Data Protection Certification Mechanisms

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

Final report

Justice and Consumers

Data Protection Certification Mechanisms

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

Final Report

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)

Directorate – General for Justice and Consumers
Unit C.3 Data Protection and Unit C.4 International Data Flows and Protection

Acknowledgements
The authors would like to thank the Dutch Standardisation Institute (NEN) for providing the research team with access to technical standards.
The authors would also like to thank the reviewers from the European Commission, and the participants of the stakeholder workshops organised in January and April 2018 for their valuable feedback.
Special thanks to Leonie Reins, John Waterson, and Ghislaine van den Maagdenberg (TILT).

DISCLAIMER
The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the European Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use, which may be made of the information contained therein.

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

Executive summary

- Certification is part of Chapter IV of the GDPR on Controller and processor obligations and responsibilities. Articles 42 and 43 provide the aims, safeguards, and roles of actors together with overarching principles for the certification and accreditation processes.
- Subject to certification are one or more processing operations by controllers or processors.
- Although the object of certification is explicitly determined in the GDPR, the subject matter may vary. Art. 42 and 43 do not limit the subject matter to one specific topic, potentially thus covering a legal obligation such as data security or even the full spectrum of controller and processor's GDPR obligations.
- Despite the novelty of the GDPR data protection mechanisms, valuable lessons can be learned from the analysis of the existing certifications. Existing certifications already have mechanisms in place: assessment methodologies, contractual arrangements, and auditors that can and should be used in the establishment of the GDPR data protection mechanisms.
- The supervisory authorities will need to use all the guidance and knowledge from other fields and especially technical standards to carry out the assessment of certification criteria in the data protection field. Ultimately, the supervisory authorities will work with the GDPR as main point of reference and framework, which will be the main source of what can and cannot be approved: protected rights and freedoms, the subject matters, and the specific conditions of Art. 42 and 43 GDPR will be the main point of reference for the supervisory authorities.
- The certification process stages are determined in the GDPR and may be complemented by the stages identified in the ISO/IEC 17065 standard. However, beyond generic provisions, one should look at existing certifications to identify best practices. Issues such as dispute resolution management, techniques of monitoring granted certifications, and sanction policies are crucial for developing trustworthy data protection certification mechanisms.
- Several issues arise from the possible adoption of different accreditation models in the Member States relating to recognition of certifications across Member States, harmonisation of auditing techniques, peer evaluation and assessment, function creep.
- The concept of additional requirements in Art. 43(1)(b) GDPR refers to a. Requirements related to the certification body and its auditors' expertise in the field of data protection b. Requirements related to certification body and its auditors' competence in

performing audits, and c. Requirements related to the integrity of the auditors and the certification body.

- There is a structural lack of knowledge in the market as regards the availability of technical standards relevant in the context of data protection. The body of standards relevant in the context of data protection is rapidly evolving, to a large extent triggered by the introduction of the GDPR.
- Relevant stakeholders (industry associations, SMEs and large enterprise) seem to favour European and international standards over national ones. In promoting standardisation in the field of privacy/data protection the EU should maintain its focus on these levels.
- Uptake factors for standards and certifications relate to economic considerations, quality, endorsement by authorities, and trust/reputation.
- Mechanisms to promote and recognise data protection certifications, seals, and marks include the development of technical standards underlying certifications, awareness raising, information and training, and a number of possible negative incentives such as penalties and sanctions.
- Examples of existing certifications for data transfers such as the APEC CBPR provide a good example from an organisational perspective on how to set up oversight mechanisms. However, the actual relationship of the normative criteria and redress mechanisms of such certifications does not fully correspond to the conditions of the data protection certification mechanisms as provided in Art. 42 and 43 GDPR.
- Data protection certification as a data transfers tool by means of appropriate safeguards should include a number of components, namely the scope of certification, information & supporting documentation, the certification criteria, the evaluation methodology, methods and procedures to ensure integrity and consistency of the process, the conditions for the use of the certification seal and mark, the resources necessary to carry out the evaluation, the determination of corrective actions, surveillance procedures, complaint handling mechanisms and appeals, reporting mechanisms, and the content of the contractual certification agreement between the certification body and the certified entity.

Abbreviations

ADR – Alternative Dispute Resolution Mechanism

APEC - Asia-Pacific Economic Cooperation

BCR – Binding Corporate Rules

BDSG - German data protection legislation (Federal Data Protection Act of 30 June 2017)

BSI - British Standards Institution

CBPR - Cross Border Privacy Rules

CCM – Cloud Controls Matrix

CEN - Comité Européen de Normalisation

CENELEC - Comité de Normalisation Electrique

CNIL – French Supervisory Authority

COPPA - US Children's Online Privacy Protection Act

CPEA – Cross-Border Privacy Enforcement Arrangement

DPA – Data Protection Authority

DPD – Data Protection Directive 95/46/EC

EC – European Commission

EDPB – European Data Protection Board

ENISA - European Union Agency for Network and Information Security

ETSI - European Telecommunications Standards Institute

GDPR – General Data Protection Regulation (EU) 679/2016

ICO - Information Commissioner's Office (UK Supervisory Authority)

IEC - International Electrotechnical Commission

IO – international organisation

ISO - International Organization for Standardisation

JIPDEC - Japan Institute for Promotion of Digital Economy and Community

JIS - Japanese Industrial Standards

JOP – Joint Oversight Panel

JTC – Joint Technical Committee

LDSG - Data Protection Act of Schleswig-Holstein

NLF - New Legislative Framework

PECA - Protocol on European Conformity Assessment

PbD – Privacy by Design

PII - Personally Identifiable Information

PMS - Protection Management Systems

SCC – Standard Contractual Clauses

SGOA - Stichting Geschillenoplossing Automatisering

SME - Small and medium-sized enterprise

SOGIS – Senior Officials Group Information Systems Security

TR –Technical Report

ULD - Schleswig-Holstein DPA

WG5 – ISO/IEC JTC 1/SC 27/WG 5

Table of contents

Table of figures

Table of tables

1. Introduction

1.1. Background and aim of the study

The General Data Protection Regulation 679/2016 (GDPR) provides a number of new instruments to help data controllers demonstrate compliance with its provisions.[1] The certification mechanisms introduced in Articles 42 and 43 GDPR are among these new instruments. Running up to May 2018, the Commission and national supervisory authorities within the Article 29 Working Party have been taking actions to facilitate

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, *OJ L 119, 4.5.2016*

the creation of compliance-ready environment from the moment GDPR becomes applicable. Exploring making use of the Commission's empowerments in the area of certification mechanisms via delegated and implementing acts is part of these actions.

The certification mechanisms should facilitate the transition from the ex-ante to the ex-post enforcement approach: the GDPR abolishes most notifications and pre-authorisation requirements on which the present system of data protection is based and moves to a system of accountability and stronger enforcement. The controllers are required to assess the risks arising from the processing operations and to implement appropriate and effective measures in order to show the compliance with the GDPR. In this new environment, certification could offer more transparency to the data subjects and reduce the asymmetry of information commonly unbalancing the relationship with data controllers. It could reward privacy-aware technologies and offer a competitive advantage on the market to these technologies to the extent that those technologies support a specific processing operation being done in compliance with GDPR (e.g. privacy by design of an app). Certification may also provide more certainty to controllers and processors as certification mechanisms can be used to demonstrate compliance with the GDPR. Hence going through a certification procedure may be a useful test for controllers and processors to check their compliance, especially in the initial phase of the new regulatory framework, where controllers and processors will be faced with and will have to adapt to a new legal landscape.

In this context, the Commission is asked to encourage the establishment of certification mechanisms and, to that end, it has been granted the power to adopt both a delegated act specifying the requirements, which must be considered for the certification mechanism, and implementing acts laying down technical standards for certification mechanisms.

In addition, this is one of very few instances in the GDPR where the specific needs of micro, small and medium-sized enterprises are to be taken into account. Working on certification mechanisms could thus allow developing micro- and SME–friendly, cost-efficient compliance tools.

The certification system adopted under the GDPR allows certifications to be issued by supervisory authorities or by certification bodies, without giving preference to any of those bodies and therefore permitting operators to choose between them. Certifications issued by supervisory authorities and by certification bodies of different Member States might be based on different requirements approved by the supervisory authorities. In addition, criteria approved by the European Data

Protection Board (EDPB) may lead to the European Data Protection Seal.

The overall aim of the study is to support the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Articles 42 and 43 GDPR.

More specific the purpose of the assignment is to: i) accompany the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Art. 42 and 43 GDPR and ii) collect all relevant information for the Commission in view of the possible implementation of Art. 43(8) GDPR on the requirements for the data protection certification mechanisms and of Article 43(9) GDPR on the technical standards for certification mechanisms and data protection seals and marks, and for mechanisms to promote and recognise those certification mechanisms, seals and marks.

Objective 1: explain the various terms in Art. 42 and 43 GDPR in view of the terminology in the field of certification (Task 1)

Objective 2: map the data protection certification schemes and related technical standards existing in the Member States and identify existing ones in the main trading partners of the EU; and analyse the selected 15 certification schemes (including one or two international ones, for both substantive and procedural requirements) and related technical standards" (Task 2);

Objective 3: Based on the results of objective two and additional research, provide recommendations for:

- criteria for certifications (Art. 42(5), and requirements for data protection certification mechanism (Art. 43(8) (Task 3);
- additional requirements for the accreditation of certification bodies (Art. 43(3)) (Task 4);
- technical standards for certification and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks (Art. 43(9)) (Task 5);
- identification of possible appropriate safeguards in relation to the transfers of personal data to third countries (Task 6)

1.2. Content and structure of the report

The report is divided in eight main chapters. Chapter 2 analyses the data protection certification mechanisms as in Art. 42 and 43 GDPR. Chapter 3 provides an overview of the current certification landscape in the broader field of privacy, data protection, including information security. The GDPR certification mechanisms are novel, but best practices and lessons can be derived from the multiple certifications

already in operation. The chapter identifies models based on the scope of certification, the normative basis of the certification criteria, and the certification scheme arrangements. Chapters 4 and 5 focus on the main blocks of the GDPR data protection certification mechanisms, namely the certification criteria, the certification process (Chapter 4) and accreditation (Chapter 5). The aims of Chapter 4 are to: a. provide guidance on the potential scopes of the data protection certification mechanisms, b. identify the steps for the assessment of certification criteria by the supervisory authorities, and c. clarify the certification process as determined in the GDPR, building on lessons from existing practices. Chapter 5 discusses mainly Art. 43 GDPR. We elaborate on the actors, legal effect and implications of the accreditation models of the GDPR. Part of Chapter 5 is dedicated to accreditation requirements for certification bodies providing services in line with the GDPR certification mechanisms. The National Accreditation Bodies and the supervisory authorities were consulted via a survey on the issue of accreditation requirements and qualifications of auditors and certification bodies. The results of the survey are presented in both Chapter 5 and in full-length in an Annex of the Report. Furthermore, standards are expected to play a role in the GDPR certification mechanisms. Chapter 6 elaborates on technical standards and Art. 43(9) GDPR. The Chapter identifies technical standards useful for conformity assessment, evaluation and review of processing activities, as well as the scope of certification. The analysis was informed by a stakeholder workshop, addressed to industry, including SMEs, organised by the consortium, and a stakeholder survey circulated to industry, certification, and standardisation bodies. The Chapter also analyses uptake factors for standards and certifications based on the survey results and literature review. Chapter 7 is dedicated to mechanisms to promote and recognise data protection certifications. The analysis builds on the survey results of Chapter 6, and provides a catalogue of mechanisms with potential positive and negative incentives for certification.

One of the key incentives for certification, provided in the GDPR, is data transfers. Thus, Chapters 8 and 9 provide an analysis of data protection certification mechanisms as a legal basis for data transfers and examine different models of data transfers certifications. Chapter 10 concludes the report and provides the main findings to assist the European Commission in relation to its power to adopt delegated and implementing acts.

2. GDPR certification mechanisms under 42&43 GDPR

2.1. Data protection certification mechanisms, seals and marks per Art. 42 &43 GDPR

In this Chapter, we outline the main elements of Articles 42 and 43 GDPR. The elements of those provisions and the interpretation thereof inform the approach we follow throughout the project.[2]

Certification is part of Chapter IV of the GDPR on Controller and processor obligations and responsibilities. Articles 42 and 43 provide the aims, safeguards, and roles of actors together with overarching principles for the certification and accreditation processes.

The GDPR establishes an obligation for the Member States, the data protection authorities, the European Data Protection Board, and the European Commission to encourage the establishment of data protection certification mechanisms.[3] The purpose of the data protection certification mechanisms is to help demonstrate compliance with the GDPR. The focus is rather on the element of demonstration of compliance than compliance as such. There are two practical consequences of this statement: 1) certification of Art. 42 and 43 GDPR should be read in the context of the accountability principle of Art. 5(2) GDPR. 2) Compliance with the GDPR takes place independently of the existence of – and in any case prior to - certification. Compliance with the GDPR is mandatory for the legal actors subject to the scope of the Regulation, whereas certification is a voluntary mechanism for a controller or a processor to demonstrate how they comply with one or more specific provisions. In fact, as explicitly expressed in the Regulation, certification pursuant to Art. 42 does not reduce the responsibility of the controller or processor to comply with the GDPR and any granted certification does not prejudice the tasks and powers of the competent supervisory authorities.[4]

Subject to certification is one or more processing operations by controllers or processors. The object of certification being the processing operation is clearly stated both in Art. 42(1) and Art. 42(6) GDPR. For instance, an organisation acting as data processor may wish to demonstrate that it stores health-related data in a secure way.

[2] The analysis is based on Irene Kamara, Paul De Hert, 'Data protection certification in the EU: Possibilities, Actors and Building Blocks in a reformed landscape' in Rowena Rodrigues and Vagelis Papakonstantinou (eds), *Privacy and Data Protection Seals* (T.M.C. Asser Press 2018); Irene Kamara, Paul De Hert 'Art. 42 & 43 GDPR' in Döhmann Spiecker, Vagelis Papakonstantinou, Gerrit Hornung, Paul De Hert (eds), *Commentary on the European General Data Protection Regulation* (NOMOS, forthcoming).
[3] See Chapter 3.
[4] Art. 42(4) GDPR.

Another example is an organisation acting as data controller that wishes to demonstrate that the collection, use, and erasure of HR data of its employees are performed in line with Art. 24 of the Regulation, which establishes the responsibility of the controller, and all the relevant provisions of the Regulation triggered by Art. 24. When such processing takes place as part of a service – the data processor in the above example is a cloud service provider – or a product – the controller in the above example uses a software tool for erasing data, then certification allows the data subjects to quickly assess the level of data protection of the specific processing operation or chain of operations certified in relation to the service or the product.[5] The European Data Protection Board acknowledges the object of certification being one or more processing operations, but it additionally assigns three core components for consideration in the assessment of a processing operation: 1. Personal data 2. Technical systems (infrastructure used to process personal data) and 3. Processes and procedures related to the processing operations.[6]
Although the object of certification is explicitly determined in the GDPR, the subject matter of certification is not clear. Art. 42 and 43 do not limit the subject matter to one specific topic, potentially thus covering a legal obligation such as data security or even the full spectrum of controller and processor's GDPR obligations.[7]

Certification, beyond the demonstration of compliance function, may also be used to demonstrate appropriate safeguards for transfers of personal data.[8]

Several stages of the certification process are included in Art. 42 GDPR, while some others can be deducted from the powers and tasks of the supervisory authorities. The certification process is conducted by either an accredited certification body or a supervisory authority. The GDPR does not provide any conditions for the supervisory authorities acting as certification bodies. The option is left open for the Member States to identify the model that is best suited for their national market needs. When a certification body is assigned with the power to certify in line with Art. 42 GDPR, the data protection authority has a supervisory role with enhanced powers to withdraw certifications or order the certification body not to issue a certification.
The GDPR also provides the development of a common certification, which works in parallel with the national or cross-national certifications within the EU. The common certification, called the European Data

[5] Recital 100 GDPR.
[6] European Data Protection Board, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679. (adopted 23rd January 2019) p.13.
[7] See analysis in p.57 f.
[8] Art. 42(2) and 46 GDPR.

Protection Seal, requires a set of criteria approved by the European Data Protection Board.

According to Art 43(1) GDPR, Member States must indicate which is the accreditation authority in their jurisdiction. The role of such accreditation bodies may be played by national accreditation bodies or the national data protection authorities, while joint accreditation is also deemed possible. National accreditation bodies are expected to carry out their activities in accordance with EN-ISO/IEC 17065:2012 and with the additional requirements established by the competent supervisory authority.[9] Supervisory authorities will exercise their activities as accreditation bodies on the basis of requirements established by themselves. From the ongoing work of the authorities on this matter, it appears that there is an interest on both sides to ensure consistency of approach: this means DPA accreditation requirements reflecting the requirements of the ISO/IEC 17065. The GDPR provides minimum safeguards for the accreditation process in Art. 43 about the capacity, integrity and independence of the certification body.
Finally, the Commission is empowered to adopt delegated and implementing acts in a series of issues as outlined in the previous section, and as further detailed in this study.

The graph below presents an overview of data protection certification under Art. 42 and 43 GDPR

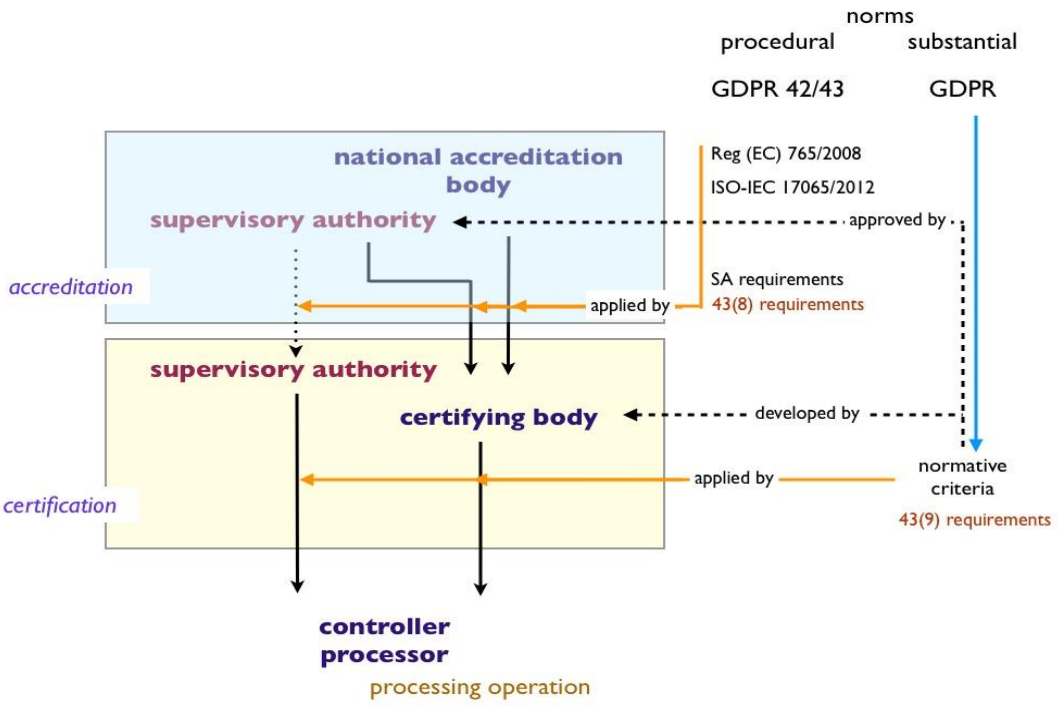


Figure 2-1 Overview of data protection certification under Art. 42 and 43 GDPR

[9] Art. 43(1)(b) GDPR.

