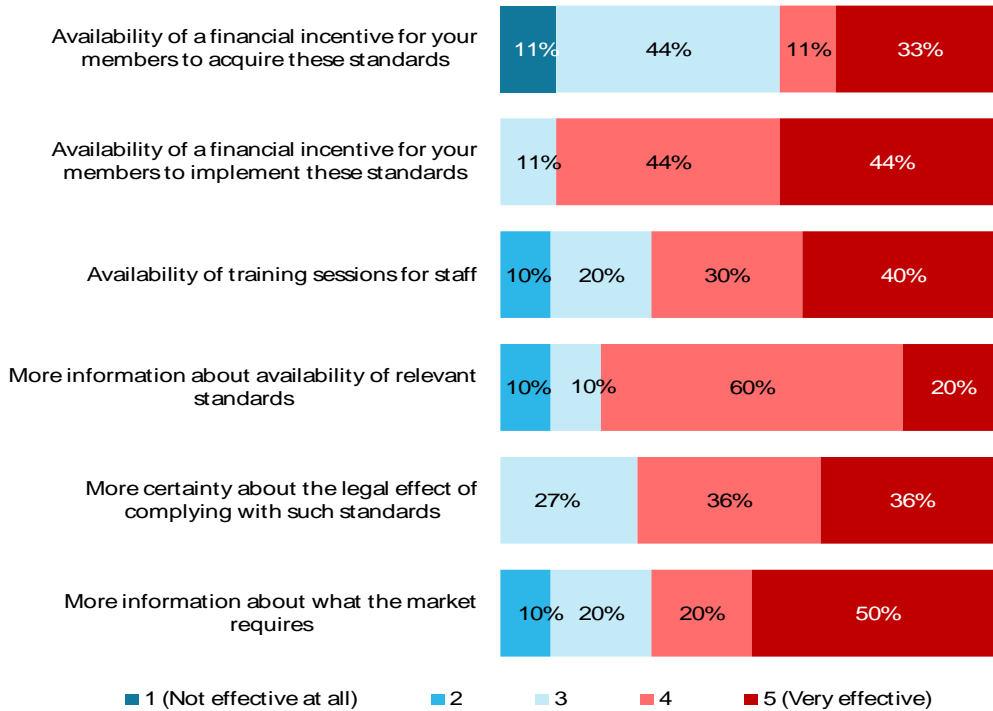


Source: Stakeholder survey

Note: N=9, 10, 10, 10, 10, 10, 10, 10, 9, 9, 10, 8, 9.

Figure 5.35

Question (Q7): "Which instrument(s)/mechanism(s) would be most effective for your organisation in making the decision to promote compliance with privacy/data protection related technical standards amongst your members?"²⁶



Source: Stakeholder survey
 Note: N=9, 9, 10, 10, 11, 10.

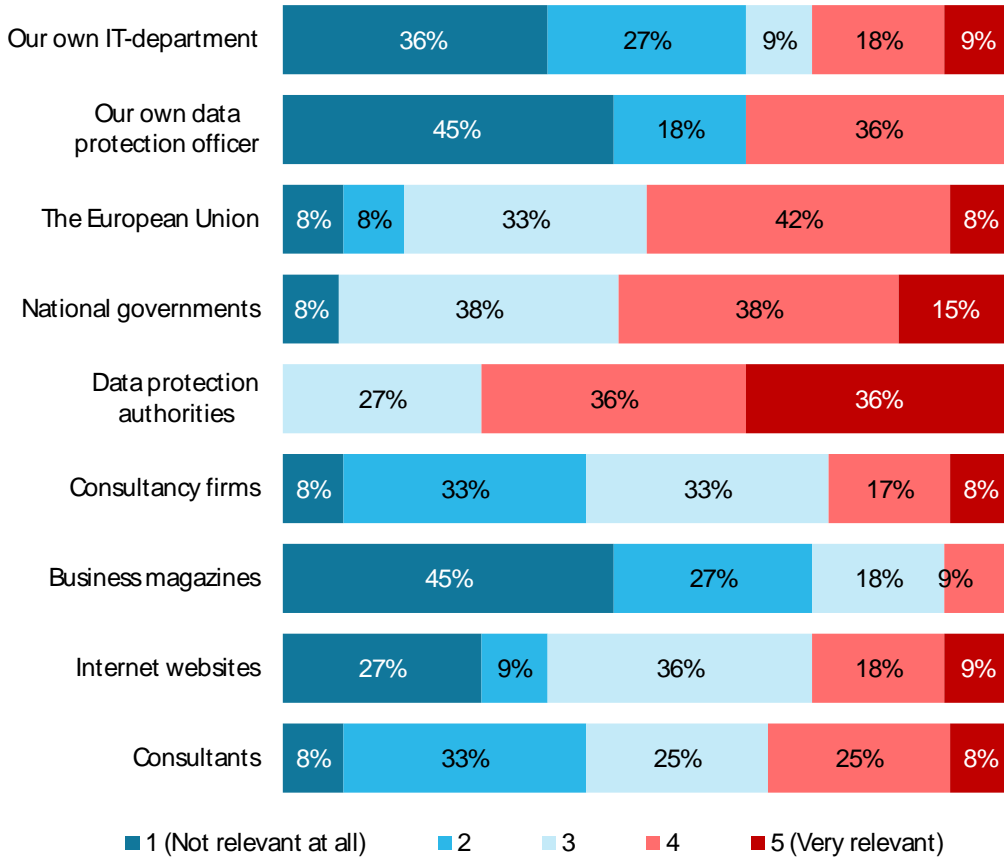
Figure 5.36

Other:

Comments
Law is the only relevant incentive

²⁶ Multiple answers were possible. Rating from 1 (Not effective at all) to 5 (Very effective). If the answer is "don't know", the respondents were asked to leave the line blank.

Question (Q8): "Which source(s) would your organisation rely on most as regards obtaining information that could improve your awareness about the availability and effects of technical standards in the field of privacy/data protection?"²⁷



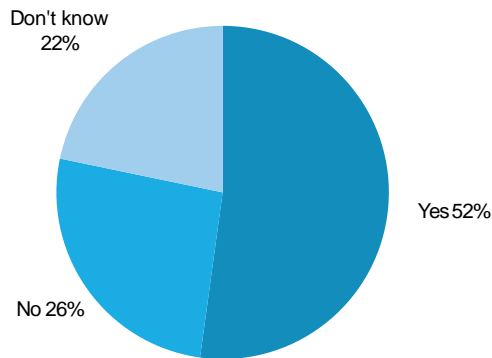
Source: Stakeholder survey
 Note: N=11, 11, 12, 13, 11, 12, 11, 11, 12.
Figure 5.37

²⁷ Multiple answers were possible. Rating from 1 (Not relevant at all) to 5 (Very relevant). If the answer is "don't know", the respondents were asked to leave the line blank.

5.7.2.2. Responses from industry

Question (Q2): "Does your organisation have sufficient information about the availability of privacy/data protection related technical standards?"

SMEs

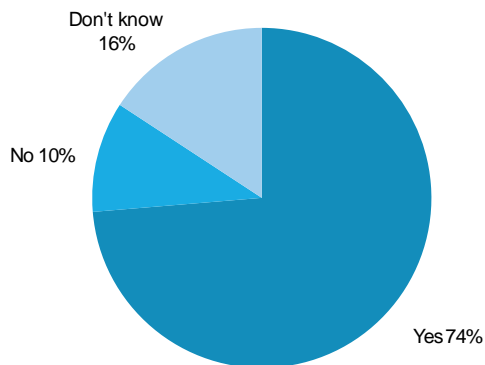


Source: Stakeholder survey

Note: N=23

Figure 38

Large enterprises



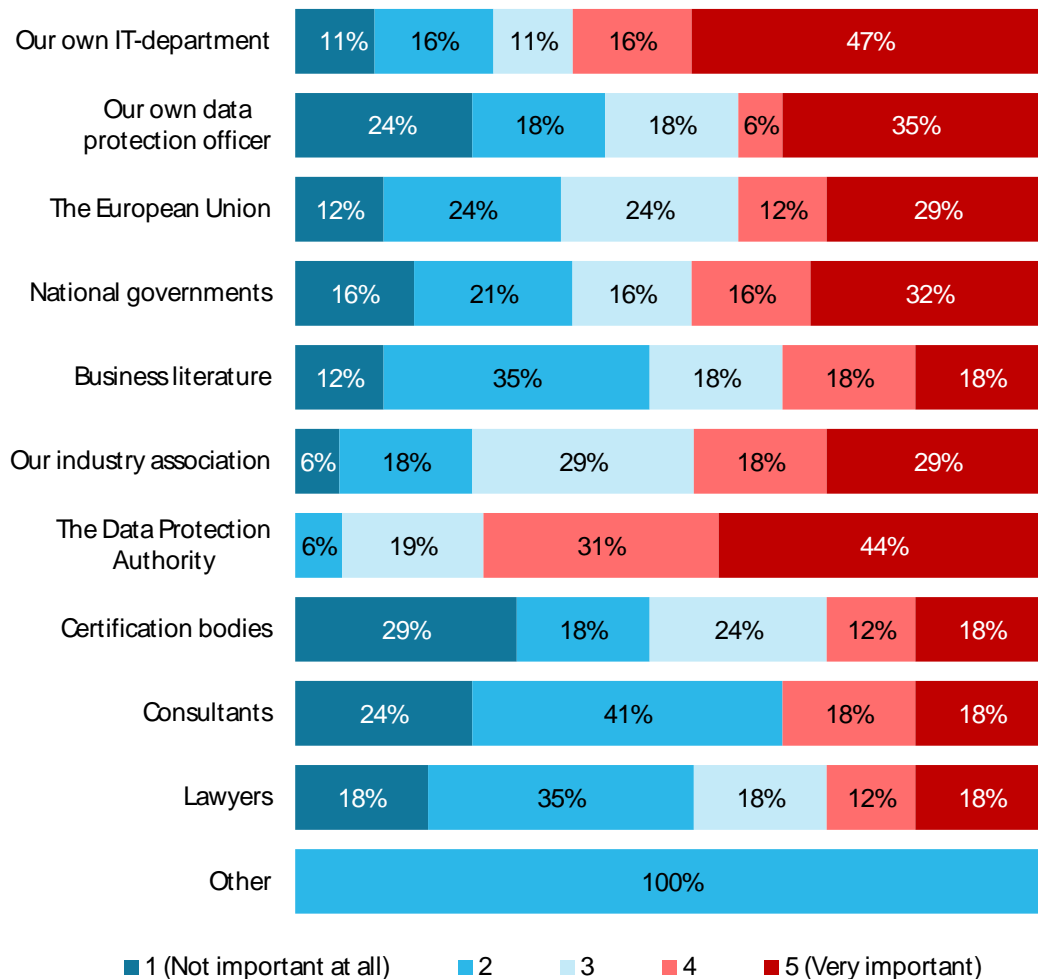
Source: Stakeholder survey

Note: N=19.

Figure 5.39

Question (Q3): "Which source(s) does your organisation rely on most for obtaining information about privacy/data protection related technical standards?"²⁸

SMEs



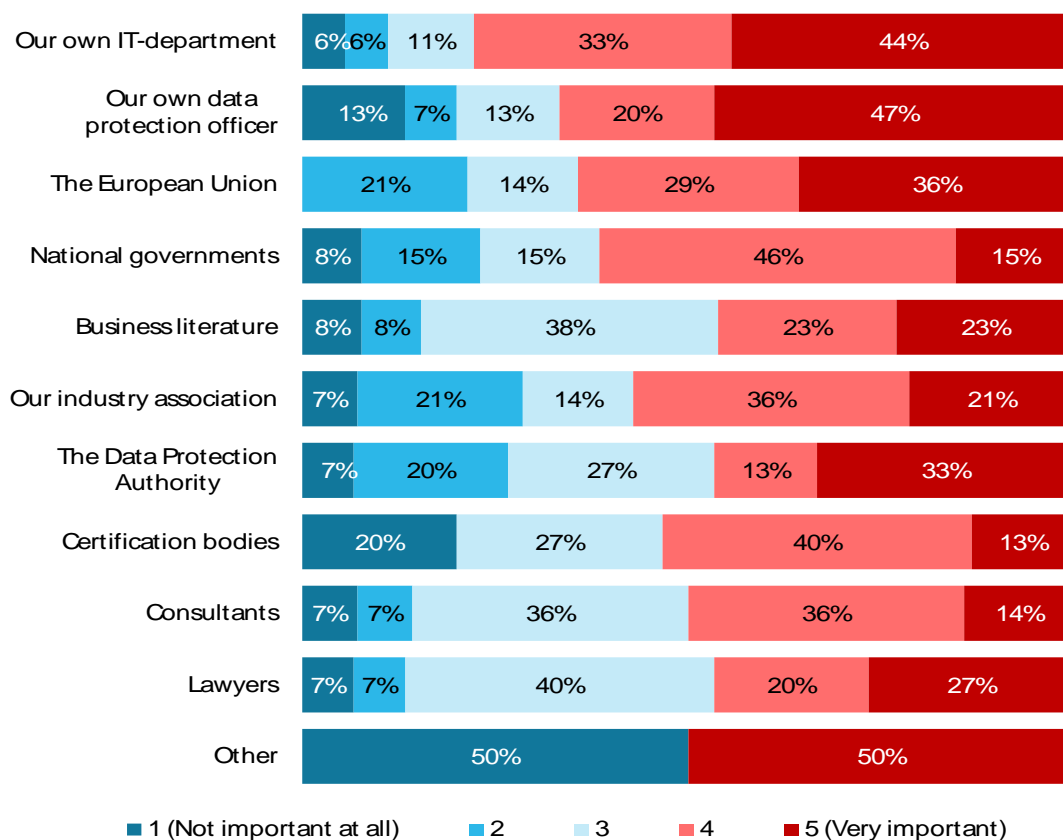
Source: Stakeholder survey

Note: N=19, 17, 17, 19, 19, 17, 17, 16, 17, 17, 17, 1.

Figure 5.40

²⁸ Multiple answers were possible. Rating from 1 (Not important at all) to 5 (Very important). If the answer is "don't know", the respondents were asked to leave the line blank.

Large enterprises



Source: Stakeholder survey

Note: N=18, 15, 14, 13, 13, 14, 15, 15, 14, 15, 2.

Figure 5.41

Question (Q4): "What are the most relevant factors when deciding whether to implement privacy/data protection related technical standards?"²⁹

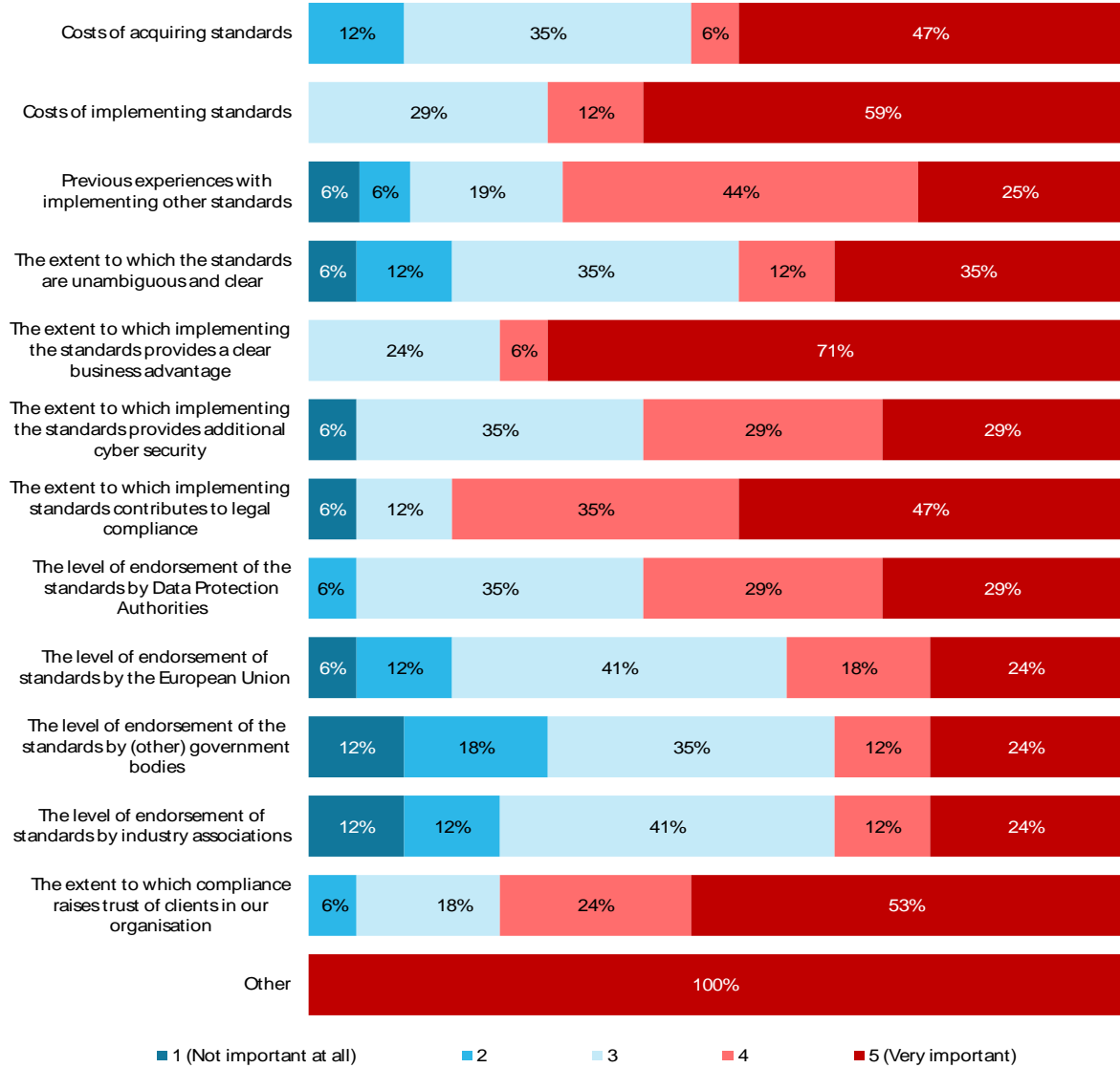
For SMEs and for large enterprises the following factors were considered to be (very) relevant:

- impact on legal compliance
- impact on trust raised by clients
- business advantage
- costs of implementing standards
- previous experiences with implementing standards

No differentiation in the kind of factors relevant was found between SMEs and large enterprises in this respect. Also, the sequence of relevance was found to be similar in both situations.

²⁹ Multiple answers were possible. Rating from 1 (No uptake at all) to 5 (High level of uptake). If the answer is "don't know", the respondents were asked to leave the line blank.

SMEs

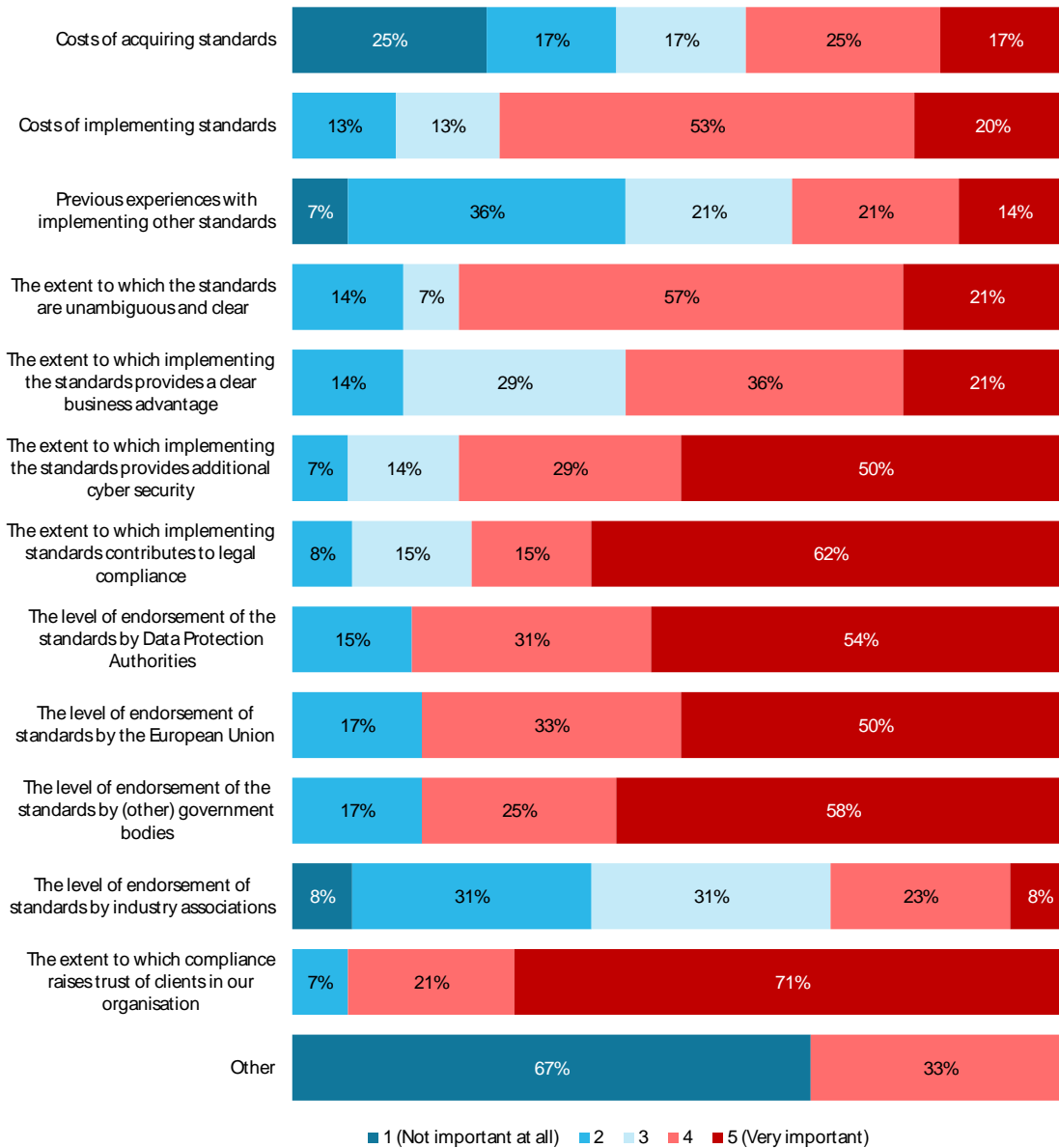


Source: Stakeholder survey

Note: N=17, 17, 16, 17, 17, 17, 17, 17, 17, 17, 17, 17, 1.

Figure 5.42

Large enterprises



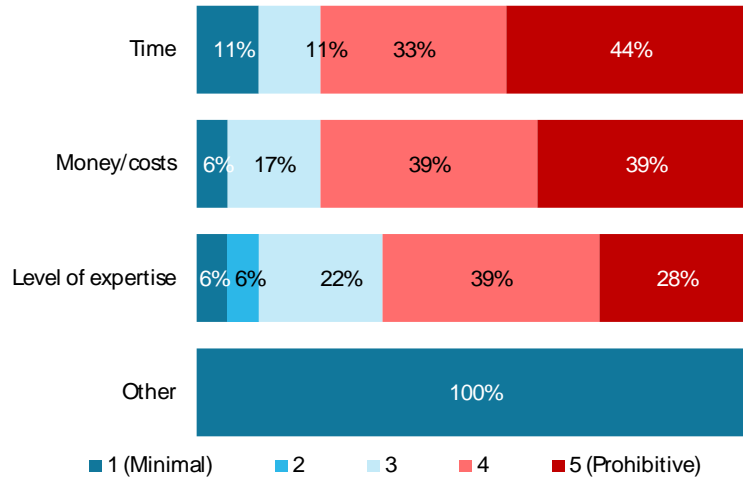
Source: Stakeholder survey

Note: N=12, 15, 14, 14, 14, 14, 13, 13, 12, 12, 13, 14, 3.

Figure 5.43

Question (Q5): " In order to achieve compliance with privacy/data protection companies in our sector have to invest:...." ³⁰

SMEs

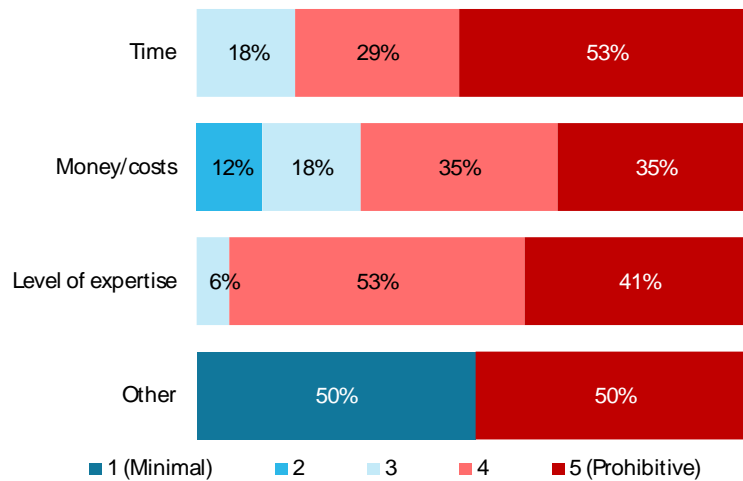


Source: Stakeholder survey

Note: N=18, 18, 18, 1.

Figure 5.44

Large enterprises



Source: Stakeholder survey

Note: N=17, 17, 17, 2.

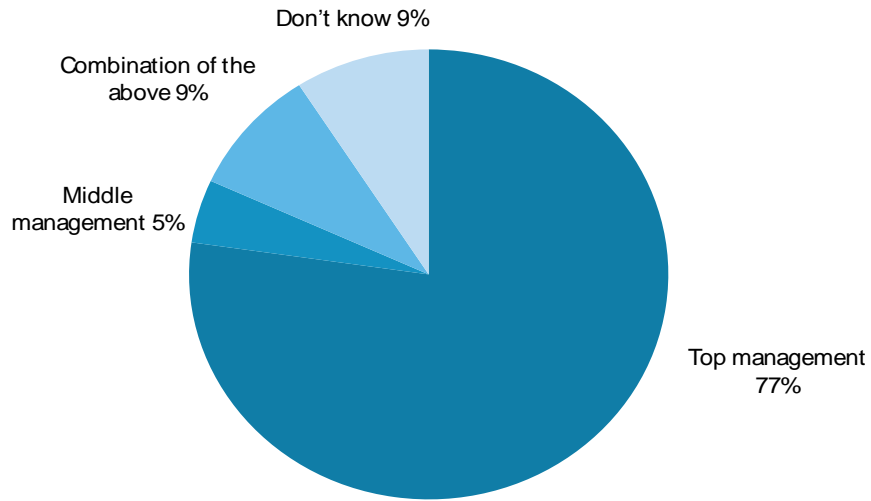
Figure 5.45

Comment by one of the respondents: "Invest in certification to gain legal certainty."

³⁰ Multiple answers were possible. Rating from 1 (Minimal) to 5 (Prohibitive). If the answer is "don't know", the respondents were asked to leave the line blank.

Question (Q6): "On which level in your organisation are decisions usually made about implementing a privacy/data protection-related standard?"

SMEs

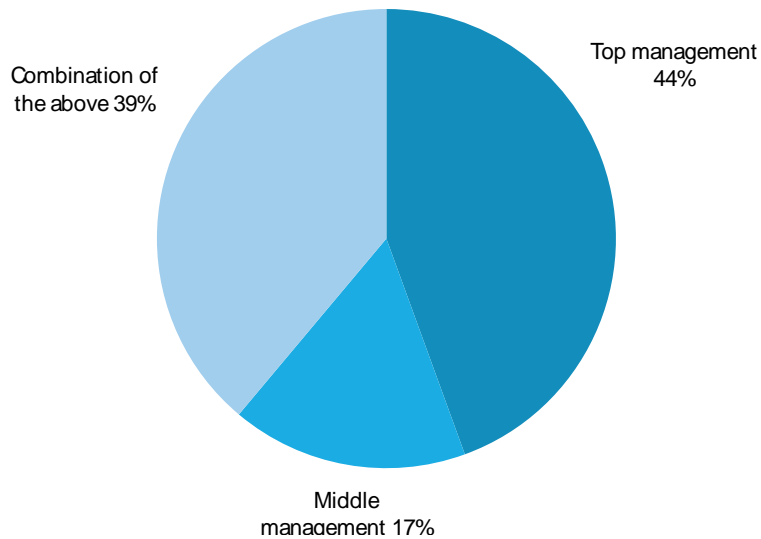


Source: Stakeholder survey

Note: N=22.