2.2. A closer look at distribution of roles in data protection certification mechanisms

The GDPR, as mentioned above, provides powers and duties to supervisory authorities, regulates the activities of private bodies (certification bodies), but also leaves several activities open to *other* actors.[10]

The table below shows the stages of certification, as provided in the GDPR:

Certification stage	Actor	Relevant provision(s)
Application for certification: the applicant submits its processing for review and provides access to necessary information	Data controller or processor	Art. 42(6)
Review of application and file: 'certification procedure'	Accredited certification body or supervisory authority	Art. 42(6)
Issuance and granting (with provision of justification) of certification for a period of three years	Accredited certification body or supervisory authority	Art. 42(5), 43(5), 42(7)
Periodic review of issued certifications OR Surveillance of granted certifications	Supervisory authority OR Accredited certification body	Art. 57(1)(o), 58(1)(c) OR EN ISO/IEC 17065:2012
Renewal of certification	Accredited certification body or supervisory authority	Art. 42(7)
Withdraw certification (with justification)	Accredited certification body or supervisory authority	Art. Art. 42(7), 43(5), 58(2)(h)

Table 2-1 Overview of relevant provisions for certification process per Art. 42/43 GDPR

2.2.1. **Drafting of certification criteria per 42(5) GDPR**

The criteria are the backbone of the certification mechanism.[11] Even though a mandatory approval stage by the national supervisory authority or the European Data Protection Board is established in Art. 42(5) GDPR, the specification of certification criteria is left open to any party. As seen later in the study,[12] the certification criteria may in general be based on a technical standard and/or in the law.[13] In the case of the GDPR data protection certification mechanisms, this means

[10] This section provides an overview of the different activities of the GDPR certification mechanisms with a focus on the actors. For a comprehensive overview of the certification process and accreditation process, see Chapters 4 and 5 of this Report.
[11] Rodrigues et al. (2014).
[12] Chapter 3.3.2 p. 36f.
[13] Criteria based on the law does not mean criteria merely repeating the text of the law. See Chapter 4 on formulation of certification criteria.

that, any entity can submit criteria to a national supervisory authority or the European Data Protection Board (in this case the aim is to establish a common certification across the EU) for approval. Such entities include for example:

- Certification Bodies
- Standardisation bodies, in case of a standard based on one or more provisions of the GDPR
- Industry or industry associations

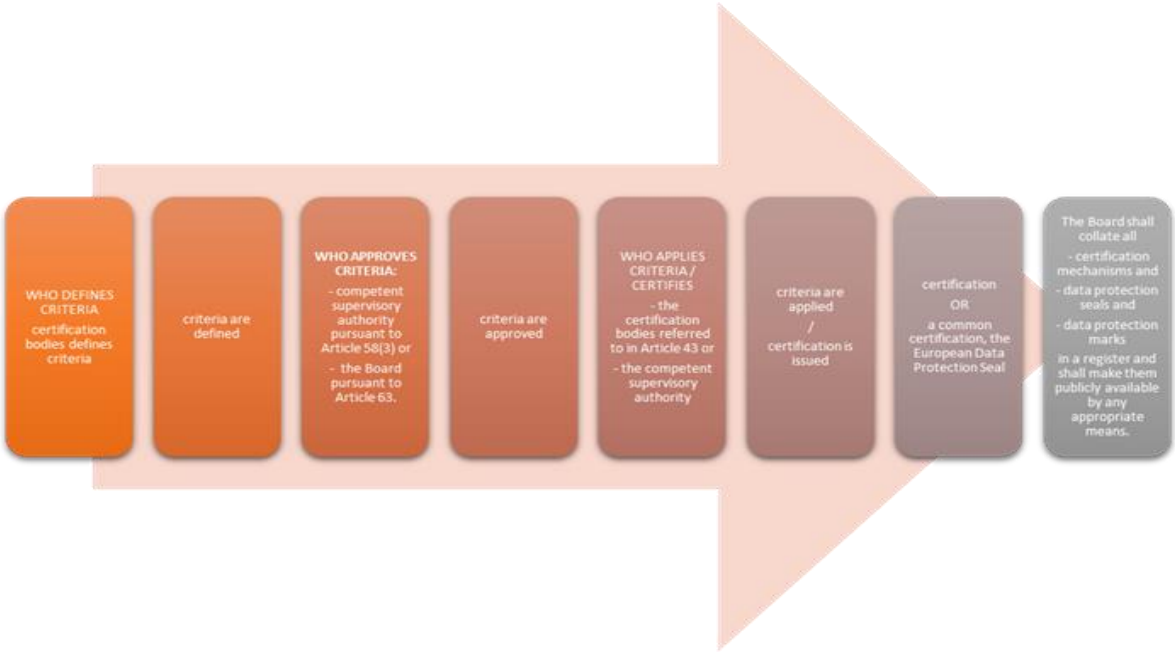


Figure 2-2 Steps in the certification process per Art. 42 GDPR

Another option is that the role is taken up by supervisory authorities drafting and adopting their own criteria, alongside or independently of certification criteria submitted for approval by other actors.[14] An alternative scenario is that the European Commission takes on such a role via the power to issue standardisation requests to the European Standardisation Organisations, as discussed later in this Chapter.

2.2.2. Approval of certification criteria and issuance of certification

Option 1: Criteria are approved by the European Data Protection Board, result is a common certification, the European Data Protection Seal

[14] The issue of proliferation of certifications and a risk to confusion to consumers has been brought up in several fora. Read among others: CIPL, Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms, Discussion Paper, April 2017.

1.a. certification is issued by accredited certification bodies
The competent supervisory authority has a corrective power to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met.

1.b. certification is issued by the competent supervisory authority
The competent supervisory authority has the power to withdraw a certification.

Option 2: Criteria are approved by the competent supervisory authority

2.a. certification is issued by accredited certification bodies
As in Option 1, the competent supervisory authority has the corrective power to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met.

2.b. certification is issued by the competent supervisory authority
The competent supervisory authority has the power to withdraw a certification.

2.2.3. Actors and conditions for issuance, revocation, and withdrawal of certification

The GDPR provides that certification bodies or the supervisory authorities are competent to issue, revoke, or withdraw certifications.
Taking a close look at the certification stages of issuance, revocation, and withdrawal of certification, the GDPR provides a set of conditions, which however are not fully addressing all the necessary steps a certification body or a supervisory authority providing certification needs to undertake.
In practice, as detailed in Chapter 4, the body providing certification needs to:

- Make an assessment on whether the applicant fulfils the certification criteria (evaluation stage)
- Review the necessary information and evaluation results (review stage)
- Make a decision on the application based on the information and report of the evaluation stage (decision stage).

The GDPR does not specify, the above stages prior to the issuance, even though implies them,[15] by referring to:
1) The certification procedure (Art. 42(6)) GDPR
2) The responsibility of the certification body to make a *proper assessment* leading to certification or its withdrawal according to Art. 43(4) GDPR,
3) The ISO/IEC 17065:2012 (which details the above stages) when the certification body is accredited by a National Accreditation Body. In the case the supervisory authority is providing accreditation, although not formally bound by the ISO/IEC 17065:2012 standard, it should be accepted that comparable, if not identical, procedures should be followed.[16]

In addition, when certification bodies are providing certification services, they are bound by an obligation of information towards the supervisory authorities. The information should be reported prior to the issuance (and granting) and renewal of certifications.[17] The reporting should include the reasons for granting or withdrawing a certification.[18]

2.2.4. **Actors involved in the post-certification stage**

The reliability of a certification is linked to whether the granted certification corresponds to the conditions for which it was granted. The post-certification controls, often called 'surveillance' stage, aim at offering this assurance. The GDPR provides that the supervisory authorities have the task (Art. 57(1) (o)) and the investigative power (Art. 58(1) (c)) to carry out periodic reviews of issued certifications. Where there is an accredited certification body involved, the certification body needs to have established procedures for periodic review of data protection certifications, as provided in Art. 43(2)(c) GDPR. The GDPR does not specify details for such periodic reviews, even though the ISO/IEC 17065:2012 standard applied to certification bodies, provides a minimum framework for such reviews.

[15] See also European Data Protection Board, Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) – Annex 1 (version for public consultation, adopted on 4th December 2018).
[16] This view was also supported by the EDPB on its Guidelines on Accreditation 4/2018 (also the Annex 1 to the 4/2018 Guidelines) and raised by several participants of the Stakeholder Workshop organized in the course of the Study in April 2018 (See Annex – Workshop Report).
[17] Art. 43(1) GDPR
[18] Art. 43(5) GDPR

2.3. The Commission implementing powers

The GDPR equips the Commission with the power to adopt acts in relation to data protection certification mechanisms. The Commission has the power to adopt:

- Delegated acts for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms of Art. 42(1) GDPR[19]
- Implementing acts laying down:[20]
    - Technical standards for certification mechanisms and data protection seals, and marks, and
    - Mechanisms to promote and recognise those certification mechanisms, seals, and marks.

The aim of such powers in the context of the data protection certification mechanisms is to ensure a smooth and homogenous implementation of the GDPR certification provisions. As mentioned earlier, Art. 42 and 43 GDPR and the other provisions relating to certification, address several key issues but naturally not all aspects of the data protection certification mechanisms.[21] While the supervisory authorities or the EDPB have several tasks and powers in that regard, there is a role for the European Commission as well. The following sections delve into the specifics of Art. 43(8) and 43(9) GDPR.

2.3.1. **The scope and role of Art. 43(8) GDPR**

The delegated acts of Art. 43(8) aim at specifying requirements to be taken into account for certification mechanisms. The purpose of *specification* of requirements indicates that the delegated acts aim at supplementing the GDPR in terms of data protection certification mechanisms, instead of amending the text thereof.[22] The delegation of power to supplement the GDPR in the context of Art. 43(8) GDPR therefore should be read as a power *to flesh out the act* with regard to data protection certification mechanisms. In addition, two things should be kept in mind, in relation to the delegated acts, on the basis of Art. 290 TFEU:

- The content of the delegated act should be in compliance with the entirety of the GDPR and the adoption of the rules in the

[19] Art. 43(8) GDPR
[20] Art. 43(9) GDPR
[21] See p. 17
[22] On the meaning of the concept "supplementing" in the context of Art. 290 TFEU, see Judgment of Court of Justice of 17 March 2016, C-286/14, EP v Commission (Connecting Europe Facility), ECLI:EU:C:2016:183.

delegated act come within the regulatory framework as defined by the GDPR.[23]

- The delegated act should refer to non-essential elements of the legislation, that the law itself has not specified. Essential are those elements which, "in order to be adopted, require political choices falling within the responsibilities of the EU legislature".[24]

Furthermore, the acts of Art. 290 TFEU need to be of general application, which excludes the possibility to cover individual measures.[25]

The GDPR provides in Article 42(1) that the Commission shall encourage the establishment of data protection certification mechanisms, seals and marks. Data protection certification mechanisms, seals and marks should allow data subjects to quickly assess the level of data protection of one or a set of processing operations (recital 100 GDPR). The GDPR is based on Article 16(2) TFEU which provides for ensuring a high level of protection of personal data and free movement of personal data. In order to ensure legal certainty and free movement of personal data, a high level of harmonisation concerning data protection certification mechanisms is required.

Bearing in mind the above, the term 'requirements' in Art. 43(8) covers all aspects of data protection certification mechanisms in order to lay down a general framework to be further operationalised by the criteria approved by DPAs/EDPB and to ensure that they are easily understandable to data subjects throughout the EU and serve as one of elements to show compliance.

Recital 166 refers to the powers of the Commission to adopt delegated acts "in respect of criteria and requirements for certification mechanisms,".[26] The aim of delegated acts is to supplement the GDPR, namely to specify all requirements for the data protection certification mechanisms, which are not determined in the GDPR.

[23] CJEU, Judgment of the Court 18 March 2014, C-427/2012, European Commission v. European Parliament and the Council of the European Union, ECLI:EU:C:2014:170, paragraph 38.
[24] CJEU, Judgment of the Court 11 May 2017, Case C-44/16 Dyson Ltd v European Commission, ECLI:EU:C:2017:357, paragraph 61, CJEU, Judgment of 5 September 2012, Parliament v Council, C-355/10, EU:C:2012:516, paragraph 65.
[25] Xhaferri, Zamira. "Delegated Acts, Implementing Acts, and Institutional Balance Implications Post-Lisbon." Maastricht Journal of European and Comparative Law 20, no. 4 (2013): 557-575.
[26] Recital 166 GDPR

2.3.2. **The scope and role of Art. 43(9) GDPR**

Independently of the power to adopt delegated acts, as explained in the previous section, the Commission has the power to adopted implementing acts on the basis of Art. 43(9) GDPR. As illustrated in Recital 167 GDPR and further in Art. 291 TFEU, the aim of implementing acts is to 'ensure uniform conditions for implementing' the Regulation. Implementing acts in general are a means to ensure sufficient levels of uniformity of the legislation, in this case the GDPR.[27] The content of implementing acts is not necessarily limited to matters of mere technical character.[28]

The purpose of referring to technical standards for data protection certification mechanisms should be done only to ensure uniformity in the implementation of the GDPR. Examples could be standards which deal with how a certification body deals with non-conformities, or with the use of seals and marks.

The second intent of the provision of Art. 43(9) empowers the Commission to deal with the promotion and recognition of data protection certification mechanisms, seals, and marks. Recognition in this context could mean the formal recognition/ acceptance of certifications cross-border or the (visual) distinction of certifications, seals, and marks from other seals and marks.

The promotion of GDPR certifications should be seen in the context of the general aim of Art. 42(1) GDPR, namely the obligation of the Commission to encourage the establishment of data protection certification mechanisms, seals, and marks. This obligation is established in particular to Union level activities, with an outreach to all MS. Furthermore, it should be noted that Recital 167 provides that the Commission should consider specific measures for SMEs.

2.4. European Commission standardisation requests

Next to the powers explicitly provided to the European Commission in Art. 43(8) and 43(9) GDPR, the Standardisation Regulation (Art. 10) provides that the European Commission may request one or several European Standardisation organisations to draft European standards. Standardisation requests may play the role of a policy tool to support the application of Union legislation and policies.[29] In the field of data protection, the European Commission had already issued a

[27] Jürgen Bast "Is There a Hierarchy of Legislative, Delegated and Implementing Acts?" In Carl Fredrik Bergström and Dominique Ritleng, Rulemaking by the European Commission: The New System for Delegation of Powers, Oxford Scholarship Online, 2016.

[28] Ibid p. 161.

[29] European Commission (2015) Vademecum on European Standardisation in support of Union Legislation and Policies, Part I, Role of the Commission's Standardisation requests to the European Standardisation Organisations, Commission Staff Working Document, SWD 205 final.

standardisation request in the form of a Commission Implementing Decision to the European Standardisation Organisations (ESOs) in 2015.[30] The standardisation request was based on Art. 10 of the Standardisation Regulation 1025/2012, and took into account:[31]

- the Charter of Fundamental Rights (Art. 8(2)), the Data Protection Directive 95/46/EC, and the proposal for a General Data Protection Regulation[32]
- The annual Union work programme for European standardisation which included a point for a privacy management standardisation request.
- The Commission Communication in support of the security Industrial policy of 2012, where the European Commission committed to issue a standardisation request.

Although this example was based on the former Directive 95/46/EC, the Commission may also in the case of the data protection certification mechanisms in the GDPR issue a standardisation request to the ESOs. This could be done for example for the drafting of new technical standards providing criteria that form the basis of the certification mechanism or other matters not explicitly assigned to the supervisory authorities or other entity.[33]

While an explicit legal basis in the legal instrument (GDPR) is not as such required (other than Art. 10 Regulation 1025/2012) for issuing a standardisation request, there are limitations in this activity of the Commission. As provided by the Vademecum on European Standardisation: "In certain cases, the Union legislation itself may limit the subject matter that can be covered by European standards. In particular, standardisation requests cannot be issued in relation to technical rules or technical standards for which the Union legislation provides that they are adopted by a Commission delegated or implementing act. For example, in Articles 15(11), 16(2) and 20(13), the Tobacco Products Directive 2014/40/EU37 provides a specific

[30] Commission Implementing Decision of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy, C(2015) 102 final, 20.1.2015. available http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548 accessed 15 June 2018.

[31] Read further on the standardisation request: Kamara, I., "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'", in European Journal of Law and Technology, Vol 8, No 1, 2017.

[32] COM (2012) 11 final.

[33] See also Chapter 7, p. 127.

empowerment to the Commission to determine the technical standards relevant for its implementation."[34]

2.5. Discussion

Although several aspects of the data protection certification mechanisms such as the object of certification and the actors involved in issuing, revoking and withdrawing certifications, are determined in the GDPR, there are several other aspects such as non-conformities, drafting of certification criteria, assessment methodology, and others, which are either left to the market to be determined or can be further specified by either the Commission exercising its power to adopt delegated or implementing acts, or the supervisory authorities and the EDPB, in case there is a consistency issue to be addressed via the consistency mechanism of Art. 63 GDPR. Several of those issues are highlighted in the study looking at current practices and the boundaries of roles of the different actors.

[34] European Commission (2015) Vademecum on European Standardisation in support of Union Legislation and Policies, Part I, Role of the Commission's Standardisation requests to the European Standardisation Organisations, Commission Staff Working Document, SWD 205 final.

3. Mapping the existing certification landscape

3.1. Introduction and methodological approach

This Chapter aims to identify different models of certification in already existing data protection certifications and derive practices to be considered for the implementation of the data protection mechanisms, established in art. 42 and 43 GDPR. The work for this task builds on already existing research, such as the Study on "EU Privacy seals project Inventory and analysis of privacy certification schemes"[35] and "Security certification practice in the EU - Information Security Management Systems - A case study", taking into account the most recent developments in the field.[36]

As an initial step, we compiled an extended list of existing certification mechanisms, which was after consultation with the European Commission shortened to a list of 15 certifications for the in-depth study. To compile the extended list, the research team used a literature review of previous studies relevant to data protection certification, scientific articles published in the field,[37] Internet search[38] and other communications means.

Although the focus of the study is primarily on the EU, we did not limit its search only to EU Member States. This methodological choice, apart from being mandated in the Tender for this study, is justified by the novelty of the certification model introduced in Art. 42 and 43 GDPR, which in turn seeks to learn from models and schemes that are already

[35] Rowena Rodrigues, David Barnard-Wills, David Wright, Paul De Hert, Vagelis Papakonstantinou,'EU Privacy seals project. Inventory and analysis of privacy certification schemes' (Publications Office of the European Union 2013)
http://www.vub.ac.be/LSTS/pub/Dehert/481.pdf> accessed 12 March 2018.

[36] ENISA, 'Security certification practice in the EU - Information Security Management Systems - A case study' (2013) <https://www.enisa.europa.eu/publications/security-certification-practice-in-the-eu-information-security-management-systems-a-case-study> accessed 12 March 2018.

[37] See among others: Trilateral Research, Vrije Universiteit Brussel, First report of the Study: Inventory and Analysis of Privacy Certification Schemes, October 2013. Final Report Study Deliverable 2.4: Comparison with other EU certification schemes, 2013. Final Report Study Deliverable 3.4: Challenges and Possible Scope of an EU Privacy Seal Scheme, 2014. Final Report Study Deliverable 4.4: Proposals and evaluation of policy options, 2014, Trilateral Research, Certification Schemes for Cloud Computing, 2014; ENISA, 'Security certification practice in the EU (…)' (ibid); Irene Kamara, Paul De Hert , 'Data protection certification in the EU' (n 2); Eric Lachaud, 'The General Data Protection Regulation Contributes to the Rise of Certification as Regulatory Instrument' [2017] Computer Law & Security Review; Eric Lachaud, 'Why the certification process defined in the General Data Protection Regulation cannot be successful' (2016) 32(6) Computer Law & Security Review 814; Eric Lachaud, 'Could the CE Marking Be Relevant to Enforce Privacy by Design in the Internet of Things?' in Serge Gutwirth, Ronald Leenes, and Paul De Hert (eds) *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer Netherlands 2016); Eric Lachaud, 'Should the DPO Be Certified?' (2014) 4 International Data Privacy Law 189. In addition, the research of Eric Lachaud for his PhD thesis was taken into account, as it included a similar overview of existing certifications.

[38] The literature study further has provided titles of certifications, entities in the data protection certification realm, websites of known certifications and a set of search terms to start a web search and subsequent 'snowballing'. On the basis of this material we have explored the web through direct links, link traversal and web-search.

operational. The research team explored non-EU certification models with a focus mainly on the organisation of certification, and to a lesser extent to the substantial (normative) requirements assessed in the certification, due to the different normative basis (legislation or standards) of non-EU based schemes. The schemes identified in this stage of the study are relevant to data protection and privacy, but could have a broader scope than meant in Art 42 and 43 GDPR, such as for instance to include information security and management. Since the aim of this stage is to map the landscape of existing schemes, such schemes are included in the list. In the quick-scan the aim was to be inclusive in order not to miss potentially relevant schemes.

The results of the quick scan have been recorded in a table capturing some basic information about the various certification schemes, most notably:

Active	Aim to ensure the scheme is still active during the scan
Certification name	Displayed in English and in native language
Owner of the certification scheme	Legal owner of the scheme
Country of origin	Main establishment of the legal owner of the scheme
Subject	Product, Processes, Management systems
Sector	E-Commerce, Health, Smart Card, cloud and others
GDPR topic relevance	Which provision of the GDPR the scheme can help to comply with
Special Features	Does the scheme offer some special features? e.g. Mandatory certification, self-certification, children privacy certification
Origin	Public, Private, NGO
Coverage	International, National
Legal Basis	Normative basis (data protection law, standard, code of conduct, other)
Contact Person, contact email, contact phone	Contact information

Website	Internet website on which additional information can be found

Table 3-1 Overview of main attributes of certification schemes

The quick-scan has revealed an extended list of certifications[39] in the privacy and data protection realm. The amount of information that can be obtained about these schemes through their websites, is however limited. In addition, compiling the information into a format that allows comparison and drawing lessons has been cumbersome because different certification schemes use different terminology, information is scattered over many (web)pages, and language barriers. The extended list compiled in the first stage contains similar services – there clearly is a saturation point after which adding more services does not lead to new information.

The quick-scan has resulted in identifying certifications covering a diverse range of certification schemes.[40] The schemes differ on attributes such as public/private initiatives, scope in terms of normative criteria (e.g. Data Protection Directive, COPPA, privacy by design), geographical scope (e.g. APEC CBPR, Japan), subject e.g. process: international data flows, product: e-voting machines, management system: Health Personal Data Storage (Agrément des hébergeurs de santé de données personnelles).

[39] See Annex 2 (separate document).
[40] The research for the quick-scan is updated up to 15th September 2017 and concerns certifications that were already operational by that date. The list represents the best effort to collect all relevant certifications, but several might have been missed from the list.

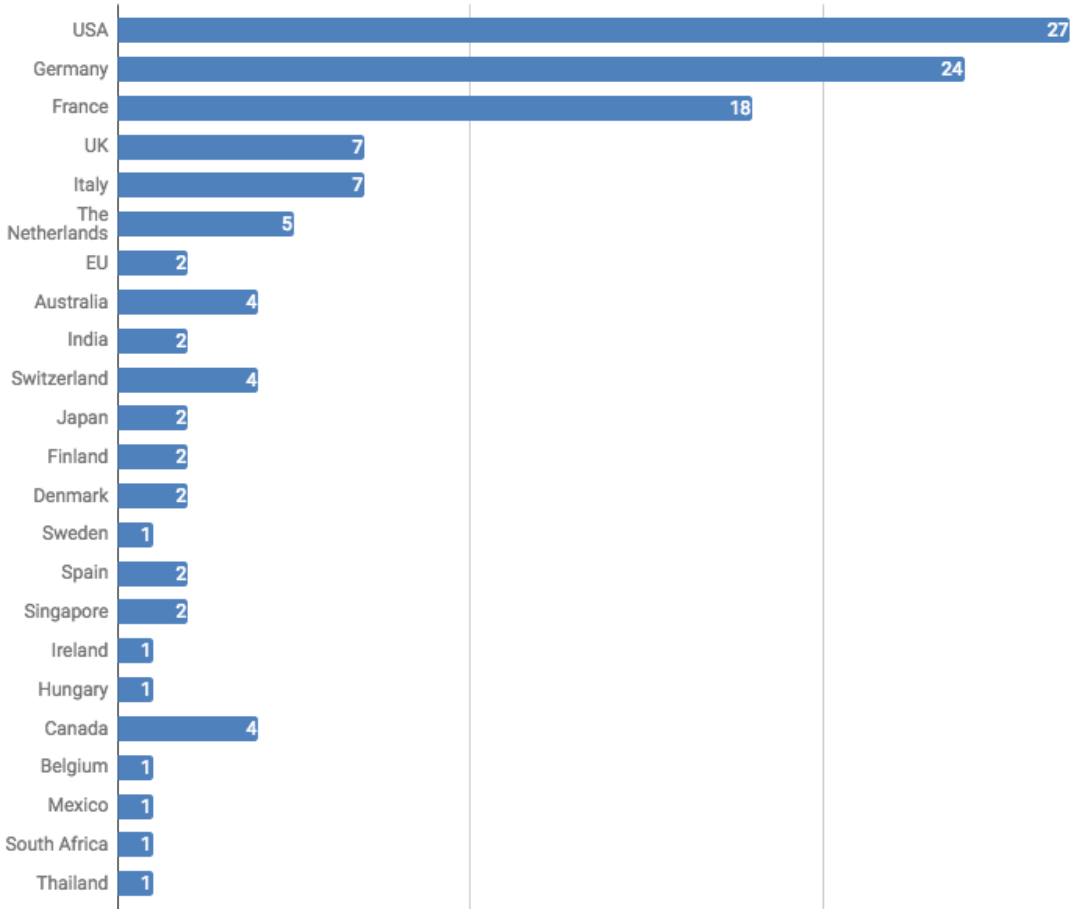


Figure 3-1 Classification of identified relevant certifications per country

On the basis of the outcomes of the quick-scan phase, we selected cases to be further explored. The selection of cases aimed at providing a broad coverage of relevant aspects to explore in order to find common grounds and best practices for data protection certification. Furthermore, the selection incorporates cases within the EU and outside of the EU (e.g. the Japanese Privacy Mark). The resulting shortlist of 15 case studies adopted for further exploration has been agreed upon with the European Commission.

The selection criteria were derived from the GDPR, existing studies regarding certification in the data protection domain and findings from the extended list that was discussed in the previous section. The selection criteria are grouped in six clusters.

A. Art. 42, 43 GDPR criteria

The research team identified a list of straightforward requirements based on Articles 42 and 43 of the GDPR, which were then used as

criteria for the selection of the schemes. The rationale is that the certification schemes which are to be proposed for a detailed study need to be relevant to the scope of Article 42 GDPR. The identified criteria are:

1. Certification concerns personal data/PII/privacy[41] in a broad sense
2. Voluntary nature of the certification
3. Third party conformity assessment (no self-certification)
4. Certification of processing operation.[42]

The jurisdiction and applicability of the EU legislation were not included in this set of criteria, mainly because of the fact that the geographical coverage of a scheme can potentially change. For instance, a US scheme owner may decide to expand the coverage of its seal to EU level by finding a certification body located in the EU.
In addition, even though accreditation is an important element of the GDPR data protection certification mechanisms, accreditation was not used as criterion to exclude certifications from the study. This decision is justified from both the fact that the Art. 43 Accreditation models have not been fully developed and launched during the course of the research for this study[43] and also because the lack of accreditation by a certification body is an element that can be easily changed, e.g. a non-accredited certification body currently operating a certification based on ISO/IEC 27001, later decides to go through the accreditation process of Art. 43 GDPR, when such procedures are established.

B. Maturity of certifications and adoption ("success")

It is important that the study analyses certifications of different levels of maturity. The focus is on mature schemes that are already operational for several years.

1. Maturity

C. Focus/topics of certifications

This criterion was derived by the wording of the GDPR. The GDPR refers to certification in Articles: 24 (controller), 25 (data protection by design & default), 28 (processor), 32 (data security), and 46 (data transfers). The identified certifications revolve around the topics of data/information security, certification as transfer mechanism, data protection by design. There are also several schemes that are not

[41] We opted not to limit the research to certifications strictly related to "personal data", due to the diversity of terminology used in practice. For instance, the ISO/IEC standards use the term PII, based on the ISO/IEC 29000 standard.
[42] As explained in p. 31 we opted to also include a number of certifications with different object, which offer lessons mainly in terms of structure and organisation.
[43] This section is updated until 15th September 2017.

limited to a specific topic, but are generic, in the sense that they aim to cover compliance dealing with more than one topics. We derived the following topics as selection criteria:

2. Comprehensive
3. Data Protection by design and by default
4. Data Security
5. Data Transfers

Additionally, the GDPR includes provisions that lend themselves for certification, such as data portability and children's consent.[44] The handling of (parental) consent for services aimed at children is a topic of certification encountered in the US and hence this case may also provide lessons for the EU. We have thus taken 'new topics' as a criterion.

6. New topics (e.g. data portability and children's consent)

D. Territoriality of regulatory basis

The focus of the study is EU regulation. There are also lessons to be learned from certification schemes in other jurisdictions, both national and regional. Thus, this topic is relevant for the selection of cases. The topic can be divided into:

7. based on EU regulation
8. based on non-EU national regulation
9. based on non-EU regional regulation

E. Concerned entity – data controller or processor

Following the wording of Art. 42(1) GDPR, data controller and data processors are the potential applicants for certification. Certifications may be addressed to either of the two entities, or to neither specifically. The research team applied the following criteria in relation to the entity that can be certified

10. Data Controller
11. Data Processor
12. Data Controller/processor

F. Sector-specificity

Another criterion is the nature of the certification as sector-neutral or sector-specific. This criterion aims to pay attention to certifications that are targeting specific sectors, such as cloud computing. Even though the GDPR is a general regulation, the steps towards compliance for controllers in different sectors are likely to differ due to, for instance, the different number of actors and activity of said actors in cloud

[44]The provisions for children seem to be inspired by the US COPPA regulation. Milda Macenaite and Eleni Kosta, 'Consent for processing children's personal data in the EU: Following the US footsteps?' (2017) 26(2) Information & Communications Technology Law, p. 146.

computing than in e-Health. In addition, the study of sector-specific schemes is also mentioned in the Tender for this study.

13. Sector-neutral
14. Sector-specific

The set of 14 criteria provides for a multifaceted range of factors that makes systematic exploration of the configurations possible. For example, a certification may be sector-specific, aimed at processors, and cover data transfer. Another may cover the same sector and concern data transfer, but target controllers. Not all criteria are of the same nature. Some criteria function as entry conditions, while others aim at generating diversity and refining or extending the most important selections. The selection procedure was as follows.

- The first set of criteria (A) served as guiding principles. Priority, for the inclusion in the in-depth study, was given to certifications that fulfil the four aspects. Nevertheless, the concept of data protection certification mechanism as introduced under Articles 42 and 43 GDPR is a novel approach in the field of data protection, which is not (yet) reflected in many certifications existing in the market. For instance, many existing certifications focus on products and systems, which is not in the scope of Article 42 GDPR. Useful lessons can be learned from such certifications, to the extent that they relate to data processing in the context of a product or a system. In addition, there are only a few certifications that are based on the GDPR. An example is certification based on the BS 10002 standard. The research team decided to propose to the European Commission to study a small in-depth selection of such certifications, as long as they are in line with the other selection criteria that follow and may bring an added value to the study.
- Maturity (cluster B) serves both as an entry condition for stage two – only certification schemes that have granted 'some' certifications are eligible – and in case of identification of multiple such schemes available, the most mature is maintained in the final selection.
- With respect to Focus (cluster C) the aim was to cover a broad range of topics; the various foci/scopes may represent different procedures and substantive normative criteria.
- Territoriality (cluster D) is used to determine the order of selecting cases. The focus of the study is on certifications based on EU data protection legislation. The aim, therefore is to have good coverage of these certifications in the selected cases for in-depth study. EU certifications are interesting both in terms of the normative criteria (subject-matter) and their organisational

model. The non-EU ones are relevant only for the organisational part, since their normative basis is different.

- Sector-specificity (cluster F) is a complementary criterion. Most identified certifications are sector-neutral. To explore the potential differences between sector-neutral and sector-specific certifications, we have included two certifications for which both exist.

	Comprehensive	Data protection by design and by default	Security	Transfers	New topics
EU					
non-EU regional					
non-EU National					

Table 3-2 Selection matrix based on the GDPR wording

On the basis of the ISO/IEC standards on certification (e.g., EN-ISO/IEC 17065:2012), existing literature and studies, documents already compiled from the certification bodies' websites and our analysis, we have developed a template to record the relevant data about the cases to be studied.

This template[45] includes aspects such as the owner of the certification mechanism, the operator of the certification mechanism operator (if applicable), legal foundation, scope, normative criteria, types of conformity assessment, methods to assess the controller, number of certificates delivered, cost, targeted customers (e.g. SMEs), and others.

The team has pre-populated the fact-sheet for each case on the basis of publicly available material. Next, we have circulated the pre-populated fact-sheet among the relevant stakeholders and arranged telephone interviews and received feedback on the accuracy and completeness of the information in the factsheet. Once the fact-sheets were completed to the maximum extent possible, we have analysed the 15 selected certifications.

3.2. The analysed certifications

[45] See Annex 3 (separate document).

On the basis of the criteria outlined in the previous section, the following certification schemes have been selected for further elaboration[46]:

1. BS 10012 Personal Information Management System Certification (UK)
2. TÜV Italia ISO/IEC 27001 Information Security Management Certification
3. BSI ISO/IEC 27018 Information technology. Security techniques. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors Certification (UK)
4. Certificazione ISDP 10003:2015 Data protection (IT)
5. Datenschutzaudit beim ULD (DE)
6. E-privacy app (DE)
7. EuroPrise - the European Privacy Seal (DE)
8. IkeepSafe Coppa Safe Harbor (US)
9. Label CNIL digital safe boxes (FR)
10. Health Personal Data Storage Agreement (FR)
11. Myobi Privacy Seal (NL)
12. Norea Privacy-Audit-Proof (NL)
13. PrivacyMark System (JP)
14. Privacy by Design Certification Ryerson (CA)
15. TrustArc APEC CBPR certification (US)

A brief description of the 15 schemes is as follows:

BS 10012:2017 Personal Information Management System (UK) is a certification based on the UK technical standard BS 10012:2009 Data Protection — Specification for a Personal Information Management System: an Implementation Methodology. It aims to improve compliance with the data protection legislation and recognised best practice and contains requirements representing the data protection principles, including a special package customised for SMEs. This certification focuses on information management processes.[47]

[46] Initially, the Spanish scheme Appytest was included in the short list for the in-depth study. However, after contacting the certification scheme owner it was communicated to the research team that that Appytest was no longer active, despite the information on the website (http://www.appytest.com/en/certificacions-3/novetat-certificacio-de-privacitat). In consultation with the EC, Appytest has been replaced by an active scheme similarly operating in mobile Apps certification, the German E-privacy app (number 6 in the list above). The selection of schemes for this list ended in October 2017 and the information on which the analysis is based is up-to-date until that date.

[47] The British Standards Institution, 'Personal Information Management',(Bsigroup) <https://www.bsigroup.com/en-GB/BS-10012-Personal-information-management/> accessed 13 March 2018.

TUV Italia ISO/IEC 27001 (IT) is a one of the numerous certification schemes based on the widely adopted standard for Information Security Management Systems issued by the International Organization for Standardization. It provides a systematic approach to managing and protecting computers, data and data centres and as such relates to data protection.

BSI ISO/IEC 27018:2014 Certification (UK) is a certification for the Cloud aimed at public cloud service providers acting as PII processors. It is based on the ISO/IEC 27018 Information technology - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. It builds on the general controls described in ISO/IEC 27002 and is appropriate for any organization that processes personal data. Additionally, it is used in conjunction with ISO/IEC 27001 (i.e. the user will need certification to ISO/IEC 27001 to be able to get certification to BSI ISO/IEC 27018.)

Certificazione ISDP 10003:2015 Data protection (IT) is a scheme consistent with ISO/IEC 17065:2012 and based on standard ISDP 10003:2015. The ISDP standard specifies requirements relating to the data protection principles in the data protection regulation. It also details security requirements and controls so that data meets the accuracy, timeliness, consistency, completeness, credibility and updating levels required by current personal data protection regulations, with particular attention to the principles of data quality and data security. The scheme is owned by INVEO. Certification is conducted by external certification bodies.[48]

Datenschutzaudit beim ULD (DE) is a certification aimed at public bodies. It certifies against the Data Protection Act of Schleswig-Holstein (LDSG). The certification assesses entire data processing operations, separate parts thereof, and individual data processing procedures. Approximately 15 public bodies have been certified since 2007 according to ULD's public register. The audit is done by ULD (the Schleswig-Holstein DPA).[49]

EuroPrise (DE) is a pan-European certification scheme developed for IT products and IT-based services, from 2007-2009, to certify against EU level data protection law (then the DPD). Since Jan 2017 the scheme covers the GDPR. The certification was co-developed by ULD and

[48] InVeo, 'ISDP 10003:2015 Data Protection Certification' (InVeo Accredited Certification Body) <https://www.in-veo.com/en/certification/isdp-10003-2015-data-protection> accessed 13 March 2018.
[49] ULD, ' Datenschutzaudit beim ULD' (ULD, 2018) <https://www.datenschutzzentrum.de/audit/ > accessed 13 March 2018.

currently run by a private entity (EuroPrise GmbH). Approximately 35 certificates were awarded from 2008 until October 2017.[50]

E-Privacy App (DE)[51] is a certification scheme dedicated to dealing with mobile Apps in assessing compliance with the GDPR, the IAB Europe Online Behavioural Advertising Framework (governing self-regulation by the digital advertising industry) and the German data protection legislation. The E-Privacy App offers two certification maturity levels depending the sensitivity of the data processed in the apps.

iKeepSafe COPPA Safe Harbor (US)[52] is a topic-specific certification that has been on the market for several years. The scheme aims to ensure that practices surrounding the collection, use, maintenance and disclosure of personal information from children under the age of 13 are consistent with principles and requirements of the US Children's Online Privacy Protection Act (COPPA). It has certified around 10 apps, cloud solutions and web services according to their public register. The scheme is owned by a non-profit organisation.[53]

Label CNIL digital safe boxes (FR) is a certification mandated by Article 11(3°) and (3°)(c) of the amended French Data Protection Act of 6 January 1978 and based on CNIL's Standard.[54] The CNIL certifies the compliance of digital vaults which are, according to the CNIL, "storage space(s) in that the data that is stored there (documents and some metadata) is only accessible to the holder of the vault" with the rules of the French data protection law translated into cumulative requirements.

MYOBI (NL) is a certification scheme aimed at certifying the compliance of products and services in relation to the Dutch data protection law (Wet bescherming persoonsgegevens), the Dutch implementation of the Data Protection Directive. The assessment is done by auditors who have attended training at the Duthler Academy. The scheme rates the level of compliance of the organisation in 'maturity' levels. The scheme has certified around 60 organisations according to the owners' public register.[55]

---

[50] EuroPrise, 'European Privacy Seal' (European Privacy Seal for IT Products and IT-Based Services) <https://www.european-privacy-seal.eu/EPS-en/Home > accessed 13 March 2018.
[51] E- Privacy seal<https://www.eprivacy.eu/en/privacy-seals/eprivacyseal/>accessed 13 March 2018.
[52] It should be noted that the certification scheme examined is third party certification and it is not related to the former U.S.-EU Safe Harbour Framework. 'Safe Harbor' here refers to its common language use 'any place or situation that offers refuge or protection'.
[53] ikeepsafe, 'About the iKeepSafe COPPA Safe Harbor Certification' (COPPA Safe Harbor) <https://ikeepsafe.org/certification/coppa/> accessed 13 March 2018.
[54] See CNIL, 'Data Protection' (CNIL) <https://www.cnil.fr/fr/labels> accessed 13 March 2018.
[55] MYOBI, 'Controle krijgen over uw eigen bedrijfsinformatie' (MYOBI, 2018) <https://www.myobi.eu/ > accessed 13 March 2018.

Norea Privacy-Audit-Proof (NL) is a national certification based on compliance with the Dutch implementation of the Data Protection Directive 95/46/EC.[56] The scheme is owned by the association of IT-Auditors in the Netherlands. Assessment of data processing operations is done by registered auditors. There are few certifications awarded through this scheme according to NOREA's public register, but those that have been awarded concern very large systems (e.g., the Dutch vehicle license registration system).[57]

Privacy by Design Certification Ryerson (CA) provided by Ryerson University and Deloitte, it certifies compliance with a set of criteria based on the former Ontario Privacy Commissioner Ann Cavoukian's 7 Privacy by Design principles. The scheme assesses IT systems, accountable business practices, and networked infrastructure. The third-party assessment is done by Deloitte. It has awarded 7 certificates in 2017 according to Ryerson's public register. The scheme is owned by Ryerson University.[58]

PrivacyMark System (JPN) is a certification provided by JIPDEC that assesses compliance with the Japanese "Act on the Protection of Personal Information (APPI)" and complies with Japanese Industrial Standard JIS Q 15001:2006 on Personal Information Protection Management System (PMS). The scheme was established in 1998 and has issued over 31.000 certificates. The Japan Institute for Promotion of Digital Economy and Community (JIPDEC) is a non-profit foundation for development of key IT technologies and policies. The scheme targets private enterprises and issues one certificate per enterprise.[59]

TrustArc APEC CBPR certification (US) The Asia Pacific Economic Cooperation, with its 21 Member Countries, including the US, is a significant economic region. It has established a Cross-Border Privacy Rules (CBPR) framework with Accountability Agents certifying data transfer practices. So far, only the US and Japan have accredited Accountability Agents. TrustArc is the Accountability Agent in the US. It offers multiple certifications and hence has extensive experience in the field of certification.[60]

[56] Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens)
[57] NOREA, 'Privacy audit proof' (NOREA) <https://www.privacy-audit-proof.nl/ > accessed 13 March 2018.
[58] Ryerson university, 'Privacy by Design Certification' (Privacy by Design Centre of Excellence, 2018)<http://www.ryerson.ca/pbdce/certification/ > accessed 13 March 2018.
[59] JIPDEC, 'PrivacyMark' (PrivacyMark System) <https://privacymark.org/ > accessed 13 March 2018.
[60] TrustArc, 'Extend your privacy commitment with the APEC Cross Border Privacy Certification' (TrustArc, 2018)<https://www.trustarc.com/products/apec-certification/ > accessed 13 March 2018.

Health Personal Data Storage (Agrément des hébergeurs de santé de données personnelles) (FR).[61] The French Ministry of Health requires processors storing personal data relating to health on behalf of data controllers to undergo a prior approval process led by the CNIL. The Ministry of Health has already issued 96 approvals since 2006.[62]

Table 3 provides an overview of the fifteen selected schemes classified according to the selection criteria outlined above. The table shows that there are numerous comprehensive schemes as well as security specific schemes. There are no data protection by design or data transfer specific certification schemes within the EU that we are aware of. Outside the EU, the research team identified schemes that cover most defined scopes (from comprehensive to specific).

Group A (PD /PII, voluntary, 3d party process)	Comprehensive	PbD	Security	Transfers	New topics children
	controller	controller	controller	controller	controller
	processor	processor	processor	processor	processor
EU wide & MS	ISDP 10003:2015 BSI BS10012 --- EuroPriSe Label CNIL Datenschutzaudit beim ULD --- Norea Myobi --- E-Privacy app Health Personal Data Storage		ISO/IEC 27001 BSI ISO 27018:2014 (cloud proc.)		
Regional non-EU				TrustArc APEC CBPR	
National non-EU	PrivacyMark	Ryerson PbD			iKeepSafe COPPA

[61] CNIL, 'Data Protection' (CNIL) <https://www.cnil.fr/fr/labels> accessed 13 March 2018.
[62] Since March 2018, the process is no longer available. See for the new certification procedure: <https://esante.gouv.fr/labels-certifications/hds/certification-des-hebergeurs-de-donnees-de-sante> accessed

Table 3-3 Overview of selected schemes classified according to the selection criteria

3.3. Certification models

The following section outlines the findings of the analysis of the certifications that were selected. The findings are grouped under categories relating to the scope, normative basis, sector, subject matter and others.[63]

3.3.1. Certification Scope

All processes v. dedicated processes

Several of the certifications that were analysed, certify all types of processes while half of them focus on dedicated processes and two schemes only certify the conformity to management systems dedicated to personal data.[64]

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

Table 3-4 Overview of dedicated v. all processes model

On the one hand, the '*all processes'* model suggests that the processing of personal data is similar enough to be certified by a single certification scheme, since the certifications do not introduce any variations regarding the type of processing operation.[65]
On the other hand, the '*dedicated processes'* model challenges the former approach or, at least, demonstrates there is room in data protection certification for another model focusing on dedicated processes.[66]

[63] The categories are not necessarily representative of the existing certification landscape. The aim of this section is to demonstrate identified trends in the analysed certifications.
[64] BSI BS 10012, TÜV Italia ISO/IEC 27001 and to some extent the Privacy by design certification Ryerson that is certifying the compliance of data processing with the privacy by design principles.
[65] EuroPrise, ISDP 2003:2015.
[66] International Data Flows, Data flows within a local network, Data processing in direction of children under 13, Mobile app processes, Data processing handled by public authorities, Health data flows, Secured data flows, Data flows in the cloud.