Figure 5.46

Large enterprises



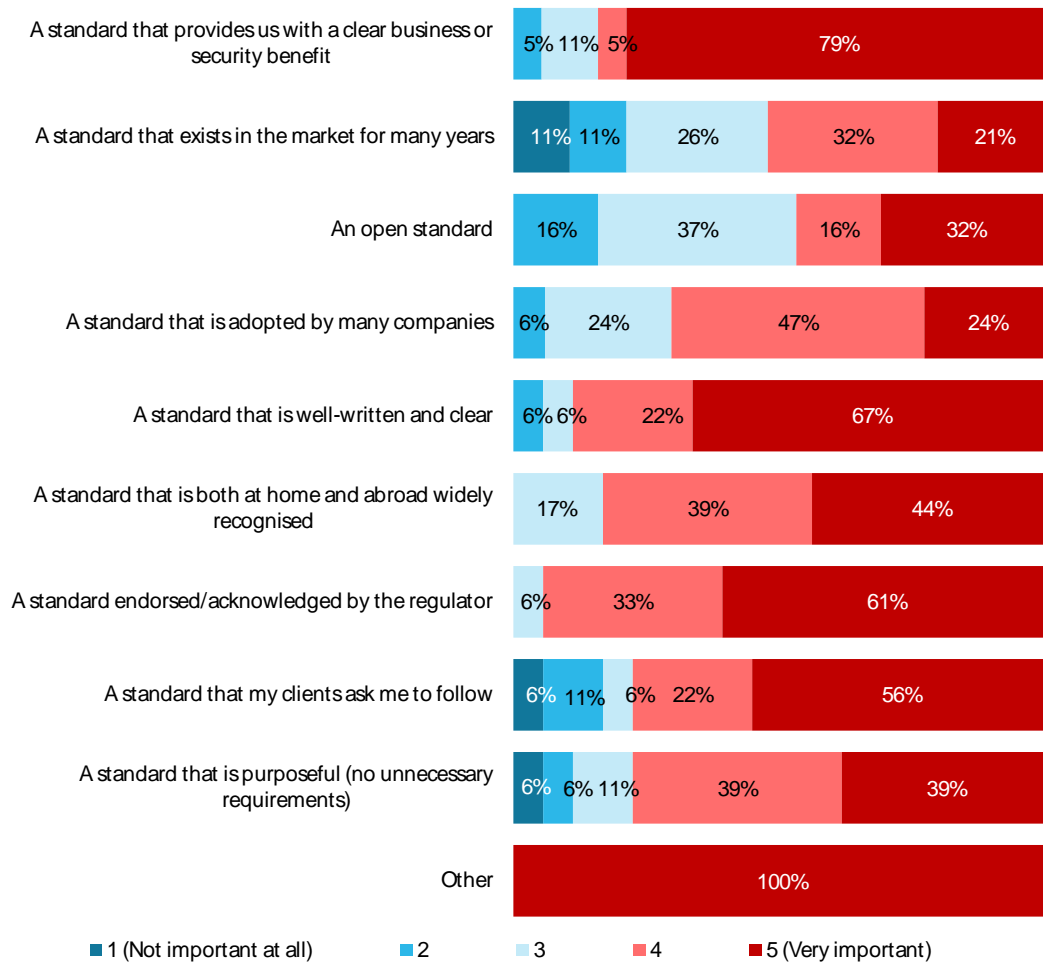
Source: Stakeholder survey

Note: N=18

Figure 5.47

Question (Q8): "What do you consider a successful standard?" ³¹

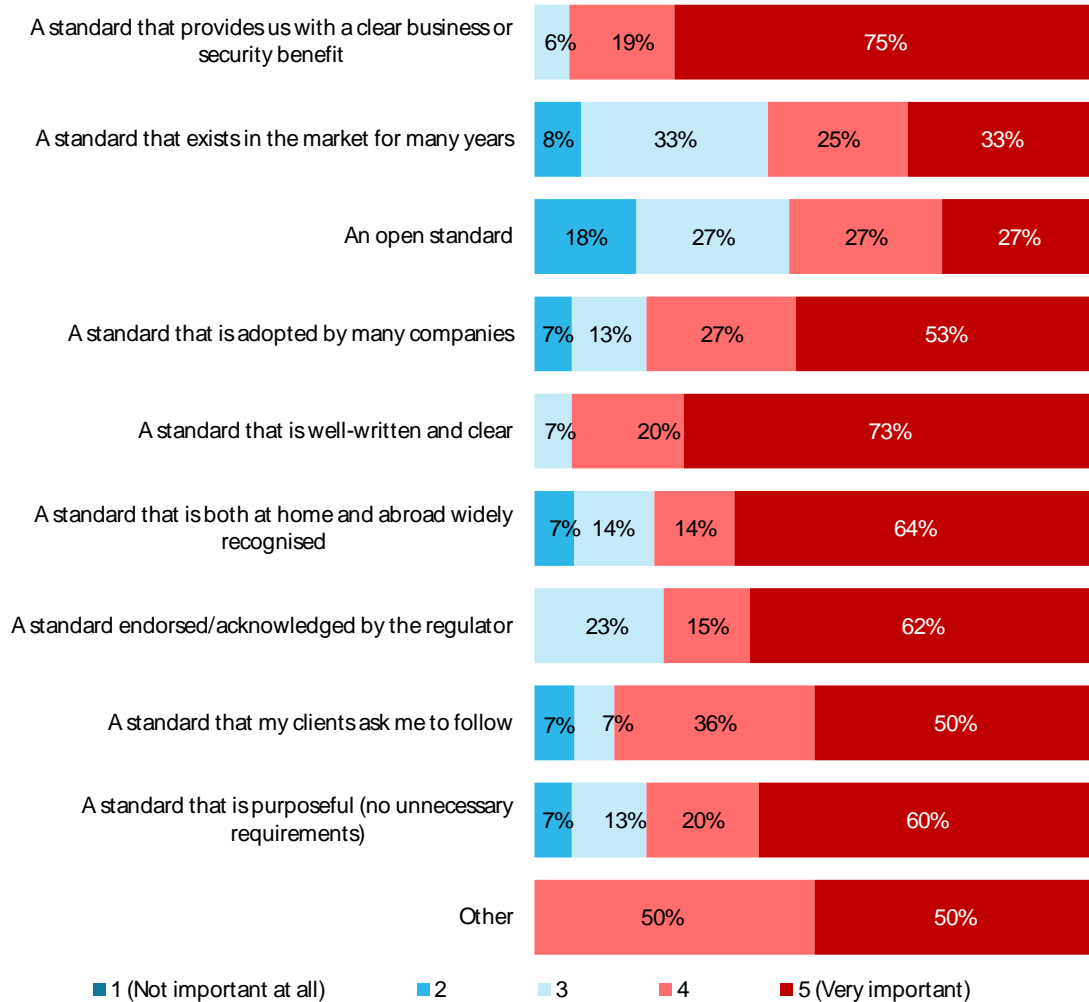
SMEs



Source: Stakeholder survey
 Note: N=19, 19, 19, 17, 18, 18, 18, 18, 18, 1.
Figure 5.48

³¹ Multiple answers were possible. Rating from 1 (Not important at all) to 5 (Very important). If the answer is "don't know", the respondents were asked to leave the line blank.

Large enterprises



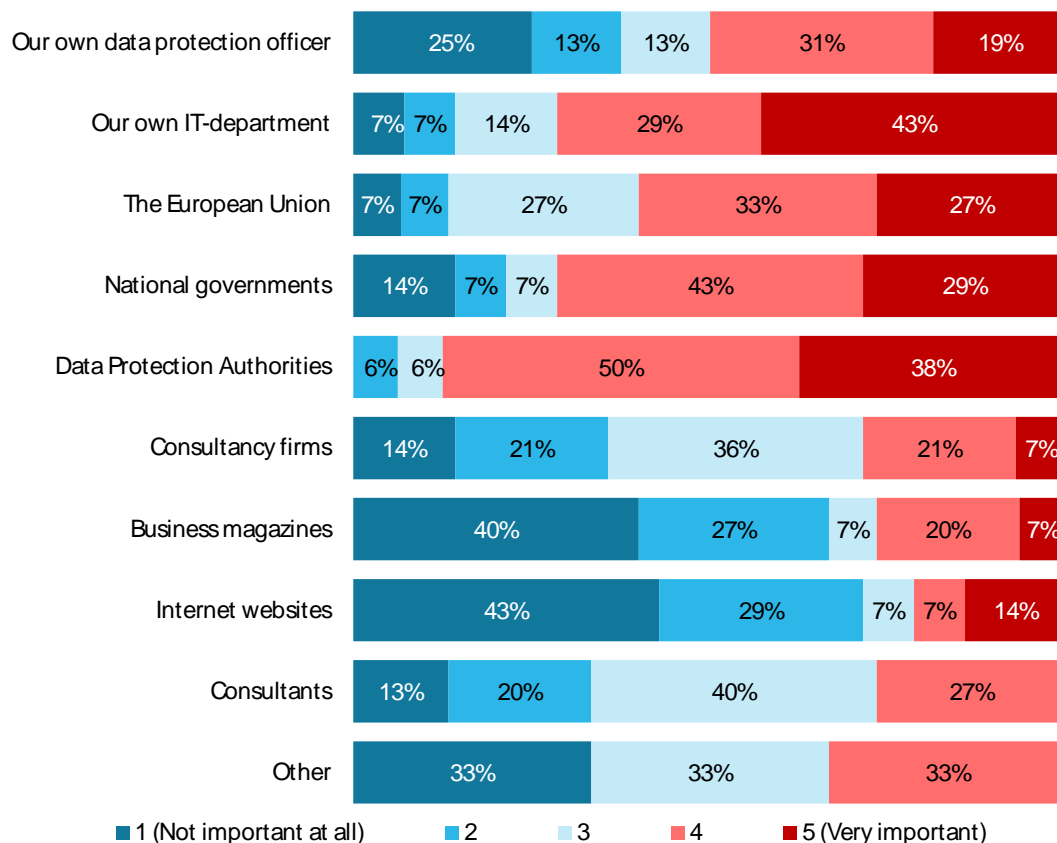
Source: Stakeholder survey
 Note: N=16, 12, 11, 15, 15, 14, 13, 14, 15, 2.
Figure 5.49

Comments by respondents:

1. "A standard that provides clear cybersecurity requirements on various layers starting with key principles to cover baseline requirements on security & privacy up to various levels of security in different segments based on proper risk and impact assessments from different angles (business/citizen/society/digital sovereignty)";
2. "Affordable: the ISO27000 standards are very expensive to attain for SMEs.

Question (Q11): "What are/is for your organisation the most important source(s) for obtaining information about the existence of privacy/data protection related certifications?"³²

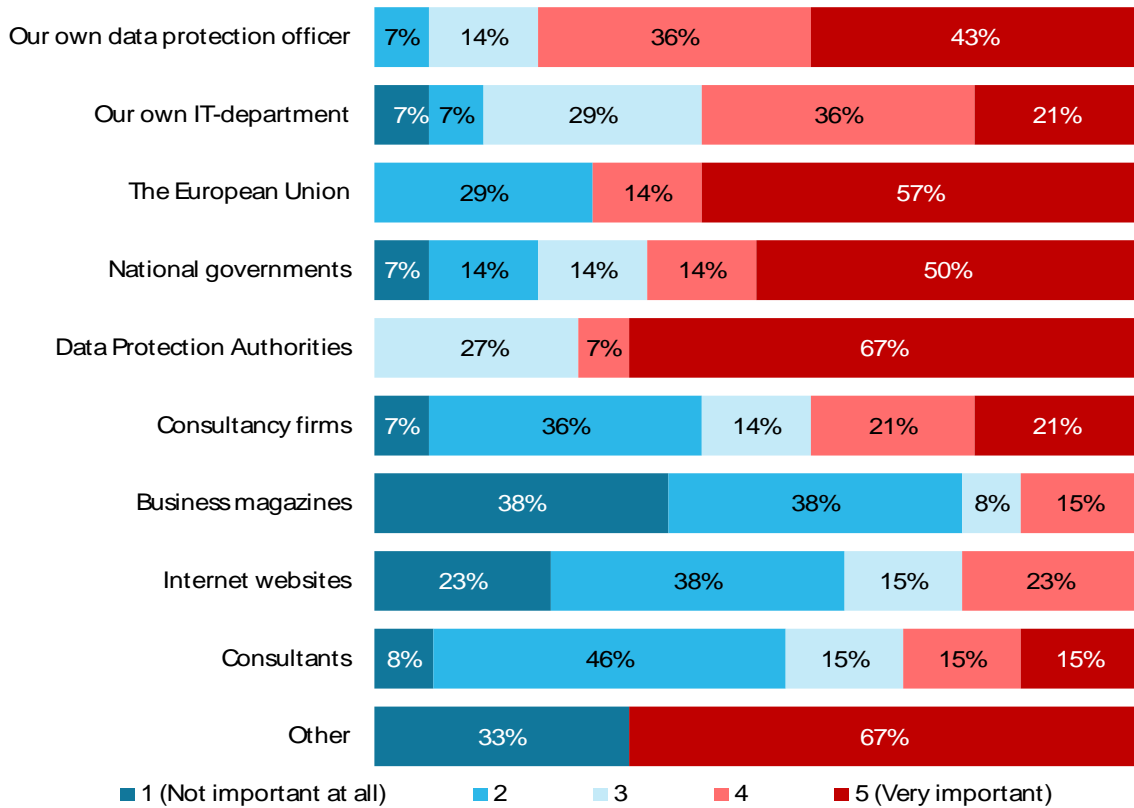
SMEs



Source: Stakeholder survey
 Note: N=16, 14, 15, 14, 16, 14, 15, 14, 15, 3.
Figure 5.50

³² Multiple answers were possible. Rating from 1 (Not important at all) to 5 (Very important). If the answer is "don't know", the respondents were asked to leave the line blank.