The sample did not provide reliable evidence regarding the inferiority or superiority of either models. The growing complexity of the processing operations, the extended collection of personal data in many business activities could advocate for dedicated schemes. This is the direction taken by the ISO/IEC 27018:2014 dedicated to cloud processors and APEC's accountability agents dedicated to international data flows. But, one must keep in mind that the most widespread scheme in data protection, the JIPDEC PrivacyMark System, belongs to the *all processes* model.

Two certifications in the sample certify the compliance of processes put in place to manage personal data processing. Management system schemes are, by design, independent of any functional or sectoral scope. However, the BSI 10012 scheme focuses on data protection while TÜV Italia ISO/IEC 27001 is specialized for security management systems.[67]

The Privacy by design certification by Ryerson suggests an interesting approach in management system certification. The scheme offers certification of compliance of the management system of personal data processing with the GDPR, but also with Privacy by Design principles. Therefore, Ryerson goes beyond the regulatory compliance to assure an additional level of compliance with the protective principles elaborated by Cavoukian.

Multi-sector (or sector-neutral) vs single sector

Several schemes[68] claim a multi-sectoral coverage, offering certification of processes in all business activities, while some others focus on dedicated business activities.[69]

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

[67] While certification of management systems *as such* is out of the scope of the GDPR data protection certification mechanisms, the research team included those certifications because they offer useful lessons in other aspects such as the organisation of the certification process or SME friendliness.

[68] EuroPriSe, ISDP 10003:2015, JIPDEC PrivacyMark, Privacy by design certification Ryerson, Privacy-Audit-Proof, Privacy Seal MYOBI, TRUSTArc APEC CBPR, TUV Italia-ISO/IEC 27001 certification.

[69] BSI-ISO/IEC 27018, CNIL - SafeBox, Datenschutzaudit beim ULD, E-Privacy App, IKeepSafe

	Datenschutzaudit beim ULD E-Privacy App IKeepSafe

Table 3-5 Overview of multi-sector v. single-sector model

The '*multi-sectoral'* model seems to suggest that data processing are similar enough in all business activities to be managed under the same scheme, while also a '*single-sector'* model exists opting for specialised schemes targeting a *single sector*.

SME 'friendly' model

Certain certifications, without focusing on Small and Medium sized companies (hereinafter SMEs) have a dedicated offer to the SMEs. Some apply a pricing policy tailored to the size of the applicant, while others apply a free of charge or a discount policy to all the certification candidates.

	Certification scope models
SME friendly model The scheme has an offer dedicated to SMEs	CNIL Safebox (Free of charge policy) CNIL - ASIP Santé (Free of charge policy) IKeepSafe, (Pricing discount policy) JIPDEC PrivacyMark (Pricing discount policy)

Table 3-6 Overview of SME friendly model

The Privacy by design certification that Ryerson offers, along with a paid third-party certification scheme, includes a self-assessment process[70] accessible for free to SMEs. This self-assessment process could be seen as a first maturity level preparing SMEs for applying to the third-party scheme.

International v. national and sub-national certifications

Several schemes[71] have an international scope in the sense that they offer to certify entities established inside and outside the EU. Other certifications[72] certify entities registered within the national territory of the scheme operator. The Datenschutz beim ULD certifies public institutions operating in the German Länd of Schleswig-Holstein.[73]

[70] Hewlett Packard Enterprise and Privacy by Design Centre of Excellence at Ryerson University, 'The Privacy Toolkit' <http://h41111.www4.hpe.com/privacy-toolkit/overview.html> accessed 12 March 2018.
[71] See Table 3-7.
[72] Ibid.
[73] Datenschutzaudit beim ULD.

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

Table 3-7 Overview of international v. national models

The origin of the applicants for certification is not always restricted by the geographical scope of the scheme. Some schemes certifying the compliance with European regulations have certified companies not registered within the EU.[74] The geographical scope of a scheme is closely related to the geographical scope of its normative basis. A certification scheme inherits the geographical limitations of its normative basis. The geographical scope of the schemes based on regulation is commonly limited to the territory where the regulation is applicable. On the opposite side, schemes based on international technical standards[75], by design, have an international scope, insofar as ISO/IEC standard criteria are not linked to a national or regional regulation.

Single-issue certification v. Comprehensive certification

	Certification scope models

[74] Subsection 2.2 of the EuroPriSe Rules of Procedure for the certification of IT products and IT-based services states "Manufacturers and vendors of IT products and providers of IT-based services can apply for a seal even if they are not subject to EU data protection law, but want to prove the compliance of their processing operations with EU law nevertheless".
[75] BSI ISO/IEC 27018, TÜV Italia ISO/IEC 27001.

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

Table 3-8 Single-issue certification v. Comprehensive certification

The regulatory scope[76] reveals two opposing models. On one hand, a Comprehensive model encompasses certifications certifying against the vast majority of provisions[77] included in the GDPR or other data protection laws. On the other hand, a single-issue certification model encompasses the schemes certifying the conformity with a single or limited number of legal obligations in the regulation.[78]
Certifications based on international standards seem to follow ISO/IEC's approach that is encouraging a dedicated/sectoral approach, while European schemes seem to prefer a more generic all-encompassing model. However, this conclusion must be used with caution to the extent that the selected sample is not fully representative of the market. Moreover, The Canadian Privacy by Design of Ryerson includes GDPR requirements.

Findings Summary

The initial mapping of the market schemes and the analysis of the 15 selected schemes have demonstrated that many different models of data protection certification are available, both within the Union and abroad. The data protection certification market offers a series of schemes focusing on certification of management systems, some of them accredited against the ISO/IEC standard dedicated to the accreditation of certification bodies specialized in this type of certification.
The market also offers subnational schemes that are based on a subdivision of the national territory. At the opposite side, some

[76] This dimension classifies the schemes in function of the regulatory scope in the GDPR they intend to cover.
[77] Only provisions referring to powers of DPAs and other organizational provisions are excluded.
[78] Ryerson on Art. 25(3) GDPR; BSI ISO 27018 on Art. 28(5) GDPR; TUV Italia ISO 27001 on Art. 32(3) GDPR; TrustArc APEC CBPR on Art. 46(2)(f) GDPR. However, it is noteworthy that the schemes studied may not have been specifically designed to help compliance with GDPR provisions.

European schemes, based on international standards, operate worldwide. The data protection certification is not limited to the European market. But also include the US and certain Asian countries.
One should keep in mind that data protection certification is still in its infancy insofar some important topics remain missing from the current market for data protection certification.

3.3.2. **Normative criteria**

Regulatory model

The *regulatory* model encompasses the schemes using a regulatory framework as the normative basis of the scheme that could be an EU or non-EU one.[79]

	Normative criteria
Normative basis: law The scheme is based on a legal framework (EU or non-EU one)	CNIL Safebox, CNIL - ASIP Santé, Datenschutzaudit beim ULD E-Privacy App, EuroPriSe, IKeepSafe (US) ISDP 10003:2015, Privacy by design certification Ryerson, Privacy Seal MYOBI, Privacy-Audit-Proof

Table 3-9 Overview of certifications based on data protection legislation

Some schemes, in this model, only refer to the EU data protection framework[80] while others refer to a national or a sub-national data protection frameworks. Two schemes refer to a non-EU regional or national regulatory framework[81]. EuroPrise refers to both the GDPR and the e-Privacy Directive in its requirements.

	Normative criteria
Regional regulation The certification refers to the EU data protection regulation (DIR 95/46/EC or GDPR or another non-EU regional regulation	BSI- BS 10012 EuroPriSe, ISDP 10003:2015, Privacy by design certification Ryerson, Privacy Seal MYOBI.

[79] COPPA guidelines in IKeepSafe (USA); APEC CBPR rules in TRUSTe APEC CBPR (USA).
[80] BSI - BS 10012; CNIL – SafeBox; CNIL - ASIP Santé; Datenschutzaudit beim ULD; E-Privacy App; EuroPriSe; ISDP 10003:2015; Privacy by design certification Ryerson; Privacy Seal MYOBI; Privacy-Audit-Proof.
[81] BSI - ISO/IEC 27018; IKeepSafe; JIPDEC PrivacyMark System; TUV Italia - ISO/IEC 27001 certification.

National regulation The scheme refers to the national or sub-national data protection law	CNIL Safebox, CNIL - ASIP Santé, E-Privacy App, IKeepSafe (US) Privacy-Audit-Proof
Sub-national regulation The scheme refers to the national or sub-national data protection law	Datenschutzaudit beim ULD
Several regulations The scheme refers to several regulations in their requirements.	EuroPrise (GDPR + e-Privacy)

Table 3-10 Overview of territorial scope of regulatory model

EU based[82] schemes are currently in the middle of a transitional period with their GDPR-update in progress. Some of them have already completed the update and, interestingly, all of the updated schemes refer to the complete set of principles defined in the GDPR.[83]
The majority of the schemes that are based on the Regulation have translated the legal provisions into auditable standards. Two schemes[84] are already using the direct provisions of the law, as requirements.
Most of the schemes have drafted their criteria in accordance with the drafting recommendations included in the ISO/IEC 17007 standard without however always referring to them. The same proportion drafted the requirements under a series of assertions organised by themes following the ISO recommendations. Some schemes[85] have drafted their criteria in the form of a questionnaire.

The *Standard* model encompasses the schemes using national or international technical standards as a basis. Almost all of them refer to an ISO standard. The JIPDEC PrivacyMark refers to a national industrial standard dedicated to data protection issues[86] while the two other ISO based schemes refer to an IT security standard. The BS 10012 uses a management system approach to address the data protection requirements included in the GDPR.

	Normative criteria

[82] CNIL Safebox; Datenschutzaudit beim ULD; Privacy Seal MYOBI; Privacy-Audit-Proof.
[83] BSI 10012; E-Privacy App, EuroPriSe; ISDP 10003:2015, Privacy by design certification Ryerson.
[84] CNIL - ASIP Santé; Datenschutzaudit beim ULD.
[85] CNIL - ASIP Santé; ePrivacyApp.
[86] Japanese Industrial Standards JIS Q 15001:2006 - Personal Information Protection Management System - Requirements.

Standard model The scheme is based on a standard issued by a national or an international standardization body	BSI -BS 10012, BSI- ISO/IEC 27018, JIPDEC PrivacyMark, TUV Italia - ISO/IEC 27001 certification

Table 3-11 Overview of certifications based on technical standards

In the *Standard* model, the requirements (:in GDPR terminology: 'certification criteria') are built and agreed in the standardisation development process via a consensus based-approach procedure. The development of standards is independent from the development of the certification scheme. The wording and approaches used included in the technical standards slightly differ[87] and sometimes might conflict with the regulatory one.
The *Regulatory* and the *Standard* model*s* did not actually compete until the enactment of the GDPR. There was a limited number of technical standards available in data protection – as opposed to information security - before the inception of the ISO/IEC 27018.

The *Combined model* includes the certifications which refer to both a regulatory framework and technical standards in order to ensure that the requirements do not conflict with any rules and concepts existing in the different sources.

	Normative criteria
Combined model The schemes both refer to a regulation and to one or several other(s) normative basis (Technical standard(s) or and code of conduct)	BSI -BS 10012, BSI- ISO/IEC 27018, E-Privacy App, ISDP 10003:2015, Privacy by design certification Ryerson, TUV Italia - ISO/IEC 27001 certification

Table 3-12 Overview of certifications based on both data protection legislation and standards

In some cases, the alignment work done by the scheme owners was aimed at preventing potential conflicts between the basic principles included in the certification requirements.[88] In other cases, it also aimed to align the scheme process with the requirements defined in recognised technical standards.[89]

[87] The ISO/IEC 27018 focuses on Personal Identifiable Information (PII), rather than Personal Data even though the definition underlying PII in the standard is quite similar, but not identical with the GDPR definition of personal data.
[88] Privacy by design certification Ryerson.
[89] BSI -BS 10012; BSI- ISO/IEC 27018; ISDP 10003:2015; Privacy by design certification Ryerson; TUV Italia - ISO/IEC 27001 certification.

Findings Summary

The study identified two certification models which are potentially competing against each other. The first one is based on the European regulation(s) while the other one stems from the ISO/IEC approach.

These two models, although similar in their foundations[90], offer slight differences in the vocabulary and key principles regarding what they intend to protect. Moreover, the ISO model is industry-led on the basis of a consensus.[91] The ISO approach appears closer to the code of conduct model described in Article 40 GDPR for which the European law requires a public approval and monitoring.

The ISO approach challenges the GDPR one insofar as the ISO leverages the businesses familiarity with its vocabulary and concepts which are well known by companies managing quality and security through ISO standards. Moreover, the ISO offers a ready to use solution already in force when Article 42 GDPR schemes are still to be defined, approved, and established. Finally, the standards organisations are already busy completing their own approach with a series of additional standards intending to address the other aspects of privacy/data protection compliance.[92]

The ISO has already influenced data protection standardisation by offering a sectoral approach built in as an additional layer on the IT security standards. A work of endorsement and/or alignment with GDPR's approved certification standards is a matter for further research. The alignment effort could be long and tough to the extent that the European authorities are not represented in the international standardisation process.

3.3.3. **Scheme arrangements**

A scheme includes a series of core components in terms of origin and arrangements. At a minimum level the scheme encompasses a conformity assessment process and a certification issuance process. A

[90] Both models leverage the same foundational principles set in the Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (European Treaty Series - No. 108) and Organisation for Economic Co-operation and Development, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data'.

[91] See Errol Meidinger, 'Forest Certification and Democracy' (2010) 16 Legal Studies Research Paper Series Paper.

[92] Enhancement to the ISO/IEC 27001 for privacy management (ISO/IEC 27552), Privacy Impact Assessment (ISO/IEC 29134), Privacy controls (ISO/IEC 29151), Privacy Enhancing Technologies for Data de-identification (ISO/IEC 20889), Online privacy notices and consent (ISO/IEC 29184).

scheme also commonly includes a monitoring and a renewal process with, frequently, but not always, an internal dispute resolution process. The scheme components can be designed and owned either by private or public bodies. A single certification body can manage the full process, assessing and certifying the applicant. The certification process can be also split between different bodies or individuals. For instance, one entity (typically an individual) performing the conformity assessment, while the another is in charge of issuing the certification (a legal personality).

Certifications by public authorities

A selection of the analysed certifications[93] have been designed and are managed by a public authority, [94] commonly a data protection authority.

	Scheme arrangements models
Certification by public authorities The scheme is fully managed by a public authority	CNIL Safebox, CNIL - ASIP Santé, Datenschutzaudit beim ULD

Table 3-13 Overview of certifications operated by public authorities

In this model, the authorities draft their own criteria derived from the law[95] or directly refer to the provisions of the national data protection law.[96] Also in this model, the authorities manage the entire certification process, sometimes in collaboration with another authority like CNIL - ASIP Santé where the French ministry of Health collaborates with the French data protection authority (CNIL).
A certification model in which the same body sets the rule, assesses them and issues the credentials once the assessment complies with the conformity can be problematic in terms of potential conflict of interests even for such authorities.

Privately-owned certifications accredited or monitored by public authorities

[93] CNIL Safebox; CNIL - ASIP Santé; Datenschutzaudit beim ULD.
[94] CNIL - ASIP Santé schemes is managed by the ASIP-Santé. The scheme is an approval process. It will be turned, next year, into a third-party certification managed by the private sector. See the presentation of the scheme (French only) on the ASIP santé website. Certification des hébergeurs de données de santé at <http://esante.gouv.fr/services/hebergeurs-de-donnees-de-sante/procedures-pour-les-hebergeurs-de-donnees-de-sante>. CNIL Safebox is fully managed by the French DPA. The Datenschutzaudit beim ULD is fully managed by the data protection authority of Schleswig-Holstein in Germany.
[95] CNIL Safebox and CNIL - ASIP Santé.
[96] Datenschutzaudit beim ULD.

Several of the certifications that were studied are monitored by a public authority. The authorities are primarily playing the role of accreditation authority. In one third of cases[97], they are directly managing the accreditation process while, in the other two thirds[98], the process is managed by the national accreditation body. The research team did not identify any schemes which are undergoing an accreditation process involving both the national accreditation body and another public authority.

	Scheme arrangements models
Monitored A public authority plays a limited but active role (eg. Accreditation)	BSI -BS 10012 (Accreditation), BSI- ISO/IEC 27018 (Accreditation), IKeepSafe (Accreditation, Requirements drafting), ISDP 10003:2015 (Accreditation), TRUSTe APEC CBPR (Accreditation, Requirements drafting), TUV Italia - ISO/IEC 27001 certification (Accreditation)

Table 3-14 Overview of monitored privately-owned certifications

Privately owned certifications

One third of the schemes studied are fully managed by some private body. In this model, the process and the requirements are designed and managed by a private body without involvement of any public authority.[99] JIPDEC (and Ikeepsafe) are the only not-for-profit companies.

	Scheme arrangements models
Privately owned The scheme is fully managed by a private body without any public authority intervention	E-Privacy App, EuroPriSe, JIPDEC PrivacyMark, Privacy by design certification Ryerson, Privacy Seal MYOBI, Privacy-Audit-Proof

Table 3-15 Overview of privately-owned certifications

Internally managed v. outsourced certification process

Most of the scheme owners internally manage the certification process. A number of the schemes studied outsourced the conformity assessment to external auditors but maintain the process of managing

[97] Ikeepsafe; TrustaArc; APEC CBPR.
[98] BSI - BS 10012; BSI - ISO/IEC 27018; ISDP 10003:2015; TUV Italia - ISO/IEC 27001 certification.
[99] EuroPrise may be seen as an exception, as the certification scheme was originally owned by a data protection authority and was later privatised.

the issuing internally.[100] The ISDP 10003:2015 offers to fully outsource the certification process under a licencing agreement.

	Scheme arrangements models
Internally managed model The scheme owner manages the entire certification process	BSI - BS 10012, BSI - ISO/IEC 27018, CNIL - SafeBox, CNIL - ASIP Santé, Datenschutzaudit beim ULD, IKeepSafe, Privacy Seal MYOBI, TRUSTe APEC CBPR, TUV Italia - ISO/IEC 27001 certification
Out-sourced model The scheme fully or partly out-source the certification process to external auditors	E-Privacy App, EuroPriSe, ISDP 10003:2015, JIPDEC PrivacyMark System, Privacy by design certification Ryerson, Privacy-Audit-Proof

Table 3-16 Overview of internally managed v. outsourced certification process

The team did not find any convincing pattern underlying the choice of outsourcing. Either options can be linked to the market conditions, business opportunities or to the need of flexibility, but none of these explanations give an answer as to why the scheme owners have chosen one process over another.

Findings Summary

The analysed certifications demonstrate the various arrangements one can find in certification. The flexibility offered by this procedure is, at the same time, its strength and weakness.
On the one hand, flexibility offers to easily adapt the certification process to any business needs, regulatory conditions or any requirements. On the other hand, this flexibility creates a wide variety of certification schemes diluting the notion of certification and challenging what certification is.

For instance, the quick scan highlighted the existence of many trustmarks on the data protection certification market presented as certification marks. However, trustmarks in principle do not require external assessment process to be granted.

[100]The different assessment models are further detailed in the assessment process section.

3.4. Conclusion

The chapter presented different certification models that exist in the market. The analysis was based on a selection of both EU and non-EU oriented certifications. Despite the novelty of the GDPR data protection mechanisms, valuable lessons can be learned from the analysis of the existing certifications. Existing certifications already have mechanisms in place: assessment methodologies, contractual arrangements, and auditors that can and should be used in the establishment of the GDPR data protection mechanisms. The analysis identified models of certifications with varying degree of involvement of public authorities ranging from privately owned certification schemes to certifications owned by public authorities. Certifications monitored – in the form of accreditation - or owned by public authorities are offering examples for the GDPR certification mechanisms that require oversight of the supervisory authorities. Another lesson relates to the auditors. When the certification body does not have the capacity in its internal staff, the best practice is to collaborate with external auditors.[101] In external collaborations, the overall responsibility for the quality, integrity and due diligence of the auditors' performance should remain with the certification body, alongside any professional liabilities of the auditor towards the applicant for certification.

As per the normative sources and criteria, the analysed certifications follow three models: the regulatory model, the standards model and the combined model. Certifications following the regulatory model use legislation as their normative basis. This is a model close to the GDPR data protection certifications, which imply that certifications in line with Art. 42 GDPR relate to one or more GDPR provisions ("single-issue" or "comprehensive" certifications), as analysed in the following chapter. Certifications following the regulatory model are often combining ePrivacy with the GDPR, the national law implementing the former Data Protection Directive or other local data protection-related legislation. On the one hand, this practice reduces significantly the bureaucracy and costs for applicants, as it provides a single certification for different legal requirements. On the other hand, one should be careful in combining legal instruments as a basis for the same certification, as risks of incompatible goals or criteria might arise.[102] A quite common model is the standards model. Certifications based on international, European, or national standards. Such certifications do not usually –at least formally - claim any relationship with legislation. The international

[101] An example of EU wide certification which follows a decentralised approach with regard to its auditors is EuroPrise. EuroPrise trains its auditors, who are not internal staff of the certification body and are established in different EU Member States.

[102] See on the certification criteria in Chapter 4 on Certification.

standards from ISO and IEC are drafted with the aim to serve organisations established globally, thus references to national or regional legislation are avoided. It is quite often seen however that in practice such standards and subsequently certifications are used in relation to legal obligations. Before a claim can be made, that an ISO/IEC based certification is used to demonstrate compliance with (certain) GDPR legal obligations several necessary steps should be undertaken such as reviewing the compatibility of the terminology and matching the scope of the standard to the requirements for the fulfilment of the legal obligation.[103] A third model identified in the combination of normative sources: both standards and legislation. The combined model approach offers the advantage of combining the experience from standards with legislation as a normative source. Again, such certifications need to clearly explain a methodology of combining the two different types of normative sources and how incompatibilities are resolved.

Another identified type of model relates to the types of processing operations and the subject matter of certifications. Certifications such as the PrivacyMark and EuroPrise follow a comprehensive and all-processes model, meaning that they do not differentiate per type of business process; neither do they focus on a single topic. This practice is often called "one-size-fits all", even though in the assessment methodologies of the said certifications, one can identify a more tailored approach.[104] In the same category, we identified certifications focused on dedicated processes (e.g. mobile app processes or cloud processes) and single-issue models (e.g. by design, data security). Both models are compatible with the GDPR; however issues of transparency on the scope and soundness of the assessment methodology will be critical to determine whether the outcome meets the aim of the data protection certification mechanisms to demonstrate compliance of processing operations with provisions of the Regulation.

[103] See more on Standards in Chapter 6 on Technical standards for certification p.129f.

[104] The assessment may be done on the basis of protection goals for the specific process under review. See Kirsten Bock "Data protection certification: Decorative or effective instrument? Audit and seals as a way to enforce privacy" in David Wright, Paul De Hert (eds.) *Enforcing Privacy*. Springer, Cham, 2016. 335-356.

4. Certification

4.1. Introduction

This section focuses on the certification criteria and the certification process. The first part explores lessons to be learned from the New Approach legislation and harmonised standards, the eIDAS Regulation and the proposal for a Cybersecurity Act.[105] Building on the case studies and literature review on requirements engineering, we provide step-by-step guidance to the supervisory authorities for the review and approval process of certification criteria in line with Art. 42(5) GDPR. Following that, the Chapter provides insights on current practices in relation to certification process and issues such as complaint handling, dispute resolution and training of auditors. The insights are derived from the ISO/IEC 17065 technical standard and the research conducted in Chapter 3 of the Report.

4.2. Lessons from other fields: case studies

In order to provide guidance on how to assess whether the transformation of abstract and open norms (GPDR) into auditable requirements is done adequately, we can draw lessons from a number of other domains in EU regulation.

4.2.1. Case study: New Approach legislation and harmonised standards

4.2.1.1. Aim

The first domain that can offer insights on how to transform open norms into auditable standards is that of the New Approach and harmonized standards. Despite the differences of the New Approach legislation with the EU data protection legislation, it can provide valuable inspiration. First, it provides an example of how open norms are operationalised into (harmonised) technical standards in practice. Second, the case provides some insights in how technical standards can be evaluated (in view of the higher-level open norms).

4.2.1.2. Overview of New Approach Legislation and rationale

The New Approach,[106] as updated by the New Legislative Framework (NLF),[107] determines a system of legal instruments and non-legislative instruments (for instance providing guidance or establishing cooperation agreements among institutions) which are relevant to product safety

[105] Since the legislative process is ongoing, the current Study takes into account the European Commission proposal for a Cybersecurity Act (COM (2017) 477).
[106] European Commission, 'The New Legislative Framework' (Growth, 2018) <https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en> accessed 14 March 2018.
[107] Ibid.

and can be used across the board in all industrial sectors. The rationale is that all the elements of this system (NLF) form a *quality chain*,[108] in that they are complementary. As the European Commission has stressed "if one element goes missing or is weak, the strength and effectiveness of the entire 'quality chain' is at stake".[109] The rationale for such a system in product safety is that the quality of products often relates to the quality of the manufacturing, which in turn may be affected by the quality of testing, inspection or other conformity assessment activity.

4.2.1.3. Essential requirements and standardisation requests

The common element of the New Approach Directives is the provision of the Essential Requirements, which are mandatory for manufacturers to be complied with. The Essential Requirements are the necessary requirements for a product to be placed in the EU market and circulate freely in line with the principle of free movement of goods. These Requirements define "the results to be attained, or the risks to be dealt with, but do not specify the technical solutions for doing so, suppliers are free to choose how the requirements are to be met."[110] The Essential Requirements need to provide sufficient information to enable assessment of whether products meet them.[111] The Toys Safety Directive[112] is a New Approach Directive. Article 10(2) of the Directive ("Essential Safety Requirements") provides:

"*Toys, including the chemicals they contain, shall not jeopardise the safety or health of users or third parties when they are used as intended or in a foreseeable way, bearing in mind the behaviour of children*."[113]

In addition, Annex II of the Directive provides a set of Particular Safety Requirements regarding a range of topics such as toy safety and hygiene.

In the case of hygiene, for instance, the Directive requires[114] that toys are designed and manufactured "in such a way as to meet hygiene and

[108] The EC explains that the word 'quality' is used to "designate the level of safety and other public policy objectives which are aimed by the Union harmonisation legislation" (European Commission, 'Commission Notice. The 'Blue Guide' on the implementation of EU products rules 2016' (26.7.2016), OJ C 272/01.
[109] Ibid.
[110] European Committee for Standardization, 'The 'New Approach'' (CEN, 2016)<https://boss.cen.eu/reference%20material/guidancedoc/pages/newapproach.aspx > accessed 13 March 2018.
[111] Ibid.
[112] Directive of the European Parliament and the Council on the safety of toys [2009] OJ 2 170/01, available: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02009L0048-20140721&from=EN accessed 13 March 2018.
[113] Art. 10(2) Toys Safety Directive
[114] Annex II (V) Toys Safety Directive

cleanliness requirements in order to avoid any risk of infection, sickness or contamination."
All the above Essential and Particular Safety Requirements consist of high-level obligations, in the sense that they do not provide specific information on what a manufacturer should do to comply with the obligation. Instead, the Essential Requirements provide the achievable result (e.g. safety) or the result to be avoided (e.g. contamination). Article 10(2) of the Directive, as seen above, for instance, provides that the toy shall not jeopardise the health or safety of the users or third parties. This provision does not explain however to the manufacturer what to do in order to avoid such a result. Similar requirements with open legal norms, such as safety, risk, adequate protection, adverse effects, are also found in the other New Approach Directives.[115]

To assist manufacturers, to comply with their legal obligations, as set out in the New Approach Directives, the European Commission publishes standardization requests addressed to the European Standardisation Organisations (ESOs).[116] Such requests (otherwise called 'mandates') instruct the ESOs to elaborate European Standards, or identify existing European Standards, which will offer technical solutions to meet the Essential Requirements.[117] The aim of such standardisation requests is therefore to first make sure that the existing or new standards cover the scope of the Directive's essential requirements, so that potentially, for all Essential Requirements there are relevant technical standards and second, to satisfy those Essential Requirements. Such standardization requests, if accepted by the ESOs, are undertaken by the relevant Technical Committees. In relation to Toy Safety for example, CEN has established the Technical Committee 52 (TC 52),[118] the primary purpose of which is to establish requirements and test methods, which support the essential requirements of the Toy Safety Directive.[119] The participants of the Technical Committees are

[115] See for instance Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, as amended by Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 OJ L 331 1 7.12.1998; Directive 2000/70/EC of the European Parliament and of the Council of 16 November 2000 OJ L 313 22 13.12.2000; Directive 2001/104/EC of the European Parliament and of the Council of 7 December 2001 OJ L 6 50 10.1.2002; Regulation (EC) N Directive 2001/104/EC of the European Parliament and the Council of 29 September 2003 OJ L 284 1 31.10.2003; Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007 OJ L 247 21 21.9.2007.
[116] See Glossary in Annex 1 (separate document).
[117] The process of standardization requests is provided in Regulation 1025/2012 of the European Parliament and the Council on European standardisation of 25 October 2012 OJ L 316/12.
[118] More information: CEN, 'CEN/TC 52 - Safety of toys' <https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:6036&cs=11F6E318EDC183DBB11833CD71FA138F9> accessed 12 March 2018.
[119] CEN/TC 52, 'Business Plan. Safety of Toys' (2017) available <https://standards.cen.eu/BP/6036.pdf> accessed 13 March 2018. The experts participating in the Technical Committees are appointed by the national standardization bodies of the Member States, which have expressed the interest to participate in the Technical Committee, either actively contributing to the development of the standards or as observers.

experts who apply their know-how to the development of the requested standards.

4.2.1.4. Performance approach of technical standards

Technical standards are voluntary in nature, even when they determine technical solutions for a manufacturer to comply with, the Essential Requirements in the harmonized New Approach legislation. Technical standards include straightforward requirements. According to the CEN CENELEC internal guides, European Standards preferably follow a performance approach.[120]

EXAMPLE Different approaches are possible in the specification of requirements concerning a table: Design requirements: The table shall have four wooden legs. Performance requirements: The table shall be constructed such that when subjected to ... [stability and strength criteria].

Source: CEN CENELEC[121]

Table 4-1 Example of design v performance requirement

In addition, the **requirements should be consistent and objectively verifiable**. As per the formulation of standardization requirements, there are specific mandatory rules followed by the Technical Committees of the European Standardisation Organisations.

[120] European Committee for Standardization, 'Internal Regulations Part 3' [2017] 1(1) Principles and rules for the structure and drafting of CEN and CENELEC documents <https://boss.cen.eu/ref/IR3_E.pdf > accessed 13 March 2018.

[121] Ibid.

Verbal form	Equivalent phrases or expressions for use in certain cases
shall	is to is required to it is required that has to only ... is permitted it is necessary needs to
shall not	is not allowed [permitted] [acceptable] [permissible] is required to be not is required that ... be not is not to be need not do not
EXAMPLE 1 Connectors shall conform to the electrical characteristics specified by IEC 60603-7-1.	
Imperative mood: The imperative mood is frequently used in English to express requirements in procedures or test methods. EXAMPLE 2 Switch on the recorder. EXAMPLE 3 Do not activate the mechanism before...	
Do not use "must" as an alternative for "shall". (This will avoid any confusion between the requirements of a document and external constraints – see 7.6). Do not use "may not" instead of "shall not" to express a prohibition.	

Source: CEN CENELEC[122]
Table 4-2 Formulation of requirements

4.2.1.5. Assessment by New Approach consultants

According to the Standardisation Regulation, the Commission together with the European Standardisation Organisations "*shall assess the compliance of the documents drafted by the European standardisation organisations with its initial request*".[123] In practice, this assessment is conducted by independent assessors, the New Approach Consultants. The New Approach Consultants are also assigned to provide advice to the Technical Committees while developing the requested technical standards.
The competences of the New Approach Consultants are the following:[124]

[122] European Committee for Standardization, 'Internal Regulations Part 3' [2017] 1(1) Principles and rules for the structure and drafting of CEN and CENELEC documents <https://boss.cen.eu/ref/IR3_E.pdf > accessed 13 March 2018.
[123] Art. 5 Regulation on European standardisation.
[124] CEN and CENELEC, 'Guide 15 Tasks and responsibilities of the New Approach Consultants' <ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Guides/15_CENCLCGuide15.pdf> accessed 12 March 2018.

- Deep technical understanding of the field of work of the relevant technical bodies and a recent state of the art experience of the subject;
- Extensive knowledge and experience of relevant directives/regulations and the related processes;
- Experience of developing and implementing standards;
- Knowledge of the main rules (e.g. CEN-CENELEC Internal Regulations, ISO/IEC Directives, different timeframes within the drafting process);
- Knowledge of the Vienna Agreement and/or Dresden Agreement;
- Social competence/interpersonal skills.

In the case of possible disagreements between the New Approach Consultant and the Technical Committee, the Technical Board of CEN and CENELEC decides on the resolution of the dispute. In general, during the assessment of the draft standard, a consultant does not have the right to veto a draft and there is no obligation for the technical body/Reporting Secretariat to accept comments given by a consultant.[125]
In the performance of his/her Tasks, the New Approach Consultant is not bound by pre-determined assessment criteria in relation to the topic of the specific standard. The assessment of whether the standard conforms to the standardization request and subsequently covers the Essential Requirements depends on the state-of-the art and the judgement of the New Approach Consultant.

Following a positive assessment by the New Approach Consultant that a harmonised standard satisfies the requirements, which are set out in the relevant New Approach Directive, the European Commission publishes the harmonised standard in the Official Journal of the Union.[126] Compliance with harmonized standards offers presumption of conformity with the Essential Requirements of the harmonised legislation. [127]

Apart from the assessment by the New Approach Consultant, the Standardisation Regulation introduces a right to object to the publication of the harmonised standard in the Official Journal. The European Parliament and the Member States have a right to raise a formal objection, in case they consider that the standard does not

[125] CEN and CENELEC, 'Guide 15 Tasks and responsibilities of the New Approach Consultants' <ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Guides/15_CENCLCGuide15.pdf> accessed 12 March 2018.
[126] Art. 6 Regulation on European standardisation 1025/2012.
[127] CEN and CENELEC, 'Frequently Asked Questions (FAQs)'<https://www.cencenelec.eu/helpers/Pages/FAQ.aspx> accessed 12 March 2018.

comply with the Essential Requirements of the New Approach legislation.

4.2.1.6. Lessons to be learned for data protection certification

- Translating legal norms to essential requirements

1. From legal norms to standardisation goals and further to substantial requirements[128]

The New Approach legislation includes essential requirements that are in essence open norms ("legal standards"). Such open norms are vague and context-specific. The open norms are further "translated" into standardisation goals by the European Commission and then turned to straightforward requirements by the standardisation organisations, which incorporate them in standards.

2. Performance-based approach, consistent and objectively verifiable requirements in technical standards.

- **Assessment of relevance and suitability**

1. Assessment by independent assessors based on the state of technical know-how at a given moment[129]
The system that relies on the expertise of individual experts offers flexibility in the sense that the appointed expert may take into account the latest technological or other developments. At the same time, such flexibility and over-reliance on individual experts (Consultants) may have implications as per the objectivity and reproducibility of the assessment results. A system which allows for the scrutiny of the assessment and the selection and appointment of the Consultant is necessary.

2. Involvement of the Assessor (observation) in the development of the standard
The Consultant is aware of the discussions, proposals and concerns around the content of the technical standard, which provides him/her with the opportunity to have a comprehensive overview of the issues at stake.

[128] Corresponds to the certification criteria (GDPR terminology) of Art. 42(5) GDPR.
[129] European Committee for Standardization, 'The 'New Approach'' (CEN, 2016) (n 90).

4.2.2. Case study: Electronic Identification and trust services for electronic transactions in the internal market

4.2.2.1. Aim

The second domain that provides insight in how to assess the results of transforming open norms into auditable requirements is the domain of Electronic Identification and Trust services. The Regulation 910/2014 (eIDAS Regulation) introduced common grounds for the operation of electronic signatures, electronic seals, timestamps, electronic delivery service, and website authentication[130]. The example of the eIDAS Regulation offers useful lessons for the operationalisation of the GDPR certification because it provides insights in procedural and organisational aspects of certifications and seals, as well as guidance on the assessment criteria applied by public bodies/authorities to decide on the approval (or in the case of eIDAS "notification") of the seal.

4.2.2.2. Overview of the Electronic identification legal framework under the eIDAS Regulation

The Regulation 910/2014 replaced the Directive 1999/93/EC and reformed the landscape on electronic identification in the EU. Most of the provisions of the Regulation started applying in July 2016.[131] In terms of electronic seals, the Regulation establishes a legal framework for the qualification and operation of electronic seals.[132] Electronic seals fall under the umbrella term "electronic services". The Regulation includes both generic provisions on trust services and specific provisions on electronic seals. Unlike the GDPR, the eIDAS Regulation provides definitions of the terms relevant to seals and certification. An electronic seal is "data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity".[133] Electronic seals allow several parties to sign electronic documents.[134]

The eIDAS Regulation provides for the classification of electronic seals, namely basic electronic seals, advanced electronic seals and qualified electronic seals. Qualified electronic seals are considered to provide

[130] Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014.
[131] Art. 52 ibid.
[132] The analysis of the legal framework in this section for the purposes of the study is not exhaustive. For a comprehensive analysis of the Regulation see: Jos Dumortier, 'Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation)' (2016) available: https://ssrn.com/abstract=2855484 accessed 12 March 2018.
[133] Art. 3 (25) Regulation on electronic identification and trust services for electronic transactions (n 110).
[134] Information Commissioner's Office, 'Key Definitions' (ICO, 2018) <https://ico.org.uk/for-organisations/guide-to-eidas/key-definitions/#electronic_seal> accessed 14 March 2018.

more security guarantees and meet stricter criteria.[135] In order to verify whether a seal is valid and to identify the person responsible for the electronic seal, certificates for electronic signatures may be issued by qualified trust providers. The legal effects of electronic seals are regulated in Art. 35 of the Regulation. Qualified electronic seals offer a presumption of integrity to the data and of correctness of the origin of the data, to which the electronic seal is linked.[136] Electronic seals may also, in principle, be admitted as evidence in legal proceedings.[137]

4.2.2.3. Scalability via the introduction of assurance levels and standardisation of requirements

In relation to electronic identification, the eIDAS Regulation establishes assurance levels. The Regulation relates the assurance levels to a degree of confidence of the electronic identification service.[138] Article 8 of the Regulation provides three levels of assurance:

Assurance level	Degree of confidence	Purpose of technical specifications, standards & procedures
Low	Limited	To decrease the risk of misuse or alteration of identity
Substantial	Substantial	To decrease substantially the risk of misuse or alteration of the identity
High	Higher	To prevent misuse or alteration of the identity.

Table 4-3 Assurance levels of electronic identification per Art. 8 eIDAS Regulation

Following the mandate provided in the eIDAS Regulation, the European Commission adopted a Commission Implementing Regulation[139], which sets out the minimum technical specifications and standards for electronic identification. The Commission Implementing Regulation is based on ISO/IEC 29115, which provides four assurance levels[140] (low, medium, high and very high) and further specifies the criteria and guidelines for achieving each of these four levels of entity

[135]International commissioner's office, 'Key Definitions' (ICO, 2018) <https://ico.org.uk/for-organisations/guide-to-eidas/key-definitions/#electronic_seal> accessed 14 March 2018.
[136] Art. 35 Regulation on electronic identification and trust services for electronic transactions.
[137][137]See conditions in Art. 35(1) ibid.
[138] Recital 16 eIDAS Regulation.
[139] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, OJ L 235/7, 9.9.2015.
[140] Information technology-Security techniques-Entity authentication assurance framework. Available <https://www.iso.org/standard/45138.html> accessed 12 March 2018.

authentication assurance. The rationale behind different levels of assurance resides with the difference between the needs of each element of the electronic identification process, depending on context and application areas, namely eHealth, eProcurement, eInvoicing, online banking and others.[141] The establishment of assurance levels also facilitates the mutual cooperation among the supervisory authorities.

Technical standards are in general the backbone of demonstrating compliance in the eIDAS system, as established in the Regulation. The abstract legal requirements are further specified as technical requirements in technical standards. Technical standards that pre-existed the eIDAS Regulation are already mentioned in the Regulation, as a point of reference, such as the Common Criteria ISO/IEC 15408 framework.[142] In addition, ETSI[143] and other standards organizations undertook the initiative to develop or adapt technical standards to fit the legal requirements of the eIDAS Regulation. Standards introduce controls which "allow for specific elements of the normative requirements to be verified or tested, thereby assisting the audit team in assessing the conformity with a requirement".[144]

Standards are useful also for the audits performed by the competent authorities. The eIDAS Regulation introduces a system on electronic trust services, in which there is no central authority at EU level, but national competent authorities competent for the supervision, enforcement and imposing of fines.[145] The penalties are established with national legislation in the Member States.[146] In parallel or independent of the regular (every 24 months) audit by a conformity assessment body, qualified trust service providers may be audited by or at the request of the national supervisory body.[147]

4.2.2.4. Certification and seals in the eIDAS electronic trust services

Certification is regulated in relation to qualified electronic signature creation devices and electronic seals. The scope, of the certification of the qualified electronic signature devices, is explicitly required to be limited. Recital 56 of the eIDAS Regulation provides that only the

[141] See infographic with eIDAS application areas. Available: <https://ec.europa.eu/digital-single-market/news/eidas-infographic-2016> accessed 12 March 2018.
[142] See Chapter 9, **Error! Reference source not found.**.
[143] The relevant ETSI standards are accessible: <https://portal.etsi.org//TBSiteMap/ESI/ESIActivities.aspx> accessed 12 March 2018.
[144] Arvid Vermote, 'Return on Experience from Conformity Assessment Bodies' (presentation at ETSI eIDAS workshop June 2016) available: <https://docbox.etsi.org/Workshop/2017/201706_SECURITYWEEK/02_eIDAS/S03_CONFORMITY_ASSES_BODIES_NATI_ACCR_SUP_BODIES/ERNST_YOUNG_VERMOTE.pdf> accessed 12 March 2018.
[145] Art. 17 Regulation on electronic identification and trust services for electronic transactions, Regulation 910/2014.
[146] Art.16 Regulation 910/2014.
[147] Art. 20 Regulation 910/2004.

hardware and system software, which are used to manage and protect the creation of the signature creation data, stored or processed in the signature creation device, can be certified. The certification process is carried out by either public or private organizations, according to the national law of each Member State.[148]

The requirements are primarily aimed at ensuring that certificates for electronic seals contain all the necessary information related to the issuance of the certificates that allow independent parties to verify the validity of the electronic seal. The requirements, among others, relate to:

- Information of the legal or natural persona that issued the certificate
- The name of the creator of the seal, details of the validity period
- The identity code of the certificate
- The advanced electronic signature or advanced electronic seal of the issuing qualified trust provider.
- Location where the certificate is free of charge

The requirements for qualified certificates for electronic seals[149] are also provided in the Regulation.[150] The requirements are aimed at providing all the necessary information for transparency and verifiability purposes. For instance, the qualified certificates need to contain:

- an indication that the certificate has been issued as a qualified certificate for electronic seal.
- information on the qualified trust provider, such as the Member State, the registration number of the legal persons or name of the natural persons and others.
- the name of the creator of the seal
- the validity of the certificate
- electronic seal validation data
- the location of the services where the certificate can be used, and others.