Large enterprises



Source: Stakeholder survey
 Note: N=14, 14, 14, 14, 15, 14, 13, 13, 13, 3.
Figure 5.51

Comments from respondents:

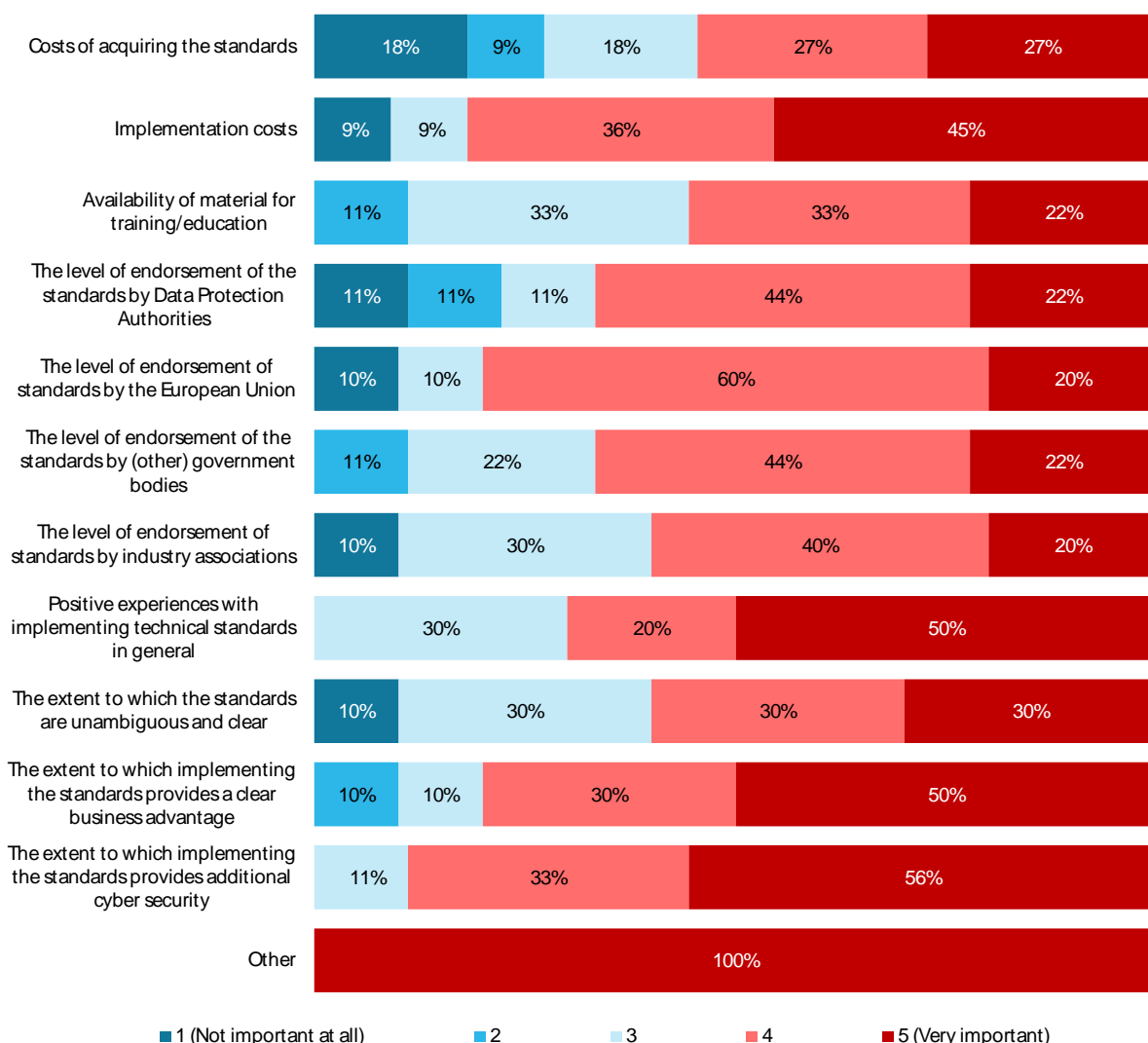
- "Certification bodies defining protection profiles"
- "Global standards team"
- "National accreditation authorities"

5.7.2.3. Responses from standardisation bodies

Question (Q3): "What are in your view the most important factors determining the level of uptake of privacy/data protection-related standards in the market?"³³

Standardisation bodies considered a whole range of challenges to be significant or very significant in this context, and in particular:

- implementation costs;
- endorsement by the European Union;
- the effect of a standard in terms of business advantage and improved cyber security.



Source: Stakeholder survey
 Note: N=11, 11, 9, 9, 10, 9, 10, 10, 10, 10, 9, 2.

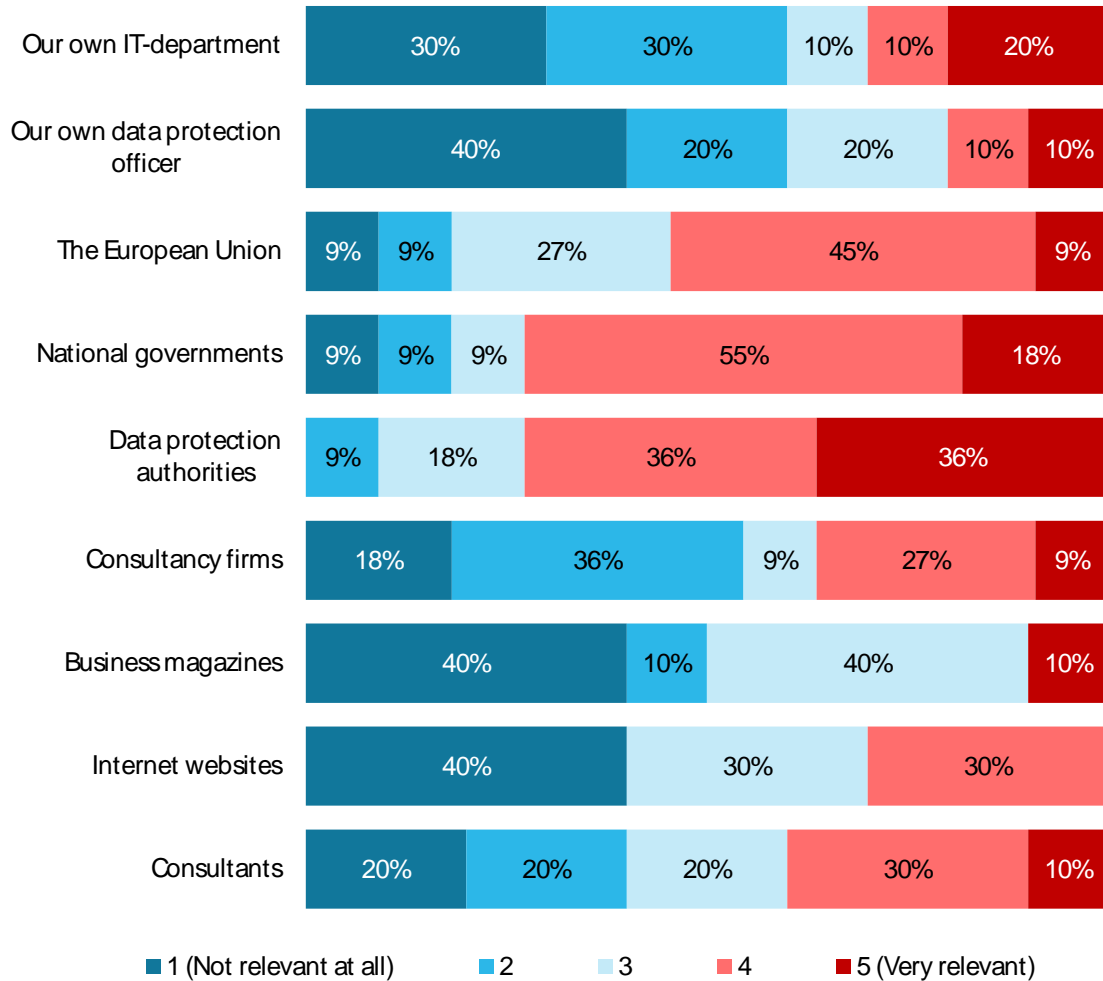
Figure 5.52

³³ Multiple answers were possible. Rating from 1 (No uptake at all) to 5 (High level of uptake). If the answer is "don't know", the respondents were asked to leave the line blank.

5.7.3. Uptake factors for certification

5.7.3.1. Responses from industry associations

Question (Q9): "Which source(s) would your organisation rely on most as regards obtaining information that could improve your awareness about the existence of privacy/data protection related certifications?"³⁴

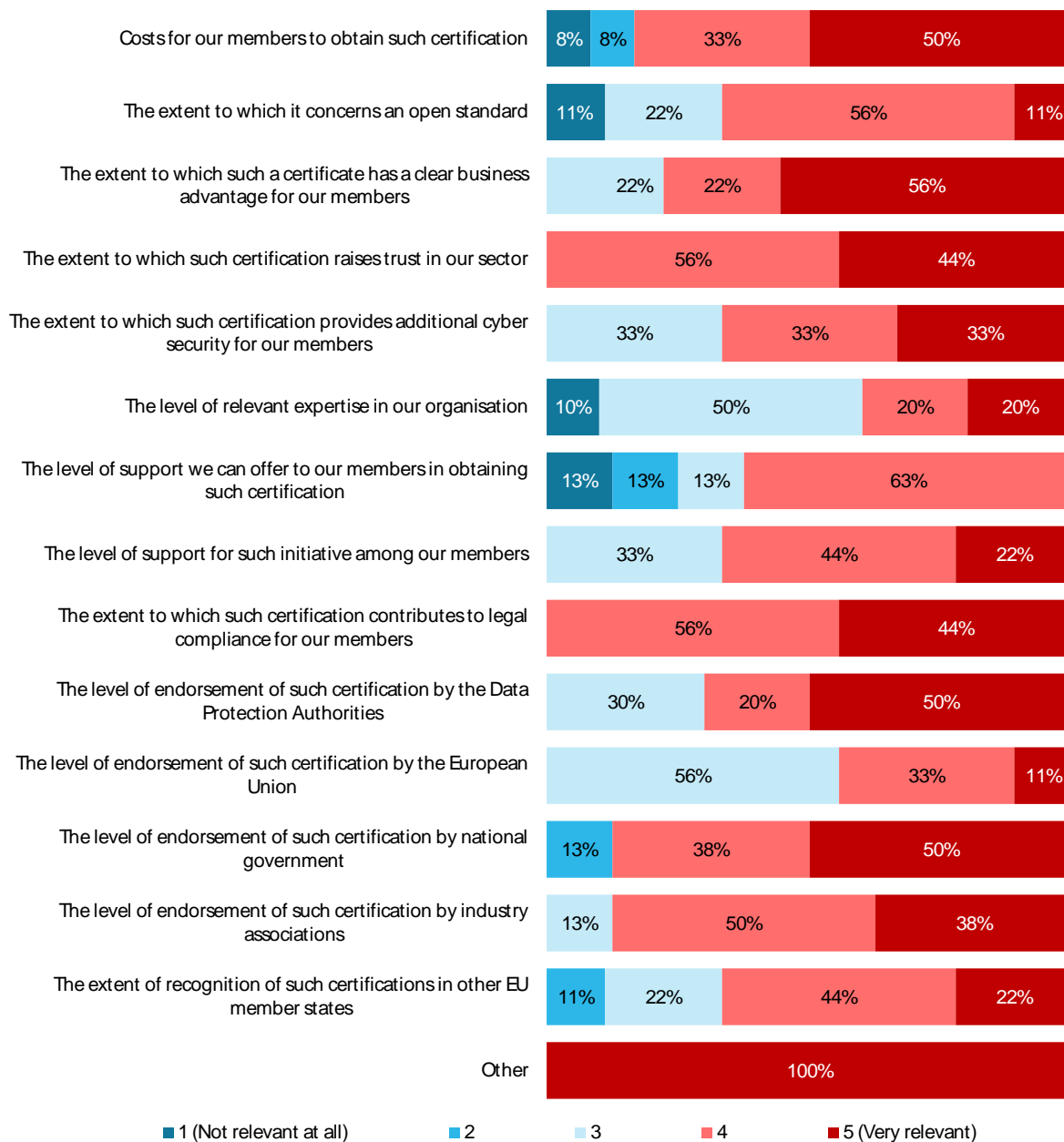


Source: Stakeholder survey

Figure 5.53

³⁴ Multiple answers were possible. Rating from 1 (Not relevant at all) to 5 (Very relevant). If the answer is "don't know", the respondents were asked to leave the line blank.