4.2.2.5. Mutual assistance, peer review system, and cross-border recognition

What is particularly interesting, in the system established with the eIDAS Regulation, is the obligation of the competent supervisory

[148] Art. 30 Regulation 910/2014 The Member States notify to the European Commission the names of the bodies, and the list is made available to the Member States.
[149] The Member States certificates for electronic seals are regulated in Art. 38.
[150] Annex III Regulation 910/2014.

authorities for mutual assistance.[151] The refusal of cooperation and assistance may only occur under the conditions the exhaustively listed in the Regulation (Art. 18(2)), which relate to the non-competence of the supervisory body, non-proportionality or incompatibility with the provisions of the eIDAS Regulation. Thus, each competent authority must, in principle, provide mutual assistance.

For reasons of legal certainty and high a level of security, the Regulation urges the regulator to seek for synergies with the Accreditation Regulation 765/2008 and other existing relevant European and international schemes.[152] This serves to provide continuity, coherence, and certainty in relation to the accreditation of conformity assessment bodies in the EU legal order. The eIDAS Regulation in specific refers to the requirements for accreditation as established in the Accreditation Regulation.

4.2.2.6. Lessons to be learned for data protection certification

- **Translating legal norms to certification criteria**

1 The eIDAS Regulation leaves the task of specifying requirements for the electronic trust services to the standardisation bodies. The Regulation defines high-level legal requirements and goals that need to be achieved. Thus, a similar approach to the New Legislative Framework is followed: the specification of requirements and criteria follows the rules set by standardisation bodies.

2 Assurance levels are introduced as a means of introducing scalability in the eIDAS system, selecting suitable criteria to each case and managing the expectations of the consumers regarding the confidence in the trust service.

- **Assessment of relevance and suitability**

3. The assessment is performed by accredited bodies on the basis of the relevant technical standards adopted in line with eIDAS.

[151] Art. 18 Regulation 910/2004.
[152] Recital 44 Regulation 910/2014.

4.2.3. Case study: Cybersecurity certification and the proposal for a "Cybersecurity Act"

4.2.3.1. Aim

The proposed Regulation of The European Parliament and of The Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification, the so-called "EU Cybersecurity Act", provides insights into certification as it proposes a European framework for cybersecurity certification in an area directly relevant to data protection. Even if it is not yet definitive, the approach to certification reflected in the proposal for the Regulation provides insights on the certification model.[153]

4.2.3.2. Overview

According to the text of the Proposal its basis was formed by, "the second mandate for the European Union Agency for Network and Information Security (ENISA) and the adoption of the Directive on security of network and information systems (the 'NIS Directive')". The Premise of the Proposal, as part of a series of new legislative measures in the area of cybersecurity, was the increased dependence of all aspects of both the economy and society on the digital infrastructure, an increase in the various risks associated with the cyber domain and the need to address them. The stated objective of the ensemble of measures, of which the Proposal is a part, is to promote "a culture of risk management, by introducing security requirements as legal obligations for the key economic actors, notably operators providing essential services (Operators of Essential Services – OES) and suppliers of some key digital services (Digital Service Providers – DSPs)."

4.2.3.3. Proposed European cybersecurity certification framework

The proposed Regulation adopted a model for a European certification framework with its own scope, functioning and governance rules and with it what could best be described as a centralised, pan-EU model regarding cybersecurity certification.

The advantages of the chosen system, situating ENISA at its centre, are expected to be:

- increased overall transparency of cybersecurity assurance of ICT products and services;
- increased trust in the digital single market and in digital innovation;

[153] For an overview of the proposal for a cybersecurity framework read: Andreas Mitrakas "The emerging EU framework on cybersecurity certification." Datenschutz und Datensicherheit-DuD 42, no. 7 (2018): 411-414.

- simplification of the processes through the introduction of the one-stop shop;
- easier cross-border operations of firms through reduced "fragmentation of certification schemes in the EU and related security requirements and evaluation criteria across Member States and sectors";
- virtual compliance tool not only with the proposed Regulation, but also with the NIS Directive;
- increased consistency with other EU policies (NIS, GDPR).

The European Cybersecurity Certification Framework (the "Framework") for ICT products and services would create a system or framework for the establishment of specific certification schemes for specific ICT products/services (the "European cybersecurity certification schemes") rather than introducing directly operational certification schemes.

The national certification supervisory authorities of all Member States would form the European Cybersecurity Certification Group with a role in advising the Commission "on issues concerning cybersecurity certification policy" and working with ENISA on the development of draft European cybersecurity certification schemes.

Such "European cybersecurity certification schemes" would set the (requirements for the) scope and object of certification, including, but not limited to:

- the identification of the categories of products and services covered,
- the detailed specification of the cybersecurity requirements (with a reference to the relevant standards or technical specifications, if available),
- the specific evaluation criteria and methods,
- the level of assurance intended to ensure (i.e. basic, substantial or high).

The adoption of a European cybersecurity certification scheme would trigger the end of the validity of other similar existing schemes, and Member States would be expected to stop the adoption of new national cybersecurity certification schemes for the ICT products and services covered by an existing European cybersecurity certification scheme.

This approach would make it possible for certificates issued through such "European cybersecurity certification schemes" to be:

- compliant with specified cybersecurity requirements;
- more affordable;

- valid and recognised across all Member States, helping to reduce the current market fragmentation.

Manufacturers of ICT products or providers of ICT services would have a free choice in deciding to which conformity assessment body they wish to submit an application for certification.

Conformity assessment bodies would have to be accredited by an accreditation body provided they complied with certain specific requirements. Accreditation would be issued for a maximum of five years and may be renewed on the same conditions, should the conformity assessment bodies meet the requirements.

Member States would be tasked with the monitoring, supervision and enforcement of the Regulation and would have to provide for one certification supervisory authority. The national certification supervisory authorities would carry out the supervision of "compliance of conformity assessment bodies and of certificates issued by conformity assessment bodies established in their territory, with the requirements of this Regulation and the relevant European cybersecurity certification schemes." The same national certification supervisory authorities would be tasked with complaint handling within their jurisdiction, and insofar as appropriate, the investigation thereof and providing information to the complainant of the progress and the outcome of the investigation. An additional task of the national certification supervisory authority would be to cooperate and share information with similar organizations within the EU.

The maintenance and updating of a public inventory of schemes approved under the European Cybersecurity Certification Framework would fall under the responsibility of ENISA. The proposed Regulation defines certification as "the formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria standards and the issuing of a certificate indicating conformance." As mentioned, the scope of the cybersecurity certification would include ICT products and services. Similarly to certification in the area of data protection, cybersecurity certification, too, would remain voluntary.

4.2.3.4. Lessons to be learned for data protection certification

Within the proposed Regulation, certification is recognised as being of particular importance in contributing to increasing trust in security products and services, and realising the single market in this area. However, both the premise (pronounced fragmentation of the ICT

security certification landscape including SOG-IS MRA,[154] national and sectorial schemes, international standards, internal standards etc.) and the approach (centralised) would be different from those provided by the GDPR. In terms of scope of certification, object, and criteria, those are expected to be specified as part of specific "European cybersecurity certification schemes" within the European Cybersecurity Certification Framework, be detailed and refer to standards or technical specifications, where available. In addition, the schemes will reflect the requirements not only of the Cybersecurity Act, but also those of the NIS Directive. The proposed European Certification Framework also acknowledges that during the lifecycle of certification several stages can be distinguished and should be addressed accordingly (from applicable criteria to pricing). The proposed Regulation further acknowledges that a one-size-fits-all approach to certification and signage/labelling would not be appropriate. To that effect, the proposed Act would allow, for example, for different levels of assurance (e.g. from basic to high) and self-certification for the low-assurance products and/or services. It would further distinguish between "regular" criteria applying to commercial products and services, and higher-assurance criteria applying to emergency products and services. According to the proposed Regulation, the formal evaluation of products, services and processes is to be performed by an independent and accredited body against the defined set of criteria standards. A successful assessment results in the issuing of a certificate indicating conformance.

[154] "The SOG-IS agreement was produced in response to the EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC) on common information technology security evaluation criteria." Available: <https://www.sogis.org/> accessed 12 March 2018.

4.3. Assessment guidance of Art. 42(5) GDPR certification criteria

As mentioned in Chapter 2, supervisory authorities are tasked with the approval of certification criteria (Art. 42(5)). This section aims to provide high-level, step-by-step guidance to supervisory authorities when considering approving certain certification criteria, submitted by third parties. As explained, the GDPR does not provide guidance to the DPAs on how to assess the suitability and sufficiency of the certification criteria. A uniform or harmonised assessment methodology is crucial to improve legal certainty when approving certification criteria. In parallel, this section may offer insights to organisations drafting certification criteria for a data protection certification mechanism of Art. 42(1) GDPR.

4.3.1. **Pre-conditions**

The scope of certification and its criteria should be within the competence of the supervisory authority and the scope of the GDPR. The review and approval process should start with a check of whether the proposed certification criteria are within the competence of the supervisory authority, where the criteria are submitted. Competence entails both territorial competence and material competence.[155] For nationally focused certifications the supervisory authority can follow the procedure it has established for verifying competence of complaints handling. In the case of EU-wide certifications, the European Data Protection Board is competent for approval of certification criteria. Apart from the distinction of national or EU-wide certification models – as identified in the previous Chapter –cross-national certifications, namely certifications that target the market of more than one Member States but not all EU Member States, may also be developed. In cases of cross-national certifications, the receiving supervisory authority must establish whether it is the lead supervisory authority and in consultation with the other concerned supervisory authorities proceed with the review and approval of criteria of Art. 42(5) GDPR.

Beyond the territorial competence, the material competence of the supervisory authority should also be established. The material competence refers to both the GDPR material scope and the permitted scope of certifications (and their subsequent criteria) in line with Art. 42 and 43 GDPR. As presented in Chapter 3,[156] certifications may be based on more than one normative sources. The normative sources may range

[155] The Guidelines 1/2018 on certification published by the EDPB adopt the view that the competent supervisory authority is established based on where the certification body aims to offer certification and obtains accreditation. While the country where the certification body offers its services is a clear criterion, the latter (MS of obtaining the accreditation) can be useful only in cases where the DPAs provide accreditation, and not the NABs, which are bound by an obligation to accept granted accreditations from other MS NABs, as established in the Regulation 765/2008.

[156] See p. 50f

from other legal instruments (such as the ePrivacy Directive) to non-legal instruments, such as technical standards. In the case of GDPR related criteria and non-legal instruments[157], the aim of certification is crucial to determine the material competence of the authority. Even though strictly speaking a DPA does not have a mandate to review certification criteria based on technical standards, it will have to do so, if the aim of the certification under approval is to demonstrate compliance with the GDPR in line with Art. 42 and 43. Thus, standards as a normative source of such certifications should be seen as a means to achieve a goal (develop criteria that correspond to the GDPR obligations) and thus falling under the competence of the supervisory authorities.

In the case of multiple legal instruments, the supervisory authority needs to establish its competence for the part that relates to the GDPR (and any other law, within its material competence). For the additional legal instruments, the aim is again crucial. If the aim of the certification under approval is to demonstrate compliance with GDPR provision(s), and the use of additional normative sources aims at enriching the criteria-set, then the DPA should be considered competent. If the aim of the certification under approval is to provide one combined certification demonstrating compliance on the basis of the GDPR and other regulations, for which the DPA is not competent, then the material competence of the DPA should be limited to the GDPR related part. In practice, such cross-legislation comprehensive certifications might be troublesome as different legal regimes and subsequent procedures might be established for approval of the certifications and their criteria. In any case, the supervisory authority should collaborate with any other competent authority to ensure the unity and consistency of both procedures and the outcomes.

The second aspect of establishing the material scope of the supervisory authority is the conditions of Art. 42 and 43 GDPR. As mentioned earlier,[158] the GDPR provides for specific conditions related to the data protection certification mechanisms. Even though, Art. 42(5) provides that the supervisory authority approves the certification criteria, such approval procedure cannot be disconnected from the overall aim and scope of the certification mechanism. The supervisory authority therefore would need to establish that the conditions of Art. 42 and 43 GDPR are met especially in relation to the object of certification (processing activity), the concerned entity (controller or processor), the voluntary nature of the proposed certification, the operation of the certification by an accredited certification body, as described in Art. 43

[157] See "combined model" under Chapter 3 p. 27.
[158] See Introduction.

GDPR. In addition, the scope as comprehensive or single-issue should be established and correspond to the proposed criteria.

4.3.2. **Subject matter of certification**

Once the pre-conditions are fulfilled, the supervisory authorities should focus on the subject matter of the certification mechanism under review. The subject matter is the basis for the formulation of the criteria.

This section provides a concrete set of provisions and corresponding topics that can be the subject of the GDPR data protection certification mechanisms. The main source for the analysis is the text of the General Data Protection Regulation.

Articles 42 and 43 GDPR provide the general framework for certification under the GDPR. However, other provisions in the GDPR point at more specific topics for certification under the umbrella of Art 42 and 43. For instance, Art. 25(3) GDPR talks about 'approved certification mechanism(s) by which a controller can demonstrate compliance with Art. 25. We can thus distinguish between *Comprehensive GDPR schemes*, covering the full breadth of the GDPR, and *Single-issue schemes*, such as Data protection by design certification, that focuses on a particular GDPR sub-topic. We consider the list of single-issue certifications defined in the GDPR not to be exhaustive, but that there is room for certification schemes on other topics as well, e.g. consent by minors. These certifications will also have to adhere to the requirements as required by Art. 42 and 43.

Table 4-4 provides an overview of the GDPR provisions that mention the possibility of certification as a means to demonstrate compliance with (aspects of) the GDPR.

The GDPR explicitly introduces three single-issue topics – Data protection by design and by default, security of processing, and transfer to third countries –, as well as opens the possibility for schemes addressing processors or controllers specifically. This does not, however, clearly define which concrete GDPR provisions are part of such single-issue schemes.[159]

Article	Provision	Text	Topic
24.3	Responsibility of the controller	Adherence to … approved **certification mechanisms** … may be used as an element by which to demonstrate compliance	Demonstrating compliance as responsible controller
25.3	Data protection by	An approved **certification mechanism** … may be used as an element to demonstrate compliance	Demonstrating compliance by implementing

[159] See later in this Chapter, Section 4.3.4

	design and default	with the requirements set out in paragraphs 1 and 2 of this article	appropriate technical and organizational measures for DP by design and default
28.5	Processor	Adherence of a processor to … an approved **certification mechanism** may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraph 1 and 4 of this article.	Use of processors that provide sufficient guarantees to implement appropriate technical and organisational measures. Engagement of a processor by a processor that in turn provide sufficient guarantees to implement appropriate technical and organizational measures.
32.3	Security of processing	Adherence to … an approved **certification mechanism** … may be used as an element by which to demonstrate compliance with … paragraph 1 of this Section.	Appropriate technical and organisational measures to ensure a proportionate risk-equivalent level of security, through: ● Pseudonymisation and encryption. ● The ability to ensure the ongoing CIA and resilience of processing systems and services. ● The ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident. ● A process for regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.
46.2(f)	Transfers	The appropriate safeguards … may be provided for … by an approved **certification mechanisms** … together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards …	Provisions for data transfer to third countries or international organisations.

Table 4-4 Certification subject matter as defined within the GDPR.

4.3.3. **Scope of GDPR comprehensive certifications**

The material scope of GDPR comprehensive schemes can be determined by starting from the total set of GDPR provisions and eliminating procedural provisions, scope-related provisions and provisions targeting other entities than controllers and processors. For example, Art. 1 (subject-matter & objective), 2 (material scope), 3 (scope), 4 (definitions), 23 (Restrictions), 51 (Supervisory authorities) cannot be part of a certification scheme as such addressing the compliance of controllers or processors as they do not involve obligations for said parties. The table below contains an overview of the 'scope' of all GDPR

provisions. The Column 'compliance related' provides all the provisions that, in our view, must be part of a Comprehensive GDPR certification scheme.

GDPR		type			
		mentions certification	compliance related	scope, definitions sec	not related to controller processor
Article 1	Subject-matter and objectives			√	
Article 2	Material scope			√	
Article 3	Territorial scope			√	
Article 4	Definitions		√		
CHAPTER II	**Principles**				
Article 5	Principles relating to processing of personal data		√		
Article 6	Lawfulness of processing		√		
Article 7	Conditions for consent		√		
Article 8	Conditions applicable to child's consent in relation to information society services		√		
Article 9	Processing of special categories of personal data		√		
Article 10	Processing of personal data relating to criminal convictions and offences		√		
Article 11	Processing which does not require identification		√		
CHAPTER III	**Rights of the data subject**				
Section 1	*Transparency and modalities*				
Article 12	Transparent information, communication and modalities for the exercise of the rights of the data subject		√		
Section 2	*Information and access to personal data*				
Article 13	Information to be provided where personal data are collected from the data subject		√		
Article 14	Information to be provided where personal data have not been obtained from the data subject		√		
Article 15	Right of access by the data subject		√		
Section 3	*Rectification and erasure*				
Article 16	Right to rectification		√		
Article 17	Right to erasure		√		
Article 18	Right to restriction of processing		√		
Article 19	Notification obligation regarding rectification or erasure of personal data or restriction of processing		√		
Article 20	Right to data portability		√		
Section 4	*Right to object and automated individual decision-making*				
Article 21	Right to object		√		
Article 22	Automated individual decision-making, including profiling		√		
Section 5	Restrictions				
Article 23	Restrictions				√
CHAPTER IV	**Controller and processor**				
Section 1	*General obligations*				
Article 24	Responsibility of the controller	√	√		
Article 25	Data protection by design and by default	√	√		
Article 26	Joint controllers		√		
Article 27	Representatives of controllers or processors not established in the Union		√		
Article 28	Processor	√	√		
Article 29	Processing under the authority of the controller or processor		√		
Article 30	Records of processing activities		√		
Article 31	Cooperation with the supervisory authority		?		
Section 2	*Security of personal data*				
Article 32	Security of processing		√		
Article 33	Notification of a personal data breach to the supervisory authority		√		
Article 34	Communication of a personal data breach to the data subject		√		
Section 3	*Data protection impact assessment and prior consultation*				

Article 35	Data protection impact assessment		√		
Article 36	Prior consultation		√		
Section 4	*Data protection officer*				
Article 37	Designation of the data protection officer		√		√
Article 38	Position of the data protection officer				√
Article 39	Tasks of the data protection officer				√
Section 5	*Codes of conduct and certification*				
Article 40	Codes of conduct				√
Article 41	Monitoring of approved codes of conduct				√
Article 42	Certification	√			√
Article 43	Certification bodies	√			√
CHAPTER V	**Transfers of personal data to third countries or international organisations**				
Article 44	General principle for transfers		√		
Article 45	Transfers on the basis of an adequacy decision				
Article 46	Transfers subject to appropriate safeguards	√	√		
Article 47	Binding corporate rules		√		
Article 48	Transfers or disclosures not authorised by Union law				√
Article 49	Derogations for specific situations				√
Article 50	International cooperation for the protection of personal data				√
CHAPTER VI	**Independent supervisory authorities**				
Section 1	*Independent status*				
Article 51	Supervisory authority				√
Article 52	Independence				√
Article 53	General conditions for the members of the supervisory authority				√
Article 54	Rules on the establishment of the supervisory authority				√
Section 2	*Competence, tasks and powers*				
Article 55	Competence				√
Article 56	Competence of the lead supervisory authority				
Article 57	Tasks				√
Article 58	Powers				√
Article 59	Activity reports				
CHAPTER VII	**Cooperation and consistency**				
Section 1	*Cooperation*				
Article 60	Cooperation between the lead supervisory authority and the other supervisory authorities concerned				√
Article 61	Mutual assistance				√
Article 62	Joint operations of supervisory authorities				√
Section 2	*Consistency*				
Article 63	Consistency mechanism				√
Article 64	Opinion of the Board				√
Article 65	Dispute resolution by the Board				√
Article 66	Urgency procedure				√
Article 67	Exchange of information				√
Section 3	*European data protection board*				
Article 68	European Data Protection Board				√
Article 69	Independence				
Article 70	Tasks of the Board				√
Article 71	Reports				√
Article 72	Procedure				√
Article 73	Chair				√
Article 74	Tasks of the Chair				√
Article 75	Secretariat				√
Article 76	Confidentiality				√
CHAPTER VIII	**Remedies, liability and penalties**				
Article 77	Right to lodge a complaint with a supervisory authority				√
Article 78	Right to an effective judicial remedy against a supervisory authority				√
Article 79	Right to an effective judicial remedy against a controller or processor				√
Article 80	Representation of data subjects				√
Article 81	Suspension of proceedings				√
Article 82	Right to compensation and liability				√
Article 83	General conditions for imposing administrative fines				√
Article 84	Penalties				√
CHAPTER IX	**Provisions relating to specific processing situations**				
Article 85	Processing and freedom of expression and information				

Article 86	Processing and public access to official documents				
Article 87	Processing of the national identification number		√		
Article 88	Processing in the context of employment		√		
Article 89	Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes				
Article 90	Obligations of secrecy				√
Article 91	Existing data protection rules of churches and religious associations				√
CHAPTER X	**Delegated acts and implementing acts**				
Article 92	Exercise of the delegation				√
Article 93	Committee procedure				√
CHAPTER XI	**Final provisions**				
Article 94	Repeal of Directive 95/46/EC				√
Article 95	Relationship with Directive 2002/58/EC				√
Article 96	Relationship with previously concluded Agreements				√
Article 97	Commission reports				√
Article 98	Review of other Union legal acts on data protection				√
Article 99	Entry into force and application				√

Table 4-5 Scope of GDPR comprehensive certification schemes

4.3.4. **Scope of single-issue certifications**

The number of potential single-issue certification schemes is unknown. As long as the conditions of Art. 42 and 43 GDPR are fulfilled, potentially any topic in the GDPR could give rise to a certification scheme. For instance, the handling of data relating to children, data retention, data security, etc. This makes it impossible to list the relevant provisions for each of the single-issue schemes. However, we can provide an overview of some of the certification mechanisms mentioned explicitly in the GDPR, as well as some of those found during the mapping of existing certifications. It should be noted that single-issue certifications are likely going to be combined with technical standards that complement the GDPR provisions.[160] For instance, a security of processing scheme will likely incorporate criteria derived from, or even directly based on requirements incorporated in the Common Criteria standards.