Question (Q10): "What are the most relevant factors for your organisation when deciding about promoting privacy/data protection related technical certifications?"³⁵



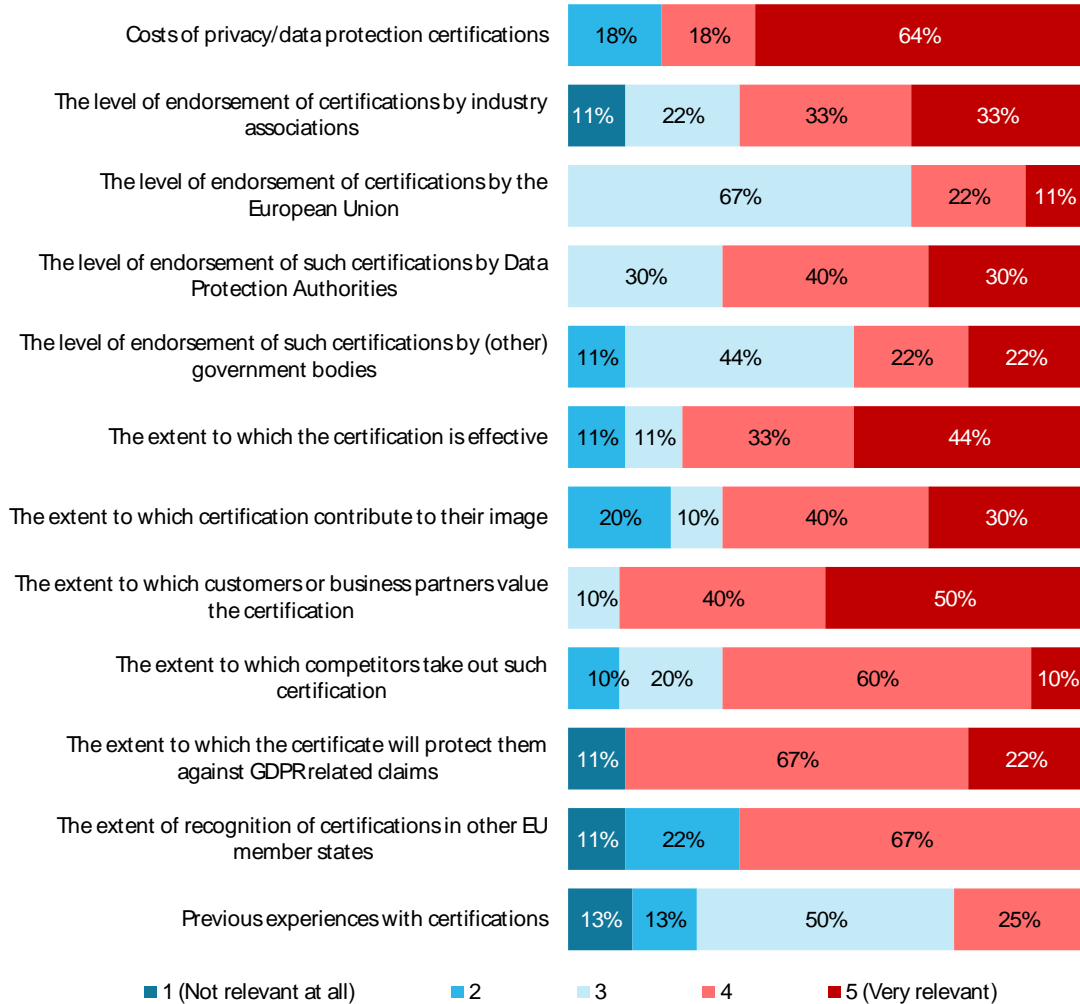
Source: Stakeholder survey

Note: N=12, 9, 9, 9, 9, 10, 8, 9, 9, 10, 9, 8, 8, 9, 1.

Figure 5.54

³⁵ Multiple answers were possible. Rating from 1 (No uptake at all) to 5 (High level of uptake). If the answer is "don't know", the respondents were asked to leave the line blank.

Question (Q12): "What are in your view the most relevant factors influencing the decision of your members whether or not to obtain any privacy/data protection related certification?"³⁶



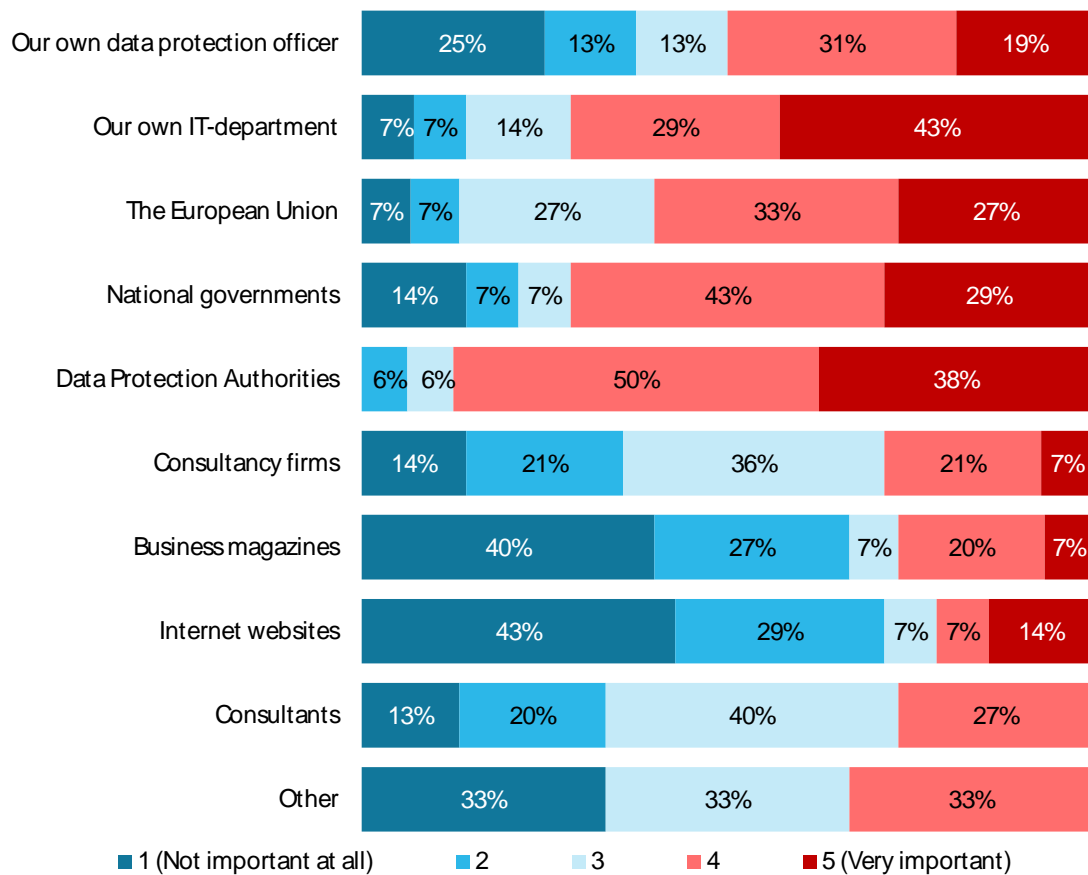
Source: Stakeholder survey
 Note: N=11, 9, 9, 10, 9, 9, 10, 10, 10, 9, 9, 8.
Figure 5.55

³⁶ Multiple answers were possible. Rating from 1 (Not relevant at all) to 5 (Very relevant). If the answer is "don't know", the respondents were asked to leave the line blank.

5.7.3.2. Responses from industry

Question (Q11): "What are/is for your organisation the most important source(s) for obtaining information about the existence of privacy/data protection related certifications?"³⁷

SMEs



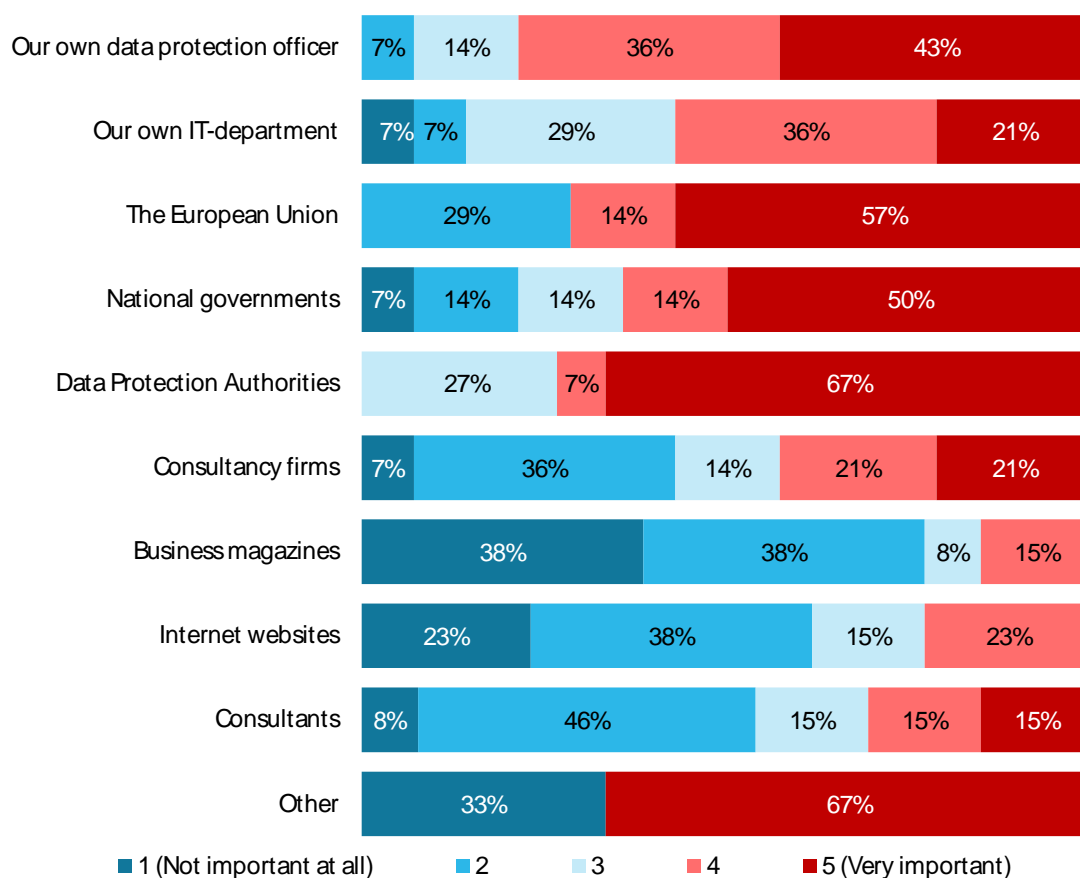
Source: Stakeholder survey

Note: N=16, 14, 15, 14, 16, 14, 15, 14, 15, 3.

Figure 5.56

³⁷ Multiple answers were possible. Rating from 1 (Not important at all) to 5 (Very important). If the answer is "don't know", the respondents were asked to leave the line blank.

Large enterprises



Source: Stakeholder survey

Note: N=14, 14, 14, 14, 15, 14, 13, 13, 13, 3.

Figure 5.57

Question (Q12): "What are the most important factors influencing your decision whether or not to obtain any privacy/data protection related certifications?"³⁸

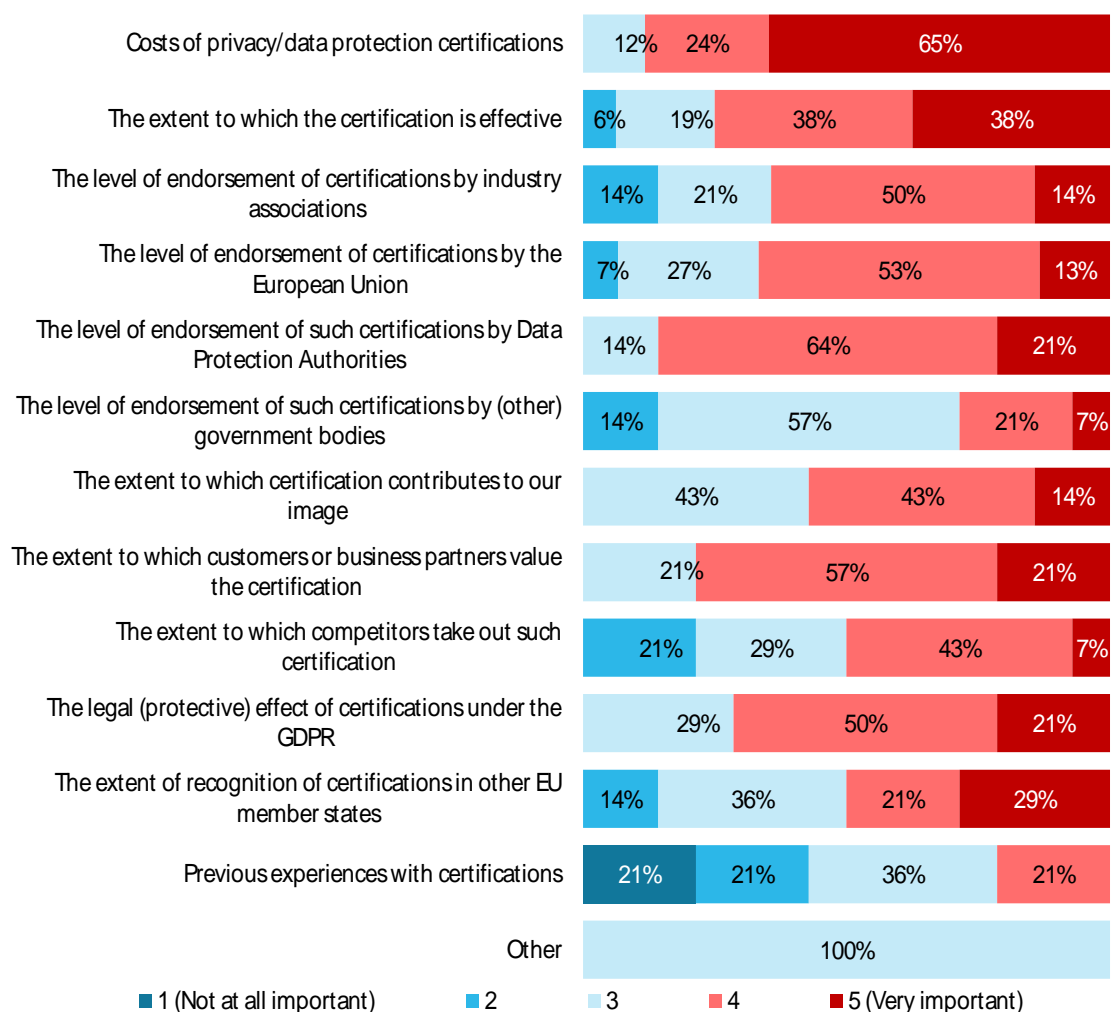
Industry validated the significant importance of all pre-indicated factors, except for:

- the level of endorsement of such certifications by (other) government bodies (moderate importance), and
- previous experiences with certifications (moderate to low importance) for SMEs and
- the level of endorsement of such certifications by (other) government bodies (moderate importance) for large enterprises.