The table below provides an overview of GDPR provisions that might be included in a data protection by design and by default certification mechanism.[161]

GDPR		
		privacy by design related
CHAPTER II	**Principles**	
Article 5	Principles relating to processing of personal data	√
Article 6	Lawfulness of processing	√
Article 7	Conditions for consent	(√)

[160] See discussion on Chapter 3 on combined models of certification mechanisms built on the basis of both standards and legislation and Chapter 6 on Standards relevant to data protection certification.

[161] In its preliminary Guidelines on certification (p.11) the EDPB shows the intention to make a set of provisions mandatory ("shall be taken into account") to be reflected in the certification criteria. Those provisions are Art. 5, Art. 6, Arts. 12-23, Art. 33, Art. 25, and Art. 32 GPDR.

Article 8	Conditions applicable to child's consent in relation to information society services	(√)
Article 9	Processing of special categories of personal data	√
Article 10	Processing of personal data relating to criminal convictions and offences	√
Article 11	Processing which does not require identification	√
CHAPTER III	**Rights of the data subject**	
Section 1	*Transparency and modalities*	
Article 12	Transparent information, communication and modalities for the exercise of the rights of the data subject	√
Section 2	*Information and access to personal data*	
Article 13	Information to be provided where personal data are collected from the data subject	√
Article 14	Information to be provided where personal data have not been obtained from the data subject	√
Article 15	Right of access by the data subject	√
Section 3	*Rectification and erasure*	
Article 16	Right to rectification	√
Article 17	Right to erasure	√
Article 18	Right to restriction of processing	√
Article 19	Notification obligation regarding rectification or erasure of personal data or restriction of processing	√
Article 20	Right to data portability	√
Section 4	*Right to object and automated individual decision-making*	
Article 21	Right to object	√
Article 22	Automated individual decision-making, including profiling	√
CHAPTER IV	**Controller and processor**	
Section 1	*General obligations*	
Article 24	Responsibility of the controller[162]	√
Article 25	Data protection by design and by default	√
Article 26	Joint controllers	(√)
Article 28	Processor	√
Article 29	Processing under the authority of the controller or processor	√
Article 30	Records of processing activities	√
Section 2	*Security of personal data*	
Article 32	Security of processing	√
Article 33	Notification of a personal data breach to the supervisory authority	√
Article 34	Communication of a personal data breach to the data subject	√

Table 4-6 Data Protection by Design and by Default related provisions for a single-issue data protection certification mechanism

A certification that will be presented to the supervisory authorities for approval needs to incorporate criteria based on the relevant provisions in the GDPR. The tables provided in this section may help the supervisory authority decide whether the subject matter of the certification mechanism submitted for approval covers all the necessary provisions.[163]

4.3.5. **Formulation of criteria**

The next step in assessing the certification criteria relates to the substance of the criteria proposed by the scheme owner: do the criteria allow for the possibility to adequately assess whether or not a particular GDPR obligation is met by an applicant of the scheme? The assessment

[162] Depending on the addressee of the certification: controller or processor.

[163] See also European Data Protection Board, Annex 2 on the review and assessment of certification criteria pursuant to Article 42(5) to the Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 (version for public consultation, adopted 23 January 2019).

of the sufficiency of the criteria has to do with the formulation of the criteria and which ultimately requires an expert assessment of the actual criteria. Useful lessons can drawn from requirements engineering, the study of other examples within the EU law dealing with certification and related literature.

The literature on legal requirements engineering shows that the process of getting from abstract requirements to requirements that can be implemented into a computer system is not a science, but rather an art. It requires expert knowledge and judgment. Similarly, assessing whether a particular criterion in a certification is an appropriate interpretation of one or more GDPR provisions, requires expert judgment. However, there are formal demands that can be specified with respect to the certification scheme that make the work of the expert assessors easier. From this perspective, we distinguish the following demands:[164]

1. **Identification of relevant regulations**
   The certification body should identify what the regulation underlying the certification scheme is. This will typically be the GDPR, but it could also incorporate other sources, such as the e-Privacy Directive or ISO/IEC standards. The certification should make its scope explicit.
2. **Classification of regulations**
   Certifications may follow the structure of the GDPR, but also may be organised based on topics or processes that allows the grouping of criteria that conceptually belong together. For instance, a set of provisions could be tagged with 'security' considerations or 'Data subject access rights'. This allows grouping provisions from various sources.
3. **Prioritisation of Regulations and Exceptions**
   This demand makes explicit another structural aspect. The GDPR contains a hierarchy of norms, where exceptions to obligations may be present in various parts of the regulation. This demand can be seen as a requirement to reorder the various normative criteria in such a way that there are entry requirements for particular blocks of requirements. For instance, if no sensitive data is being processed, then all requirements associated to such processing become irrelevant.
4. **Traceability Between References and Requirements**
   This demand requires the scheme to contain explicit links between source and the normative criteria for the assessment. This allows the supervisory authorities to assess whether all relevant

[164] Derived from Paul Otto and Annie Antón, 'Managing Legal Texts in Requirements Engineering' in Kalle Lyytinen, Pericles Loucopoulos, John Mylopoulos, and Bill Robinson (eds), Design Requirements—Engineering: A Ten-Year Perspectives (Springer Berlin Heidelberg 2009), 374-393.

provisions are covered in the scheme. It also facilitates maintainability and transparency.

5. **Annotation of criteria**
   The criteria will likely not be self-explanatory and hence explanations need to be associated to the various criteria.[165]

The next set of guiding principles can be derived from literature on decision-making and risk management. Keeney and Gregory[166] discuss how to evaluate alternative actions for achieving a certain objective. To describe the consequences of alternatives and make value trade-offs between achieving relatively more or less on different objectives, it is necessary to identify a measure for each objective. They call such measures attributes. The matching of whether an alternative contributes to achieving an objective resembles matching whether a criterion matches a GDPR provision in our case. Keeney and Gregory define five desirable properties: they should be unambiguous, comprehensive, direct, operational, and understandable.
We have elaborated these properties to the following desiderata for certification criteria. Criteria should be:

6. **Accurate and Unambiguous**, meaning that a clear and accurate relationship exists between the criteria and the provisions in the GDPR they cover.
7. **Comprehensive but concise**, meaning that they cover the range of relevant GDPR provisions but the evaluation framework remains systematic and manageable and there are no redundancies.
8. **Direct and results-oriented,**[167] meaning they report directly on the relevant GDPR concepts and provisions and provide enough information that informed value judgments can reasonably be made to assess their values (answers).
9. **Measurable and Consistently Applied to allow consistent comparisons across assessors.**
10. **Understandable**, in that their meaning should be understood consistently by everyone involved.
11. **Practical**, meaning that information can practically be obtained to assess them.
12. **Explicit about Uncertainty** so that they expose differences in the range of possible outcomes (differences in risk) associated with different applications by different assessors.

The ISO/IEC Guide 17 provides guidance for writing standards taking into account the needs of micro, small and medium-sized enterprises.[168]

[165] See for example: Kamara, I, De Hert, P, Van Brakel, R, Tanas, A, Konstantinou, I, Pauner, C, Viguri, J, Rallo, A, García Mahamut, R, Wurster, S, Pohlmann, T, Hirrschman, N, Hempel, L, Kreissl, R, Fritz, F & Von Laufenberg, R 2015, S-T-E-Fi based SWOT analysis of existing schemes: Deliverable 4.3 for the CRISP project. CRISP project. <https://cris.vub.be/files/44198092/CRISP_deliverable_D.4.3_REVISED.pdf> accessed 13 March 2018

[166] Ralph Keeney, Robin Gregory, 'Selecting attributes to measure the achievement of objectives' (2005) 53(1) Operations Research 1.

[167] ENISA, 'Recommendations on European data protection certification' (November 2017).

These guidelines can also be applied the other way around, to assess criteria. On the basis of the Guide, we can derive the following principles to assess certification criteria.

- The criteria should adopt a 'performance approach' whenever possible.
- The certification scheme should have an introduction that provides supportive information that explains what the scheme is about and what the aim of each criterion is.
- The certification scheme should be precise and complete within its scope.
- The certification scheme should avoid costly and complex assessment regimes.
- It should provide simple and cost-effective ways of verifying conformity with the criteria.
- The number of criteria to be assessed should be as limited as feasible.
- The certification criteria should be as clear, logical and as easy to follow as possible.
- The language should be simple enough to be understood by expected assessors.

The final set of guiding principles to assess the certification criteria can be derived from the experience with the New Approach Directives and the drafting of technical standards in general.[169]

13. **Design-based provisions should be transposed into design-based criteria**
14. **Non design-based provisions should be transposed into performance-based criteria**
15. **Performance-based provisions should be transposed into design-based criteria whenever possible**

4.3.6. **High level considerations and outer boundaries**

A supplementary category of principles could be defined next to the suggested certification criteria and accompanying sets of guiding principles for suitability in assessing compliance with the GDPR and

[168] ISO/IEC Guide 17:2016 Guide for writing standards taking into account the needs of micro, small and medium-sized enterprises.
[169] See Case study on New Approach earlier in this Chapter.

described in the previous sections. The supplementary category would address and, insofar as possible, the high-level aims of the GDPR. **The role of such considerations is to determine the principles that need to be respected – and in turn – not be compromised by the scope, criteria or procedural requirements of the certification under approval**.

The literature examined, in the context of this study, revealed similar models combining high-level principles with certification criteria, in particular in areas that were more abstract or had higher social or ethical aims (e.g. in the area of environmental sustainability and healthcare) that are also being pursued by means of certification. [170] Based on these examples, the text of the GDPR could provide the following similar principles:

Overarching Principles		
No	Description - Text (fragment) as potential principle	Correspondence in GDPR – recital number
P1:Protected rights	Respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.	(4)
P2: Fundamental right to protection of persona data	Everyone has the right to the protection of personal data concerning him or her.	(1)

[170] One such case is that of the Forest Stewardship Council that has as mission to "promote environmentally sound, socially beneficial and economically prosperous management of the world's forests". The FSC certification scheme thus defines not only a number of certification criteria (a total of 57 criteria in 2018), but also ten principles which, together provide the foundation for all international forest management standards. The ten FSC Principles for Forest Stewardship have to be met by all those aiming to start the certification process, and include: compliance with all applicable laws, regulations and nationally-ratified international treaties, conventions and agreements; maintenance or enhancing of the social and economic wellbeing of workers; identification and respect of Indigenous Peoples' legal and customary rights; efficient management of the range of products and services to maintain or enhance long term economic viability and the range of environmental and social benefits; commitments to maintain, conserve and/or restore ecosystem services and environmental values of the Management Unit, and avoid, repair or mitigate negative environmental impacts; availability of a management plan consistent with its policies and objectives and proportionate to scale, intensity and risks of its management activities; commitment to maintain and/or enhance the High Conservation Values in the Management Unit through applying the precautionary approach, etc. "The Forest Stewardship Council A.C. (FSC) was established in 1993, as a follow-up to the United Nations Conference on Environment and Development (the Earth Summit at Rio de Janeiro, 1992) with the mission to promote environmentally appropriate, socially beneficial, and economically viable management of the world's forests." "FSC is an international organization that provides a system for voluntary accreditation and independent third-party certification." https://ic.fsc.org/en/document-center/id/59 The Forest Stewardship Council (FSC), 'Principles and Criteria for Forest Stewardship', available <https://ic.fsc.org/en/document-center/id/59>; ibid, 'The 10 rules for responsible forest management' available <https://ic.fsc.org/en/what-is-fsc-certification/principles-criteria/fscs-10-principles> accessed 12 March 2018.

P3: Non-discrimination	The protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data.	(2)
P4: Protection of natural persons	The protection (…) should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data	(14)
P5: Facilitate control of the individuals over their data	Natural persons should have control of their own personal data.	(7)
P6: Serve – or otherwise – not compromise legal certainty	Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.	(7)
P7: Limitations to data protection should be in line with the Charter	The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.	(4)
P8: Technology neutral approach	The protection of natural persons should be technologically neutral and should not depend on the techniques used.	(15)
P9: Principles of data protection should be respected	The principles of data protection should apply to any information concerning an identified or identifiable natural person.	(26)

Table 4-7 Overarching principles for approval of certification criteria

The assessment criteria should overall be in line with the above fundamental principles underlying the GDPR and the protection of personal data. Any approved set of criteria should be in line with the above principles.

A last set of principles and high-level considerations underlying the certification criteria submitted for approval can be derived from the ISO/IEC 17007 standard.[171] The principles are:

- Principle 1: Separation of specified requirements for the object of conformity assessment from specified requirements related to conformity assessment activities
- Principle 2: Neutrality towards parties performing conformity assessment activities
- Principle 3: Functional approach to conformity assessment[172]
- Principle 4: Comparability of conformity assessment results

The above principles are useful for both drafters of criteria and supervisory authorities assessing criteria.

4.3.7. **Discussion**

In this section, we provided guidance to supervisory authorities for their task to approve certification criteria (Art. 42(5) GDPR). The study from other fields offered lessons for the formulation of the criteria, the goals to be achieved with the certification mechanism, and concrete controls in technical standards. The practice of appointing one or more experts such as the New Approach Consultants in the case of NLF was also examined. The further analysis of technical standards for drafting normative documents appropriate for conformity assessment activities reveals a number of best practices. The supervisory authorities will need to use all the guidance and knowledge from other fields and especially technical standards to leverage the assessment of certification criteria in the data protection field. Ultimately, the supervisory authorities will work with the GDPR as main point of reference and framework, which will be the main source of what can and cannot be approved: its protected rights and freedoms, the subject matters, and the specific conditions of Art. 42 and 43 GDPR will be the main point of reference for the supervisory authorities.

[171] ISO/IEC 17007: 2009 Conformity assessment – guidance for drafting normative documents suitable use for conformity assessment.
[172] This principle entails following the functions of selection, determination, review and attestation, and surveillance of granted certification (see following section of this Chapter Section 4.4).

4.4. Certification process

This section describes the process that a data controller or processor applying for certification must successfully complete.

4.4.1. GDPR certification process and EN ISO/IEC 17065:2012 requirements

The standard is international in scope and sets out "requirements for the competence, consistent operation and impartiality of product, process and service certification bodies" for third-party conformity assessment activity.[173]

The stated aim of the ISO/IEC 17065:2012 certification is to provide assurance of compliance with the requirements of the standard, the competence and impartiality of the process establishing said compliance and thereby create confidence and trust that the standard's requirements (and where applicable, additional requirements of the certification scheme within which it is applied) are met.

The standard is primarily intended for third-party certification, but can also be used for first- and second party conformity assessment and is aimed at broad constituencies, including:

- the clients of the certification bodies;
- the customers of the organizations whose products, processes or services are certified;
- governmental authorities;
- non-governmental organizations; and
- consumers and other members of the public.

The requirements are defined as general conditions, which, in some cases, can double as accreditation, peer assessment or designation criteria. The requirements, whatever the purpose for which they are used, must be considered in their totality and, where necessary, be supplemented by additional requirements (such as those specific for health and safety).

The following building blocks of the certification process should be taken into account:

- For the purpose of a first-time application for certification or for the purpose of renewing a certification or for the purpose of any modifications thereof (such as for expanding or restricting the scope of an existing certification), the certification body should be provided with or be able to gain access to all necessary information. This is also required by Art. 42 of the GDPR.

[173] See Glossary in Annex 1 (separate document).

- The certification body should have a process in place, as well as the necessary expertise to review the applications under existing certification mechanisms. In addition, the certification body should have a process in place, as well as the necessary expertise to review new certification mechanisms or new types of data processing.
- The certification body should have a process in place, as well as the necessary expertise to evaluate data processing activities.
- The evaluation conducted by the certification body should be documented and any non-conformities should be communicated to the applicant. Upon notification, the applicant decides if he wants to address potential non-conformities and continue with the certification process.
- The certification body should have a process in place, as well as the necessary expertise to review the results of evaluation process. A positive outcome of the review results in a positive certification decision.
- The activities of evaluation and decision are separate and performed by different experts. All activities and their outcomes are documented and results are kept confidential.
- The certification body should take responsibility and retains authority for all decisions described above. In the case of mutual recognition of certification mechanisms, a certification body might be able to have to assume responsibility for a prior evaluation performed by another certification body.
- Certification decisions are fully and formally documented, including registration in a public directory of certified data processing.
- Following a positive certification decision, the certification body should have a process in place, as well as the necessary expertise to perform various follow-up activities, as required. Such activities could include surveillance, changes in the scope of certification, changes in the type and range of data processing activities performed by the applicant, suspension, withdrawal, reinstating, or termination of certifications, etc.
- The certification body should have a process in place, as well as the necessary expertise to accommodate, evaluate and follow up on complaints and appeals related to its certification activities.
- The certification body should have a management system in place able to accommodate adequate performance.

4.4.2. **Lessons from existing certifications**

4.4.2.1. Conformity assessment

Explanation

The conformity assessment process (hereinafter CAP) represents a subset of the certification process aiming to "demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled" read the ISO.[174]

The CAP is a systematic examination done according to an established methodology, validating the match between some observed values and criteria included in the certification requirements. It expects an exact match between them even though it may accept some predefined offsets. The CAP may conclude that there was non-conformity even though it primarily aims to demonstrate the conformity.

The general picture with respect to the conformity assessments carried out by the certification bodies is that the majority of the analysed certifications require an onsite inspection in addition to a document review.

Some of the certifications conduct technical tests in addition to documentation review or onsite inspections. A small number of the analysed certifications conducts the conformity assessment via a documentation overview and a questionnaire. Some experts[175] argue that a documentation review already offers a good insight on a company's conformity while onsite inspection appears time consuming and disturbs the activity of companies being audited.

In all, certification schemes follow a *combined assessment model* combining onsite inspections and/or technical tests with a documentation review including, in some schemes, a preliminary questionnaire submitted to the applicant.

As for the auditors, most schemes are using only internal auditors, while fewer schemes are using both internal and external auditors. A smaller number of certification schemes use only external auditors, which are competent in the scope of the certification scheme. An external auditor can be an individual auditor or an audit company. All the schemes that use external auditors require prior 'accreditation' of these external auditors. In all cases, the process is managed by the scheme owner. Once accredited, the external auditors directly manage the contractual relationships with certification applicants. The external auditors conducting the audit are required to provide an audit report to

[174] Sub-article 2.1 EN ISO/IEC 17000:2004.
[175] Ustaran, E. et Al. (2017) European Data Protection: Law and Practice. IAPP Publication.

the applicant at the end of the conformity assessment process. The report is then submitted to the scheme owner for approval and, if conclusive, certification issuance.

	Conformity assessment models
Internal auditors The conformity assessment process is only done by auditors employed by the scheme owner	CNIL - SafeBox CNIL - ASIP Santé IKeepSafe TRUSTe APEC CBPR TUV Italia - ISO/IEC 27001 certification
Internal or external auditors The conformity assessment process is done by auditors employed by the scheme owner or by external auditors 'accredited' by the scheme owner	BSI - BS 10012 BSI - ISO/IEC 27018 E-Privacy App ISDP 10003:2015 Privacy Seal MYOBI Privacy-Audit-Proof
External auditors The conformity assessment process is only done by external auditors 'accredited' by the scheme owner	Europrise
Combined assessment model The conformity assessment process is based on a documentation review combined with an on-site inspection or/and technical tests	BSI - BS 10012 BSI - ISO/IEC 27018 Datenschutzaudit beim ULD E-Privacy App EuroPriSe IKeepSafe ISDP 10003:2015 JIPDEC PrivacyMark System Privacy by design certification Ryerson Privacy Seal MYOBI Privacy-Audit-Proof TRUSTe APEC CBPR TUV Italia - ISO/IEC 27001 certification

Questionnaire based The conformity assessment process is based on a questionnaire filled by the applicant	CNIL - SafeBox CNIL - ASIP santé

Table 4-8 Conformity assessment models of analysed certifications

4.4.2.2. Issuance of certification

Explanation

A certification is commonly found as an attestation in writing[176] issued by the third-party body in charge of the conformity assessment. The full process is sometimes licensed to a third-party body that is managing the assessment and certification issuance processes under the monitoring of the scheme owner.[177]

The issuance of the attestation of conformity can be disconnected from the conformity assessment process and managed, separately, by the scheme owner when the conformity assessment has been delegated to external auditors.