The level of competition on the basis of certification and the extent of recognition of certification in other EU member states was considered moderately relevant in case of SMEs. For large enterprise moderate score was in the field of competition.

³⁸ Multiple answers were possible. Rating from 1 (Not important at all) to 5 (Very important). If the answer is "don't know", the respondents were asked to leave the line blank.

SMEs

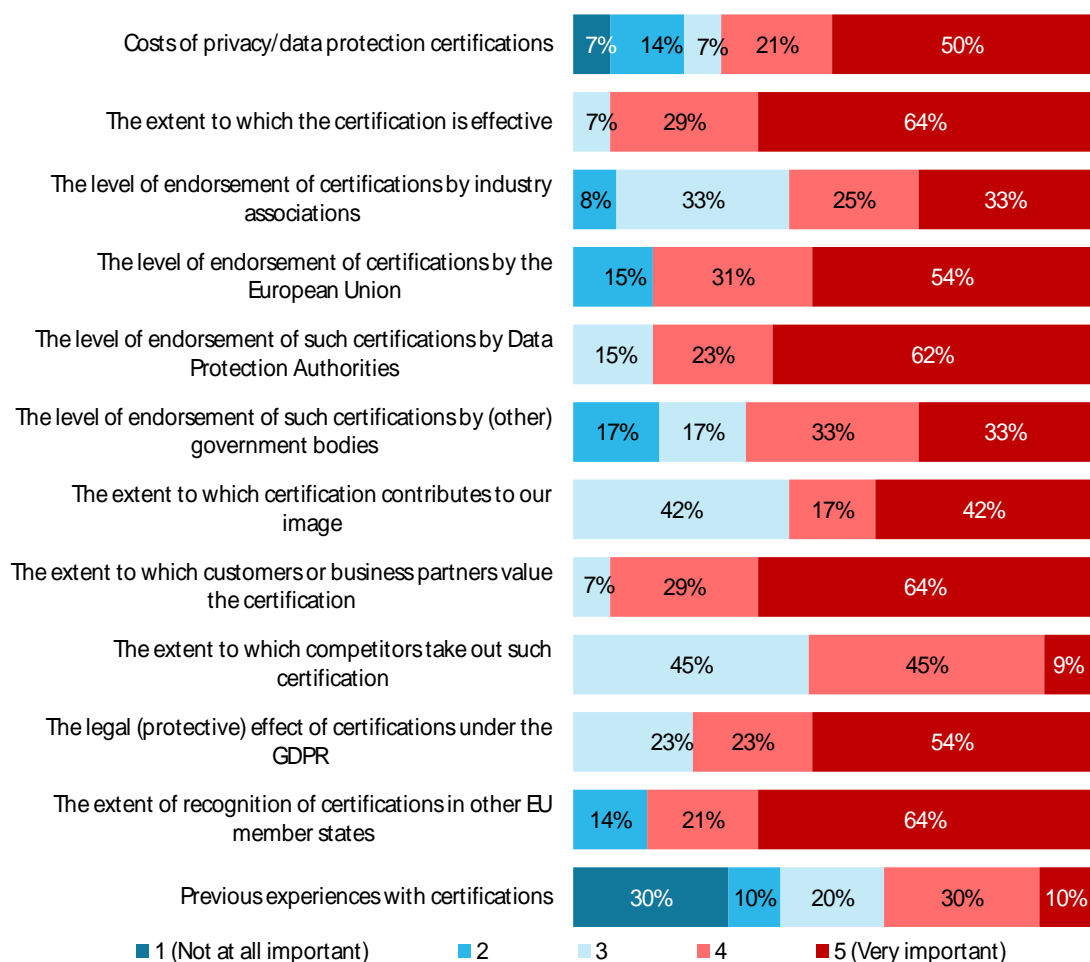


Source: Stakeholder survey

Note: N=17, 16, 14, 15, 14, 14, 14, 14, 14, 14, 14, 14, 1.

Figure 5.58

Large enterprises



Source: Stakeholder survey

Note: N=14, 14, 12, 13, 13, 12, 12, 14, 11, 13, 14, 10.

Figure 5.59

5.7.3.3. Responses from certification bodies

Question (Q8): "What are in your view the most important factors determining the level of uptake of privacy/data protection certifications in the market?"³⁹

Certification bodies considered a whole range of factors to be significant or very significant in deciding about promoting standards, and in particular:

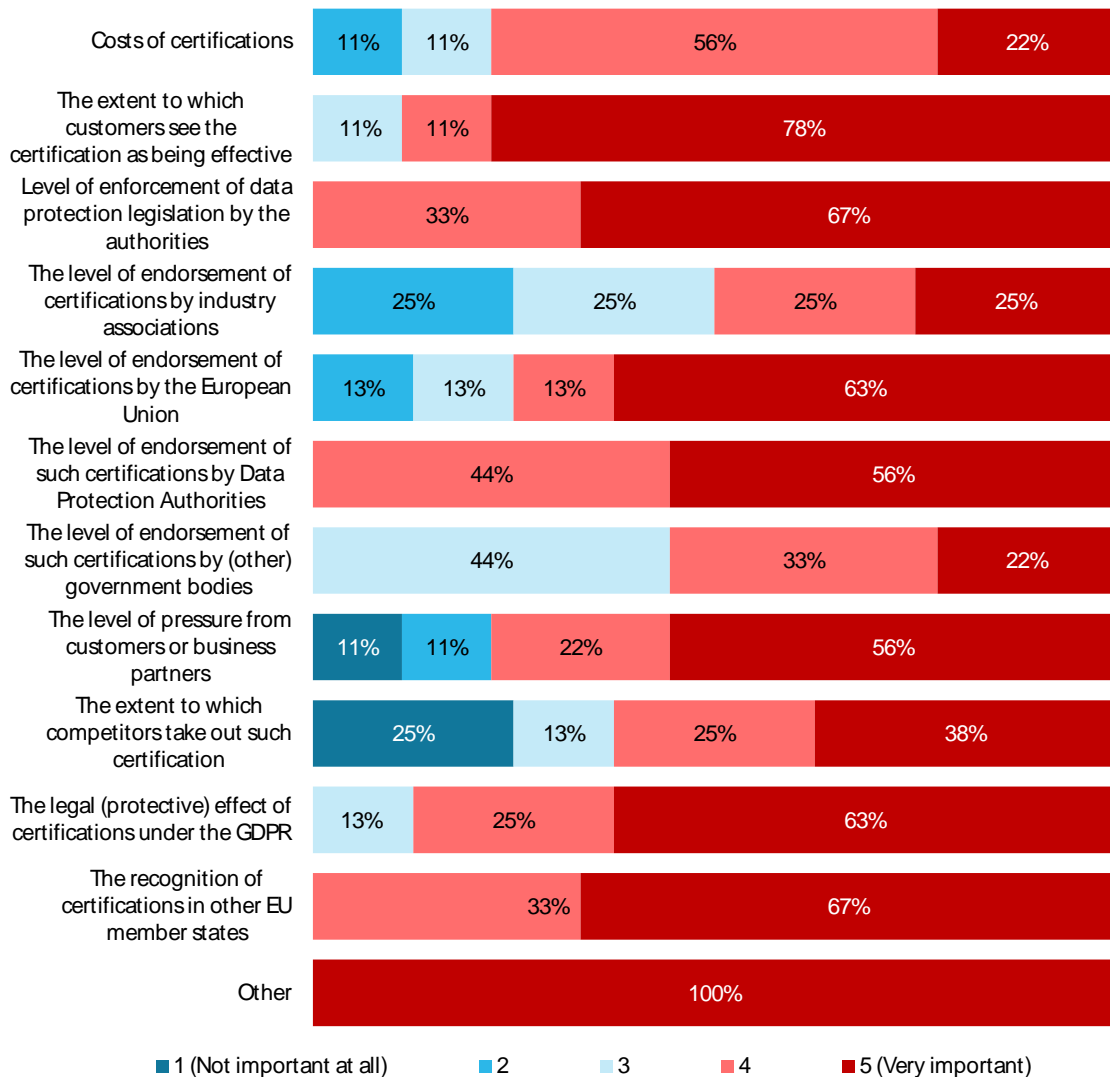
- costs of certifications;
- effectiveness;
- level of enforcement;

³⁹ Multiple answers were possible. Rating from 1 (No uptake at all) to 5 (High level of uptake). If the answer is "don't know", the respondents were asked to leave the line blank.

- endorsement of certifications by authorities;
- pressure from customers or business partners;
- legal (protective) effect;
- recognition in other member states.

In addition, some respondent attached significant value as well to:

- the level of continuous assurance of the certification scheme in view of the dynamic character both cybersecurity and privacy/data protection;
- the level of data protection expertise of certification bodies.



Source: Stakeholder survey
 Note: N=9, 9, 9, 8, 8, 9, 9, 9, 8, 8, 9, 4.
Figure 5.60

Annex 5B Overview of additionally relevant standards

This Annex contains an overview of (clusters of) standards that in addition to the set of standards described in the previous paragraph, could be taken into account by the Commission when deciding about promoting suitable existing technical standards.⁴⁰

In presenting these standards we have categorised them according to the following relevant application phases: design, accreditation, certification and monitoring. For each phase, we give a brief introduction, followed by a list of standards it concerns.

1. Design phase related standards

The following section presents relevant standards for managing the design process of certification schemes.

The review covers the drafting process, the need in terms of content and vocabulary and, the process for approving third party requirements.

The research team identified relevant standards offering drafting guidelines and reference standards defining useful vocabulary and approach to manage data protection issues. The research team did not identify any relevant standards that could help the authorities in the approval process of third party requirements.

Useful standards for design & approval process (Drafting techniques, content, approval process)						
Issuer	Name	Title	Content	Type	Interest	Limits
ISO	ISO/IEC Directives Part 2	Principles and rules for the structure and drafting of ISO and IEC documents	Principles to structure and draft documents intended to become International Standards, Technical Specifications or Publicly Available Specifications.	Drafting	<p>The standard could be useful as drafting guidance to ensure auditability and consistency of standards drafted by the authorities.</p> <p>The authorities could also promote the standard as good practice for third party bodies drafted standards.</p> <p>Accessible at no charge http://www.iec.ch/members_experts/refdocs/i</p>	<p>The guideline has been primarily designed for drafting technical standards</p> <p>The standard does not provide guidance for translating legal provisions into auditable requirements.</p> <p>The experience of DPAs</p>

⁴⁰ This Annex also includes further details about some standards that were already part of the overview presented to respondents in the questionnaire (and as such strictly spoken not 'additionally relevant'). In view of the importance of these standards some further details were nevertheless included in this overview.

Useful standards for design & approval process (Drafting techniques, content, approval process)						
Issuer	Name	Title	Content	Type	Interest	Limits
					ec/isoiecdir-2%7Bed7.0%7Den.pdf	already involved in such a process (CNIL, ULD, Hungarian DPAs) could be helpful here.
ISO/IEC	ISO/IEC Guide 17	Guide for writing standards taking into account the needs of micro, small and medium-sized enterprises	<p>Guidance and recommendations to writers of standards on the needs of micro, small and medium- sized enterprises (SMEs) in order to avoid the exclusion of SMEs from the market and the distortion of fair competition.</p> <p>The standard offers (as defined in its introduction)</p> <p>"Techniques for identifying and assessing provisions in standards that may especially impact SMEs;</p> <p>Ways to reduce negative impacts on SMEs resulting from some provisions in standards;</p> <p>Guidelines for writing SME-friendly standards;</p> <p>A checklist;</p> <p>Information on the impact that new standards can have on micro-enterprises".</p>	Drafting	<p>The standard could be useful as guidance for ensuring that standards designed by the authorities are compatible with SMEs needs and specificities.</p> <p>The authorities could promote the standard as good practice to draft private standards compatible with SMEs needs and specificities.</p>	<p>The guideline has also been designed for drafting of technical standards</p> <p>It does not provide guidance for translating legal provisions into auditable requirements.</p>

Useful standards for design & approval process (Drafting techniques, content, approval process)						
Issuer	Name	Title	Content	Type	Interest	Limits
CEN	Guide 17	Guidance for writing standards taking into account micro, small and medium-sized enterprises (SMEs) needs	<p>This Guide provides orientation, advice and recommendations to standard writers on how to take into account SMEs needs. This document addresses the issues to be considered during the development process of standards. it requires:</p> <p>Provide example, explanations. Do not just refer to other standards but explain their content</p> <p>Use clear language adapted to not expert audience</p> <p>Follow a clear and logical structure</p> <p>Design simple processes</p> <p>Use graphs and charts to be illustrative</p>	Drafting	<p>The standard could also be useful as drafting guidance to ensure the auditability of standards drafted by authorities in direction of SMEs</p> <p>The standard is accessible at no charge https://boss.cen.eu/ref/CENCLC_17.pdf</p>	<p>The guideline has been designed for drafting technical standards</p> <p>The standard does not provide guidance for translating legal provisions into auditable requirements. It should be supplemented by DPA's experience or/and additional guideline</p>
ISO/IEC	ISO/IEC 17007	Conformity assessment -- Guidance for drafting normative documents suitable for use for conformity assessment	<p>Principles and guidance for developing normative documents that contain:</p> <p>specified requirements for objects of conformity assessment to fulfil;</p> <p>specified requirements for conformity assessment systems that can be employed when demonstrating whether an object of conformity assessment fulfils specified requirements.</p>	Drafting	<p>The standard offers guidance</p> <p>To organize the conformity assessment process</p> <p>To draft the normative documents that should be used during the conformity assessment process</p>	

Useful standards for design & approval process (Drafting techniques, content, approval process)						
Issuer	Name	Title	Content	Type	Interest	Limits
ISO/IEC	ISO/IEC 29100	Information technology -- Security techniques -- Privacy framework	<ul style="list-style-type: none"> - Specifies a common privacy terminology according to ISO; - Defines the actors and their roles in processing personally identifiable information (PII); - Describes privacy safeguarding considerations; - Provides references to known privacy principles for information technology. 	Reference	The standard could be useful for realising a mapping between the ISO and GDPR approach and vocabulary in order to evaluate the gap existing between them.	
ISO/IEC	ISO/IEC 25012	Software engineering -- Software Product Quality Requirements and Evaluation (SQuaRE) -- Data quality model	<p>The standard defines a general data quality model for data retained in a structured format within a computer system. It can be used to establish data quality requirements, define data quality measures, or plan and perform data quality evaluations. It could be used, for example,</p> <ul style="list-style-type: none"> - to define and evaluate data quality requirements in data production, acquisition and integration processes, - to identify data quality assurance criteria, also useful for re-engineering, assessment and improvement of data, - to evaluate the compliance of data with legislation and/or requirements. 	Reference	<p>The standard could be helpful to include data protection into data quality requirements.</p> <p>Certain data protection principles (minimization, pseudonymization, anonymization, limited retention) could be envisaged as data quality requirements rather than just regulatory or/and security requirements.</p>	
ISO/IEC	ISO/IEC 25024	Systems and software engineering -- Systems and software	ISO/IEC 25024 defines data quality measures for quantitatively measuring the data quality in terms of characteristics	Reference	The standard could be helpful to design technical monitoring measures of above-	

Useful standards for design & approval process (Drafting techniques, content, approval process)						
Issuer	Name	Title	Content	Type	Interest	Limits
		Quality Requirements and Evaluation (SQuaRE) -- Measurement of data quality	defined in ISO/IEC 25012. It contains the following: - a basic set of data quality measures for each characteristic; - a basic set of target entities to which the quality measures are applied during the data-life-cycle; - an explanation of how to apply data quality measures; - a guidance for organizations defining their own measures for data quality requirements and evaluation.		mentioned principles for demonstrating compliance with Article 24 GDPR	
ISO/IEC	ISO/IEC 27000		ISO/IEC 27000 defines the overview of information security management systems, and terms and definitions commonly used in the ISMS family of standard	Reference	The standard could be helpful to realise a mapping between the ISO and GDPR approach on security matters and evaluate the gap existing between them.	
ISO/IEC	ISO/IEC 27002	Information technology – Security techniques – Code of practice for information security controls	ISO/IEC 27002 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).	Reference	The standard could be helpful to design conformity points of controls dedicated to personal data security "taking into consideration the organization's information security risk environment(s)".	
ISO/IEC	ISO/IEC 27017	Information technology -- Security techniques -- Code of practice for information security controls based on	ISO/IEC 27017 gives guidelines for information security controls applicable to the provision and use of cloud services by providing: - additional implementation	Reference	The standard could be helpful to design conformity points of controls dedicated to personal data security in the cloud "taking	

Useful standards for design & approval process (Drafting techniques, content, approval process)						
Issuer	Name	Title	Content	Type	Interest	Limits
		ISO/IEC 27002 for cloud services	guidance for relevant controls specified in ISO/IEC 27002; - additional controls with implementation guidance that specifically relate to cloud services.		into consideration the organization's information security risk environment(s)".	
ISO/IEC	ISO/IEC 17000	Conformity assessment -- Vocabulary and general principles	ISO/IEC 17000:2004 specifies general terms and definitions relating to conformity assessment, including the accreditation of conformity assessment bodies, and to the use of conformity assessment to facilitate trade. A description of the functional approach to conformity assessment is included as a further aid to understanding among users of conformity assessment, conformity assessment bodies and their accreditation bodies, in both voluntary and regulatory environments.	Reference	The standard could be helpful to design additional data protection requirements included by DPAs into the accreditation process defined in Article 43	
ISO/IEC	ISO/IEC 17011	Conformity assessment -- General requirements for accreditation bodies accrediting conformity assessment bodies	ISO/IEC 17011:2017 specifies requirements for the competence, consistent operation and impartiality of accreditation bodies assessing and accrediting conformity assessment bodies.	Reference	The standard could be helpful to design the requirements to use in the accreditation process when fully operated by DPAs	

2. Conformity assessment related standards

The following section presents useful standards for managing the accreditation process as defined in Article 43 GDPR.

The research team identified a series of standards that could be useful to complete the ISO/IEC 17065 standards already included in the process. It also identified a few standards useful for the accreditation audit process, issuance and renewal. In view of its central role, the research team also included the ISO/IEC 17065 in the overview.

Standards useful for the certification process (Requirements, Audit process, Accreditation issuance, Renewal)						
Issuer	Name	Title	Content	Type	Interest	Limits
ISO	ISO/IEC 17020	Conformity assessment - Requirements for the operation of various types of bodies performing inspection	ISO/IEC 17020 specifies requirements for the competence of bodies performing inspection and for the impartiality and consistency of their inspection activities.	Requirements	The standard could be useful if the authorities plan requiring from approved schemes a certification process including onsite inspections. The standard offers a process for product and service inspections.	
ISO	ISO/IEC 17040	General requirements for peer assessment of conformity assessment bodies and accreditation bodies	ISO/IEC 17040:2005 specifies the general requirements for the peer assessment process to be carried out by agreement groups of accreditation bodies or conformity assessment bodies. It addresses the structure and operation of the agreement group only insofar as they relate to the peer assessment process.	Requirements	The standard could be useful to organize a mutual recognition process between public or private certification bodies located in different Member States.	
ISO	ISO/IEC 17065	Conformity assessment -- Requirements for bodies certifying products, processes and services	ISO/IEC 17065 contains requirements for the competence, consistent operation and impartiality of product, process and service certification	Requirements	The standard is part of the process described in Article 43 GDPR	

			bodies.			
--	--	--	---------	--	--	--

Certification subject-matter related standards

This section presents the standards considered useful for the certification process. Standards that pose requirements to the certification bodies and that help those seeking conformity have been collected and are presented in by-going table.

ISO/IEC 27001 is a generic standard that can be helpful in the operational implementation of dealing with article 32 and art 25 of GDPR. It focuses on the security management systems that need to be in place to support the protection of information. It relates to PII as well but not in an exclusive manner.

ISO/IEC 27018 is a standard focused on cloud solutions. It determines guidelines for the protection of PII in a cloud environment, and thus offers an approach to the implementation of art 32 in a cloud environment.

ISO/IEC 29101 offers guidance to how PII could be dealt with by offering a privacy architecture framework. The framework helps determining the embedding of PII as part of a systems architecture, while taking notice of contextual elements.

ISO/IEC 29151 defines the code of practice in dealing with PII on the basis of a risk and impact assessment. It not only covers technical aspects of information security but includes organisational elements of securing access to and handling of PII as well.

ISO/IEC 29134 sets the criteria for performing a Privacy Impact Assessment that helps determining whether the processing of the PII may yield high risk for the data subjects. It offers elementary guidance to the staging of such a PIA and to the criteria to be used to assess the results of the various stages.

ISO/IEC Guide 23 offers guidance to what information should be included in a third party certificate that wants to demonstrate compliance to existing ISO/IEC standards.

Standards useful for the certification subject matter (Requirements, Audit process, Audit acceptance, Certification issuance)						
Issuer	Name	Title	Content	Type	Interest	Limits
ISO/IEC	ISO/IEC 27001	Information technology -- Security techniques -- Information security management systems -- Requirements	ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization	Requirements	Interesting as generic standard that determines information security requirements. Of relevance for the data protection security measures, as indicated in art 32 and art 25 GDPR	

Standards useful for the certification subject matter (Requirements, Audit process, Audit acceptance, Certification issuance)						
Issuer	Name	Title	Content	Type	Interest	Limits
ISO/IEC	ISO/IEC 27018	Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	<p>ISO/IEC 27018 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.</p> <p>In particular, ISO/IEC 27018:2014 specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services.</p>	Requirements	<p>Relevant standard for certification procedures as it sets standards for securing processing of PII; builds upon 27002; "This International Standard is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which provide information processing services as PII processors via cloud computing under contract to other organizations. The guidelines in this International Standard might also be relevant to organizations acting as PII controllers; however, PII controllers might be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors. This International Standard is not intended to cover such</p>	<p>The standard is applicable to processors and to controllers. However, the last category need to be aware that other standards may impose additional constraints.</p>

Standards useful for the certification subject matter (Requirements, Audit process, Audit acceptance, Certification issuance)						
Issuer	Name	Title	Content	Type	Interest	Limits
					additional obligations."	
ISO/IEC	ISO/IEC 29101	Information technology -- Security techniques -- Privacy architecture framework	ISO/IEC 29101 defines a privacy architecture framework that specifies concerns for information and communication technology (ICT) systems that process personally identifiable information (PII); lists components for the implementation of such systems; and provides architectural views contextualizing these components.	Requirements	Relevant standard for certification procedures; sets standards for a holistic perspective on dealing with PII in ICT systems; could be relevant in dealing with rights of data subjects [art 12 - 21 GDPR] and the way these rights are embedded in design principles.	
ISO/IEC	ISO/IEC 29151	Information technology -- Security techniques -- Code of practice for personally identifiable information protection	ISO/IEC 29151 establishes control objectives, controls and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of personally identifiable information (PII).	Requirements	Relevant standard for certification procedures; set standards for handling PII in relation to organisation of information security; human resource security; asset management; access control; use of cryptography; physical, environmental, operations	

Standards useful for the certification subject matter (Requirements, Audit process, Audit acceptance, Certification issuance)						
Issuer	Name	Title	Content	Type	Interest	Limits
					and communications security; information security incident management.	
ISO/IEC	ISO/IEC 29134	Information technology – Security techniques – Guidelines for privacy impact assessment	ISO/IEC 29134:2017 gives guidelines for - a process on privacy impact assessments, and - a structure and content of a PIA report.	Audit Process	Absolutely relevant for the certification process. Helps the organisation requesting a conformity assessment to show in a systematic manner what privacy risks it perceives and how it intends to mitigate these risks.	
ISO/IEC	ISO/IEC Guide 23	Methods of indicating conformity with standards for third-party certification systems	This Guide lays down methods of indicating conformity with standards and reference thereto in standards.	Certification Issuance	This guide defines the information that should be displayed in third party certificate when referring to a standard.	

3. Monitoring-related standards

The following section presents useful standards for the monitoring of certified bodies. The research covered the renewal process, the non-compliance remediation process and the dispute handling process. The research team only found one relevant standard in this section offering some guidelines to organize the non-conformity remediation process.

Standards useful for monitoring (Renewal, Non-compliance remediation, Dispute handling)						
Issuer	Name	Title	Content	Type	Interest	Limits

ISO	ISO Guide 27	Guidelines for corrective action to be taken by a certification body in the event of misuse of its mark of conformity	The purpose of this Guide is to identify a series of procedures which a national certification body (non-governmental) should consider in deciding how to respond to a reported misuse of its registered mark of conformity (i.e. violation of a contract, inadequate quality control, or error in assessment of conformity) or a situation in which a certified product is subsequently found to be hazardous (i.e. due to inadequate standard, unanticipated end-use of a product or a manufacturing defect).	Reference	The standard could be useful to design and manage the non-conformities remediation process.	
-----	---------------------	---	---	-----------	---	--

Annex 6 Workshop Reports

6.1. Industry views on data protection certification workshop (January 2018)

Aim:

On Tuesday, the 23rd of January 2018, between 12:30 and 17:00, the project organized a **Workshop on data protection certification mechanisms and standards: industry needs and views on the new GDPR certification.**

The context of the workshop was the use of certification mechanisms in demonstrating compliance with the new data protection rules in the GDPR. The workshop was aimed at companies, including small and medium-sized enterprises (SMEs), and industry associations interested in sharing their views regarding the use of technical standards and certifications in relation to data protection. The workshop focused on identifying the relevant factors fostering or hampering the adoption of data protection-related technical standards and certifications, with a focus on specific challenges for SMEs. The event was hosted by TNO and the Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University.

Dissemination:

The workshop was disseminated primarily as a fringe event of the CPDP (Computers, Privacy and Data Protection) conference that started one day after the workshop. Additionally, project members disseminated the event via their personal (professional) social media and extended a limited number of personal invitations, especially to SME representatives. Categories represented among the registrations and participants included both public and private organizations; large and small enterprises; representatives of certification bodies, organizations planning to provide certification services, organizations involved in certification activities or initiatives in other domains (e.g. cloud services and IoT), industry associations, researchers, standardisation organizations. The countries represented were Belgium, France, Germany, Israel, Italy, Luxembourg, Spain, the Netherlands, the UK, the USA, as well as EU representations of trade/industry associations or interest groups (see figure below).



Figure 6.61 Workshop participants

In total, 50 individuals registered for the event, one of whom after the closing of the registrations. Of the 50 registered, 28 participated and 3 others, who were otherwise engaged on the day, indicated that they would want to be kept informed about the results of the workshop and any other follow-up activities.

Agenda

Time	Topic	Speaker/Moderator
12.30 - 13.15	Registration	
13.15 - 13.25	Welcome/Introduction	Isabelle CHATELIER, European Commission, DG JUST Gabriela Bodea, TNO
13.25 - 13.35	Brief presentation of the study	Ronald Leenes, TILT
13.35 - 13.45	Preliminary study results: Lessons learned from existing data protection certifications	Eric Lachaud, TILT
13.45 - 14.45	Breakout working sessions - round 1: - 1a) Technical standards in data protection certification - 1b) Accreditation of certification bodies: GDPR models & additional accreditation requirements	Kees Stuurman, TILT Irene Kamara, TILT
14.45 - 15.00	Preliminary conclusions session 1	Kees Stuurman, TILT Marc van Lieshout, TNO
15.00 - 15.30	Coffee break	
15.30 - 16.30	Breakout working sessions - round 2: - 2a) Certifications for data transfers - 2b) Benefits & barriers to data protection certification	Ronald Leenes, TILT Gabriela Bodea, TNO
16.30 - 16.45	Preliminary conclusions session 2	Ronald Leenes, TILT Marc van Lieshout, TNO
16.45 - 17.15	Wrap-up session & concluding remarks	Ronald Leenes, TILT

The main part of the workshop had four breakout sessions during which participants were invited to share their opinions on the following topics:

- Technical standards in data protection certification
- Accreditation of certification bodies: GDPR models & additional accreditation requirements
- Certification for data transfers and
- Benefits and drawbacks of data protection certification

Session 1a: Technical standards in data protection certification

In this session, the following main issues were discussed:

- Which standards are suitable as a basis for certification?
- Uptake factors and mechanisms: what makes or breaks (compliance with) a standard?
- Adequacy of current body of standards.
- Access to standards. Two aspects were covered: the level of inclusiveness and access to the standards documents.

Session 1b: Accreditation of certification bodies: GDPR models and additional accreditation requirements

In this session, the following main issues were discussed:

- Do you think the DPA should accredit or the NAB?
- What are the advantages and disadvantages of each accreditation model?
- In case the NAB accredits certification bodies, the GDPR requires the DPA to provide "additional requirements". What type of requirements can those be?
- Related to competence of the auditor?
- Related to the specifics scope and subject matter of certification?
- Related to permissibility of scope and subject matter? E.g. no certification of data protection principles (e.g. fairness as such)?
- Are you aware of examples in other fields where there is such a model including the collaboration of a public authority with the NAB?

- When the GDPR refers to the European Data Protection Seal, it assigns a role to the EDBP to draft accreditation criteria?
- How do you see the EDBP being involved in accreditation?
- Is it preferable that the EDBP takes on the Accreditation role or the NABs in the case of the European Data Protection Seal?
- What is the view of SMEs on accreditation models?

Session 2a: Certification for data transfers

In this session, the following main issues were discussed:

- From your perspective, would you be interested in using approved certification as a basis to transfer data to countries/organisations where there is no adequacy decision?
- Under which conditions would SMEs be interested to use certification for data transfers outside the EU?
- What could the advantages of approved certifications as data transfer mechanism over other instruments, such as BCRs or standard contractual clauses be?
- What do you think should be the scope of such certifications?
- Generic accountability certifications covering all the provisions of the GDPR?
- Single-issue certifications covering only a topic e.g. data security (along with data principles)?
- Do you think there should be one type of certification developed specifically for data transfers? Or transfers could be part of the approved certification mechanism? Why?
- What can be the meaning of “binding and enforceable commitments” of art. 46 GDPR?
- What can we learn from other examples such as APEC?

Session 2b: Benefits and barriers to data protection certification

In this session, the following main issues were discussed:

- To what extent will the following factors have a positive/negative influence on the adoption of certification in the area of data protection:
- costs associated with the certification process
 - length of time associated with the certification process and impact on production/time to market
 - impact on innovation within the company
 - availability of multiple types of certification
 - variety of issuing authorities
 - general awareness of data protection regulation
 - availability of specialized personnel
 - expected changes in organizational culture
 - expected translation of certification to value to consumers
 - expected competitive advantage to be derived from the adoption of certification.

Key takeaways:⁴¹

- There is substantial heterogeneity of certification and accreditation models in the GDPR, which might prove counterproductive in having certification approved and valid everywhere. DPAs and NABs do not seem to necessarily intend to collaborate and recognize each other’s competences.

⁴¹ The takeaways are merely a recording of the remarks made by participating individuals and does not necessarily imply consensus on the topics discussed nor necessarily reflect the views of the research team.

- The additional accreditation requirements of Art. 43 GDPR should be interpreted as meaning the expertise of the auditors and the certification body in data protection.
- DPAs performing the accreditation process might lead to higher costs, which will likely make certification impossible for SMEs.
- Liability issues of certification bodies are of concern and might be demotivating for the certification bodies to enter this market of data protection certification. Guidelines are vital for this issue.
- Regarding the scope of certification: if certification is based on standards, which usually contain a control set, then the company will be evaluated against this control set. Doubts on how far up the chain certification may go, especially in certifying compliance. At the same time, it is important to have a harmonized system. Plurality of available standards to which a company can certify its processing will be difficult for companies and certification bodies.
- Compatibility of industry technical standards with the GDPR. Some participants held the view that new standards on privacy management requirements cover the GDPR. Some others explained that even were industry standards are specifically aimed at addressing data protection challenges, their approach is not (always) identical to that of the GDPR. Next to the relevance of standards, the importance of codes of conduct (should be part of schemes) and sharing of good practices should be considered.
- For SMEs, technical standards may be of added value under three conditions:
 1. Proportionality
 2. Standards that account for less formal operation of SMEs
 3. Easily accessible implementation guidelines. Pilot projects ('showcases') are valuable, especially when a supervisory authority monitors these projects (for instance ENISA guidelines for SMEs).
- Introduction of baseline standards with criteria derived from the GDPR, on which sectoral standards can build to account for the particularities of specific sectors, such as health or cloud. A common baseline could also be introduced by the regulator. Complexity should be avoided. At the same time, also the view was expressed that sector-specific certification is not appealing for companies that have cross-sector operations.
- Mutual recognition of issued data protection certifications is a necessary condition for the success of the GDPR certification mechanisms. Difficulties and high costs will occur for companies that operate in more than one EU countries due to the need for re-certification in each of those countries. The different approaches in each MS will need to be re-conciliated. Mutual recognition is easily achievable with the Accreditation Regulation. However, if the EDBP provides accreditation, then the European Data Protection Seal will not need mutual recognition procedures.
- With regard to the certification processes, reciprocity and standard way of conducting the process will be the preferable way forward for certification bodies. In contrast, fragmentation and diversity of certification processes will compromise the effort.
- Effective oversight to avoid fraudulent practices is substantial, including in the case that certification is used for data transfers.
- The APEC CBPR may offer modules for the GDPR data protection certification as means of transfers.
- When certification will be used for data transfers, practical issues will arise such as the location of the certification body (EU or non-EU). The contractual commitments of the data importer need to safeguards data subjects rights, but this can be problematic if the legal system of the third country does not support such cases.
- Clarity and concrete guidance by the regulator with regard to data protection certification is necessary.

6.2. Stakeholder workshop (April 2018)

Aim:

On Wednesday, the 18th of April 2018, between 12:00 and 17:00, the project organized a ***Stakeholder Workshop on data protection certification mechanisms, seals, and marks: share your feedback on our study results***

The workshop provided an opportunity to discuss the main findings of the Interim Report, submitted to the European Commission on the 15th of March 2018 and allowed for sharing views on some key concerns regarding the certification mechanisms under the GDPR. The workshop was targeted at national accreditation bodies, certification bodies, data protection authorities (DPAs) and private entities, including small and medium-sized enterprises (SMEs), interested in presenting their ideas, experiences and expectations with respect to the use of technical standards and other mechanisms per 43(9) GDPR, certifications for the data transfers, as well as certification criteria and certification processes. In addition, the workshop was an occasion to hear the opinions and recommendations on the process of accreditation of certification bodies. The participants received an outline of the main findings before the workshop. The event took place in Brussels and was hosted by the Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University and TNO.

Dissemination:

The invitation to the workshop was disseminated via the European Commission and personal (professional) networks. A number of participants of the previous workshop (held in January 2018) expressed their interest in joining for the second time. Categories represented among the registrations and participants included both public and private organizations; large and small enterprises; representatives of national accreditation bodies, certification bodies, organizations planning to provide certification services, organizations involved in certification activities or initiatives in other domains (e.g. cloud services), industry associations, researchers and standardization organizations. The countries represented were Belgium, Bulgaria, Czech Republic, Denmark, France, Germany, Hungary, Italy, Luxembourg, Norway, Portugal, Romania, Slovenia, Spain, the Netherlands, the UK, the US. The European Institutions (the European Commission and the European Data Protection Supervisor) were represented by 8 participants (see figure below).

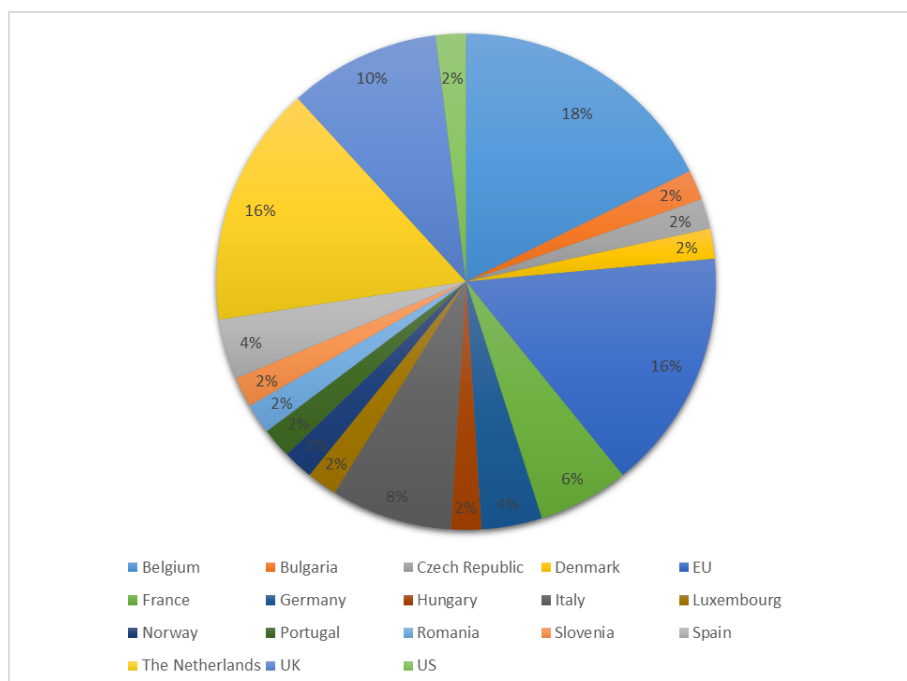


Figure 6.62 Workshop participants

In total, 56 experts registered for the event. Of the 56 registered, 51 participated.

Agenda

Time	Topic	Speaker/Moderator
12.00 – 12.30	Registration & light lunch	
12.30 – 12.45	Welcome/Introduction	Ronald Leenes, TILT, Olivier MicolEuropean Commission, DG JUST
12.45 – 13.30	Presentation of the Study; Overview of findings “Lessons from existing certifications in data protection”	Ronald Leenes, TILT
13.30 – 15.00	Working sessions - round 1: - 1 a) Technical standards and other mechanisms per 43(9) GDPR - 1 b) Accreditation of certification bodies: GDPR models & additional accreditation requirements	1 a) Kees Stuurman, TILT & Eric Lachaud, TILT 1 b) Irene Kamara, TILT & Marc van Lieshout, TNO
15.00 – 15.15	Coffee break	
15.15 – 17.00	Working sessions - round 2: - 2 a) Certifications for data transfers - 2 b) Certification criteria and certification process	2 a) Irene Kamara, TILT & Kees Stuurman, TILT 2 b) Marc van Lieshout, TNO & Ronald Leenes, TILT

The main part of the workshop was divided to four breakout sessions during which participants were presented with the key findings of the study and were invited to share their opinions on the following topics:

- Technical standards and other mechanisms per 43(9) GDPR
- Accreditation of certification bodies: GDPR models & additional accreditation requirements

- Certifications for data transfers
- Certification criteria and certification processes

Key takeaways:⁴²

- The legal significance of certification needs to be clear, especially in relation to codes of conduct.
- Since certification does not warrant compliance with the GDPR, there need to be other incentives for controllers and processors to adopt certification measures, such as positive rewards or direct financial support to SMEs. Certification could be seen as offering competitive advantage to organisations with GDPR certification. At the same time the view that certification in relation to art. 83 GDPR can be an aggravating or mitigating factor was also supported.
- There is a risk of 'market pollution' with cheap non-accredited certificates in parallel with the GDPR certification of art. 42 & 43 GDPR. There needs to be monitoring and measures against non-accredited schemes.
- Certification is just an element to show compliance with one specific thing. GDPR Certification is meant for processing operations, not for products. What is certified is the processing, not the company.
- Certification needs to be precise in addressing the different interpretations of GDPR provisions in different industry sectors.
- Regarding certification criteria: the issue of discretion and professional judgement of the certification auditor was discussed. The criteria should not allow too much space between the assessor and the process assessed. Several DPAs expressed their concern of not being ready to assess certification criteria and schemes. Others explained the steps already taken to establish a reliable certification process based on the ISA 300 standard for auditors in the financial sector.
- Consistency across EU MS means that the EDBP will need to take a more active role in relation to certification.
- The expertise to provide accreditation services depends, among other things, also on the scope of the certification.
- The potential gap that will occur from the different accreditation models following different requirements could be covered by common high-level program requirements to be followed by both NABs and DPAs. Split views on whether the DPAs should be bound by the ISO/IEC 17065. Some participants see the adoption of the ISO/IEC 17065 standard by DPAs as the way to achieve comparable results, some others argued that it might be complex and heavy process. It was also reported however that several SMEs have been accredited in line with the ISO/IEC 17065:2012 standard. Collaboration of experienced auditors that already know how businesses work and can be audited is necessary with privacy experts.
- The issue was raised when the DPA stops working as a certification body, and starts working in its regular/traditional tasks. Concerns from companies about DPA certification auditors using knowledge on controllers or processors for their inspection tasks as DPAs. Codes of conduct and ethics can be established for auditors, as in other fields.

⁴² The takeaways are merely a recording of the remarks made by participating individuals and does not necessarily imply consensus on the topics discussed nor necessarily reflect the views of the research team.

- The issue of non-conformities is an important one. An approach to be followed is the risk-based approach. There also needs to be a sort of prioritisation of requirements – a key provision for the performance of the audit is art. 30, the register of processing operations.
- DPAs can follow how NABs do their work, participate as witnesses (“witness assessment”) in real audits, and work together. In the model where the NABs provide accreditation with additional requirements from the DPAs, one possibility is that the NAB uses DPA staff as auditors, or former staff of DPAs.
- The added value of certification in relation to Standard Contractual Clauses and Binding Corporate is not clear. Also, applicability OF Art. 42(2) GDPR relates to the scope of Art. 3 GDPR. An example of added value is when a data centre in a non-adequate country wishes to start doing business with EU controllers or processors.

There is an issue of supervision of granted certifications in third countries, which also occurs in other fields such as pressure equipment. In that case, an auditor would have to travel to the third country for on-spot audits. The expenses are covered by the certified entity. Another option is local collaborators, with a duty of due diligence of the accredited certification body in the EU.