The attestation, in writing, frequently comes with, but not always[178], a visual sign called a seal, label, mark or certification. The scheme owner licenses the right to affix the seal to the certified organization which can place it on its products and documentation under the condition that the certified entity maintains its conformity during the period of validity.

Certification is, by design, time limited and issued for a period of time that may vary from one scheme to another. The certification validity period can span any period, from 1 to 3 years.

All the schemes include a review stage of the audit report before issuing the certification, as also provided in the ISO/IEC 17065 standard. This is also due to the fact that a significant number of the certification schemes are delegating the audit process to external auditors. The

[176] The ISO/IEC defines a certification as a third-party attestation (related to products, processes, systems or persons). See Glossary in Annex I.
[177] The third-party body in charge of the process on behalf of the scheme owner can be accredited. The ISDP 10003:2015 manages such a licencing process.
[178] A seal is commonly issued with customer facing certification schemes. The seal is less common in the supply chain certification.

assessment and issuance processes are then managed by different entities.
The Privacy Seal MYOBI follows a different model, since once trained and approved, the internal Data Protection Officer is entitled to certify its own organization.
When the certification body is a public authority, the authority issues a certification that is a public administration decision. The issuance of certification (or the rejection thereof) can be challenged in administrative courts. All the analysed schemes except for one[179] awards a seal along with the attestation of conformity.
On average, the analysed certification schemes have a validity period that is less than 3 years and some of them have a validity period of one year. Usually, a short validity period relates to the certification fields that are impacted by technological advancements. However, it should also be noted that a short validity period raises the costs and becomes an affordability issue for companies, especially SMEs that are supposed to fully reassess their conformity every year.[180]

	Validity period models
3 years The validity period is consistent with the maximum validity period set in Article 42 GDPR	BSI - BS 10012 BSI - ISO/IEC 27018 CNIL - SafeBox CNIL - ASIP Santé Datenschutzaudit beim ULD JIPDEC PrivacyMark System Privacy by design certification Ryerson TUV Italia - ISO/IEC 27001 certification
2 years Validity period of the scheme	E-Privacy App EuroPriSe
1 year Validity period of the scheme	IkeepSafe Privacy Seal MYOBI Privacy-Audit-Proof TRUSTe APEC CBPR

Table 4-9 Certificate validity period of analysed certifications

4.4.2.3. Monitoring (surveillance)

Explanation

The certification is conditional on the upholding of the certification by maintaining conformity during the period of validity. The body issuing the

[179] CNIL - ASIP Santé does not issue a seal insofar as the scheme focuses on the suppliers and is not end-user facing.
[180] This remark was also made during the Workshop organised by the consortium in January 2018 in Brussels (See Annex 6 – separate document). Nevertheless, the GDPR already determines the maximum validity period of issued certifications to three years.

certification, once it has conformed to the EN ISO/IEC 17065 should monitor the conformity of the certified entities in order to maintain the certification and preserve the confidence in the scheme.[181]

All of the certifications that were analysed monitor the conformity of the certified entities after the issuance of the certification.
There are three identified models of monitoring:

A. Monitoring by the certification scheme owner

a. Periodical reviews by the certification scheme owner

A percentage of 75% of the schemes monitor their clients' compliance through periodical reviews done by the scheme owner. In certain schemes, the periodical review is aligned with the renewal process. One relies on a voluntary statement issued by the certified body confirming its conformity or declaring the changes that occurred during the validity period. [182]

b. Random checks by the certification scheme owner

A smaller number of the certification schemes occasionally perform random checks in addition to the periodical review.

B. Monitoring process by a third party

A percentage of 40% of the schemes delegate the monitoring process to a third party. A small number of the schemes rely on audits conducted by DPAs. Another scheme[183] delegates the monitoring to the external auditors that performed the initial conformity assessment. Privacy Seal MYOBI delegates the monitoring to the internal Data Protection Officer trained and approved by the scheme owner.

	Monitoring models
Periodical review The scheme owner monitors certified bodies through periodical and scheduled reviews	E-Privacy App EuroPrise JIPDEC PrivacyMark System Privacy by design certification Ryerson Privacy-Audit-Proof TRUSTe APEC CBPR
Periodical review with random check The scheme owner monitors the certified bodies through periodical and scheduled reviews and	BSI - BS 10012 BSI - ISO/IEC 27018 IKeepSafe ISDP 10003:2015 TUV Italia - ISO/IEC 27001 certification

[181] The Italian law even authorizes certification recipients to sue the scheme owner in case of negligence in its monitoring task. See Priscilla Pettiti, 'Il marchio collettivo. Commento alla nuova legge sui marchi' (1994) 9-10 Rivista del Diritto Commerciale e del Dirritto generale delle Obbligazioni 621.
[182] Privacy by design certification by Ryerson.
[183] EuroPrise.

random checks	
Random check The scheme owner monitors the certified bodies through the random checks done by the data protection authorities	CNIL - SafeBox CNIL - ASIP Santé Datenschutzaudit beim ULD
Delegated monitoring The scheme owner delegates the monitoring of certified bodies	CNIL - ASIP Santé E-Privacy App EurPprise Privacy Seal MYOBI

Table 4-10 Conformity monitoring models of analysed certifications

4.4.2.4. Renewal

Explanation

Certification is granted for a limited time and is renewable, provided that the certified entity maintains its conformity to the criteria and requirements of the certification. The renewal process is voluntary and must be requested by the certified entity before the end of the validity period. The certification body may require a full or partial reassessment, only checking, in the latter case, the changes in the certified entity's compliance during the validity period.[184]

All the schemes except for one[185] are renewable under the same conditions as the initial conformity assessment, and all of them require a full reassessment process from the candidate for the renewal. EuroPrise requires a check regarding the changes in the scope of the initial certification.

	Renewal models
Full reassessment The certified body must undergo a full reassessment of its conformity to renew the certification	BSI - BS 10012 BSI - ISO/IEC 27018 CNIL - SafeBox CNIL - ASIP Santé Datenschutzaudit beim ULD E-Privacy App IKeepSafe ISDP 10003:2015 JIPDEC PrivacyMark System Privacy by design certification Ryerson Privacy Seal MYOBI Privacy-Audit-Proof TRUSTe APEC CBPR TUV Italia - ISO/IEC 27001 certification
Partial reassessment The certified body must only assess the changes occurred in its compliance to	EuroPriSe

[184] See Glossary in Annex I (separate document).
[185] EuroPrise.

renew the certification

Table 4-11 Renewal models of analysed certifications

4.4.2.5. Sanction policy

Explanation

The sanction policy organises the different penalties a certification body can impose on the certified entity that no longer complies with the conditions for issuing the certification.

The sanction policies presented below cover only those applying in the course of the certification process.[186]

All of the analysed schemes have a sanction policy. The majority have included the sanction policy in their contractual agreement with the certified entity.
The sanction policies define a gradual sanction approach with a suspension of the certification, sometimes made public,[187] followed by withdrawal of the certification, in case the non-compliant certified entity did not take action to fully mitigate the non-conformity within a pre-determined period of time.
Several certification schemes have established a time limit to the certified entities for correcting the non-compliance before the certification is withdrawn, ranging from 3 and 6 months.

4.4.2.6. Complaints and dispute resolution

Explanation

The following section discusses the claim and dispute resolution processes insofar as both processes are closely related.

The claim handling process describes the process and conditions to lodge a claim with the scheme owner and the associated resolution process.
The dispute resolution process encompasses the processes used to resolve a dispute occurring between the scheme owner, the certified body and, eventually, the end user.
There are traditionally two types of dispute resolution processes: adjudicative and out-of-court proceedings. The adjudicative processes, with litigation and arbitration, allows the court to determine the outcome. The out-of-court proceedings, also called consensual processes, includes mediation, conciliation, or negotiation.

[186] The sanction policy for non-conforming to the conditions of certification should not be confused with infringements of the GDPR. The certification body imposes sanctions based on the bilateral contractual agreement with the certified entity.
[187] BSI 10012, BSI 27018.

The majority of the analysed certification schemes internally manage the claim handling process and 20% of them[188] offer a dedicated section on their website to lodge a complaint online.
One finds two models in the dispute management process. 80% of the schemes manage the dispute resolution internally before using any adjudicative process. 20% of the schemes directly refer to court proceedings.[189] One scheme offers the option to complainants to use arbitration.[190] Several schemes describe the claim handling and dispute resolution processes in their contractual documentation. 20% do not describe such processes to the extent that they are schemes belonging to a DPA.[191] Privacy Seal MYOBI, delegates the dispute resolution to the internal DPO.

4.5. Discussion

The certification process stages are determined in the GDPR and may be complemented by the stages identified in the ISO/IEC 17065 standard.[192] However, beyond generic provisions, one should look at existing certifications to identify best practices. Issues such as dispute resolution management, techniques of monitoring granted certifications, and sanction policies are crucial for the developing trustworthy data protection certification mechanisms. What may be considered as best practice, will differ according to the scope and subject matter of each data protection certification mechanism. This does not mean however that the mechanisms to ensure the integrity and quality of the certification should be determined and judged on a case by case basis. Supervisory authorities should use a catalogue of issues to be addressed by the certification mechanism under review.

[188] EuroPriSe, Privacy by design certification Ryerson, TRUSTe APEC CBPR.
[189] CNIL Safebox, CNIL - ASIP Santé.
[190] Privacy Seal MYOBI is using arbitration in front of Stichting Geschillenoplossing Automatisering (SGOA) in The Hague on the basis of the arbitration rules or have the case tried before a Dutch Court.
[191] CNIL Safebox, CNIL - ASIP Santé.
[192] See Introduction p. 14.

5. Accreditation

5.1. Introduction and methodological approach

The International Accreditation Forum conducted a survey in 2012, which showed that businesses are generating significant benefits and added value from accredited certification. Among the benefits the survey respondents reported the improvement of internal processes of an organisation, regulatory compliance, and a positive effect on revenue.[193] In the case of the GDPR, accreditation is mandatory. However, Member States have the flexibility to choose the accreditation model applicable to the national jurisdiction, in line with Art. 43 GDPR. The flexibility to choose among different accreditation models, in combination with the novelty of the accreditation models in the field of personal data protection in comparison to accreditation of certification bodies offering services in other fields, invites research on the issues and the open questions at stake.

This Chapter discusses the different accreditation models for certification bodies that provide certification services, based on certification criteria approved by supervisory authorities. The Chapter elaborates on the three models in Art. 43(1) GDPR: a. accreditation by the National Accreditation Bodies, with additional requirements by the competent supervisory authorities b. accreditation by the supervisory authorities (Data Protection Authorities) and c. accreditation by both the National Accreditation Bodies and the competent national supervisory authorities. In each model, different potential roles of the stakeholders involved (National Accreditation Body, supervisory authority, certification body) are identified.

The Chapter also analyses the Regulation 1025/2012 and the additional requirements, specific to data protection, provided for in Art. 43 GDPR. In addition, the analysis benefits from lessons from current practices of National Accreditation Bodies and data protection authorities of the Member States, European and international accreditation fora. The research in this Chapter is based on literature review, legal analysis, and empirical research, namely a survey addressed to targeted recipients and two roundtable on accreditation in the framework of a workshop organised by the consortium in January and April 2018 in Brussels.[194] The result of this Chapter is a comprehensive overview of

The authors would like to thank Maureen van den Wijngaart (Raad van Accreditatie) and Shazade Jameson (TILT) for their feedback on the survey questionnaire.

[193] International Accreditation Forum, 'The value of accredited certification. Survey Report' (May 2012), p.11f.

[194] See Annex 6 (separate document).

the models of accreditation of certifying bodies in data protection certification as well as a set of accreditation requirements that are (to be) used in this context.

5.2. Models of accreditation based on Art. 43 GDPR

Article 43 GDPR concerns certification bodies conducting certification in line with the GDPR. Not every certification body may certify in line with Art. 43 GDPR. Unlike the usual practice in other fields, as for example information security, accreditation in the case of the data protection certification mechanisms is mandatory, in the sense that a non-accredited certification body is not allowed to certify data controllers or processors in line with Art. 42 GDPR. The GDPR regulates how certification bodies shall be accredited.

Art. 43(1) provides that Member States shall ensure that certification bodies are accredited. Each Member State shall decide which of the three models will be followed in its jurisdiction. The Regulation allows for three potential models, which are briefly presented in the following sections.

5.2.1. Accreditation model 1: Data Protection Authorities as Accreditors

The supervisory authority will accredit certification bodies that apply for accreditation and fulfil the necessary conditions. The competence of the DPA or Information Commissioner is determined on the basis of Art. 55 or 56 GDPR.[195] In case of the European Seal or for reasons of consistency, the EDPB may also approve the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies referred to in Article 43.[196]

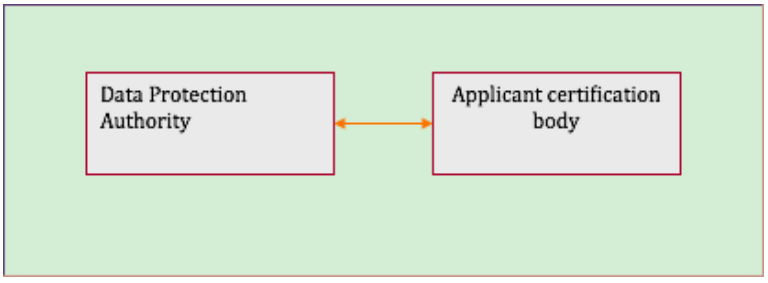


Figure 5-1 Actors of GDPR accreditation of model 1

[195] Art. 55 GDPR refers to the Competence of supervisory authorities and Art. 56 refers to the Competence of the lead supervisory authority.
[196] Art. 70 (1)(p) GDPR (after the Corrigendum to the Regulation 2016/679).

5.2.1.1. Roles of involved actors

This model involves two types of actors: the supervisory authority and the certification body. A certification body that wishes to provide services on GDPR certification mechanisms needs to apply to the supervisory authority in order to be accredited. The competent supervisory authority should be determined the rules of Art. 55 to establish competence: the supervisory authority is competent for the territory of its own Member State, where the certification body has its main or single establishment.[197] Where the certification body intends to offer services in more than one Member States, the rules of Art. 56 GDPR should be used to determine the lead supervisory authority. The (lead) supervisory authority at national level (DPA) has two main responsibilities. The first is to draft and publish criteria for accreditation of the certification body.[198] The second main task is to conduct the accreditation process of the applicant certification body.[199] In the case of the European Data Protection Seal, applicant certification bodies are accredited on the basis of accreditation requirements approved by the European Data Protection Board.

5.2.1.2. Procedures and accreditation safeguards

The GDPR does not provide details on the process of accreditation when conducted by a supervisory authority. The GDPR however provides a number of accreditation safeguards and requirements that need to be fulfilled by the applicant certification body. The safeguards relate to both procedural and organisational issues of the applicant certification body, including the integrity and expertise of the body. The applicant certification body, prior to applying for accreditation to the DPA, needs to have established procedures for issuing certifications, seals and marks, conducting periodic review and withdrawal of data protection certifications. In addition to those procedures, the applicant certification body needs to have complaints mechanisms in place to handle claims of infringement and for the implementation of the certification. The applicant needs to make those procedures publicly available to the data subject in a transparent way.

In addition, the applicant needs to be independent from the data controllers and processors who are applying for certification. The independence of the applicant certification body needs to be demonstrated, which implies that the applicant has a good track record of reliable certifications prior to the application for accreditation. The tasks and duties of the applicant certification body should not result in a

[197] Art. 43(1) GDPR.
[198] Art. 57 GDPR.
[199] Art. 57(1)(q) and 58(3)(e) GDPR.

conflict of interests.[200] An assessment of what is sufficient in terms of the independence and potential conflict of interest might be challenging. Art. 43(2) provides that both qualities need to be demonstrated to the *satisfaction of the supervisory authorit*y. This is a rather vague concept and certainly does not offer much information to the applicant as to what would be the standard required to satisfy the data protection authority. This is an area where guidance and collaboration of the DPAs among each other is critical for a harmonised practice throughout the EU Member States. Furthermore, the applicant certification body needs to commit to respect the approved criteria of the certifications, in line with Art 42(5) GDPR.

Finally, the applicant certification body needs to have demonstrated expertise in the subject matter of the certification. Expertise in relation to the subject matter is crucial for the success of the data protection certification mechanisms: the certification body is the body that examines whether a controller or processor processed personal data in line with the approved criteria of certification. Certification bodies need to have proven track records of experience and expertise in the field of data protection in general, but also in the specific field or sector of application where the controller or processor is active. That means that if a certification body wishes to provide services to controllers and processors active in the healthcare sector, the certification body needs to be accredited that it has sufficient expertise in personal data processing in that sector.[201]

5.2.1.3. Supervision and re-accreditation

Revocation of accreditation is possible by the DPA in two cases: a. When the conditions for granting accreditation are not, or are no longer, met.[202] This power of the DPA requires close supervision of the issued accreditations and on spot audits or sample examination of issued certification by the accredited certification body to verify that the accreditation conditions are respected. b. when actions taken by a certification body infringe the GDPR. This generic condition binds with the integrity safeguards discussed in the previous section. A certification body needs itself to be a good example, before being in the position to certify others that they process data in line with the criteria based on the GDPR.

[200] Art.43(2)(e) GDPR.
[201] The certification criteria of the certification mechanism need to be known before the accreditation takes place, to ensure that the applicant (for accreditation) certification body has the expertise to certify controllers or processors against the specific type of certification criteria. See EDPB Guidelines 1/2018 p. 9.
[202] Art. 43(7) GDPR.

The GDPR provides that accreditation is valid for five years[203] and may be renewed on the condition that the certification body continues to fulfil the accreditation requirements.

5.2.1.4. Legal effect

The granting of an accreditation certification by the Data Protection Authority is an administrative act with binding legal effect. In principle, decisions on accreditation could be challenged in front of the competent national courts, as is the case with every administrative act of the national data protection authorities. Apart from any provisions in national (administrative) law, the GDPR provides the right to any natural, or in this case, legal person to an effective judicial remedy against a legally binding decision made by an authority concerning them.[204]

5.2.2. Accreditation model 2: National Accreditation Bodies as Accreditors, with the support of Data Protection Authorities

The National Accreditation Body of each Member State provides accreditation to certification bodies, in accordance with the EN ISO/IEC 17065:2012 conformity assessment standard and additional requirements provided by the competent supervisory authority or the European Data Protection Board.[205]

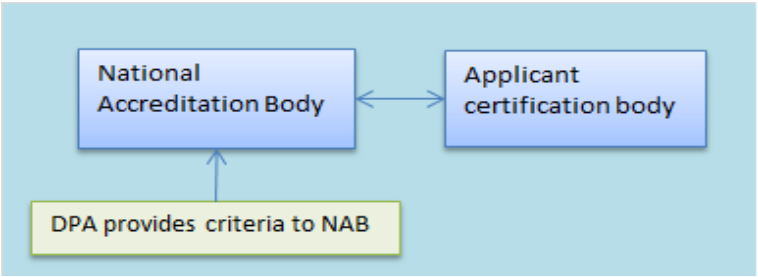


Figure 5-2 Actors of GDPR accreditation of model 2

5.2.2.1. Roles of involved actors

This model includes three actors: the applicant certification body, the National Accreditation Body and the Data Protection Authority. The main actors are the NAB and the applicant certification body. Any certification body interested to offer services based on the GDPR certification mechanisms of Art. 42 and 43 GDPR, needs to apply for accreditation to

[203] Art.43(4) GDPR.
[204] Art. 78 GDPR.
[205] Art. 43(1)(b), Art. 43(3) GDPR, Art. 63 GDPR.

the National Accreditation Body, which is established in accordance with the Regulation 765/2008. In principle, each Member State has one National Accreditation Body.[206] The Accreditation Regulation uses the criterion of establishment, to determine which National Accreditation Body is competent.[207] Thus, the NAB of the Member State where the applicant certification body has its establishment is the competent authority for accreditation in this Model. The competent DPA is determined in line with Art. 55 and 56 GDPR.[208] In practice, if a NAB in a Member State does not provide specific accreditation services, which then needs to be provided by a NAB of another Member State, or where the rule of lead DPA is applied, there might cases where the NAB of one Member State is competent together with a DPA from another state. Such cases could end up being challenging in terms of the collaboration of the two authorities but also for the applicant certification bodies.[209] The DPA does not directly participate in the accreditation process, but is tasked to provide the National Accreditation Body with "additional requirements". Presumably those additional requirements refer to the data protection field. The exact focus and type of such requirements is however rather vague.

5.2.2.2. Procedures and accreditation safeguards

In terms of safeguards, the provisions of Art. 43(2) GDPR on independence, expertise, and others apply to this model as well.[210] In addition, the accreditation process and safeguards are mandated by the Regulation 765/2008 to which National Accreditation Bodies are subject. National Accreditation Bodies evaluate applications by conformity assessment bodies (in the GDPR case: certification bodies), and in specific NABs assess whether a conformity assessment body is competent to carry out a specific conformity assessment activity.[211] In the case of the GDPR, the specific conformity assessment activity refers to the certification of controllers and processors based on approved certification criteria. The successful evaluation leads to the issuance of an accreditation certificate by the NAB. In addition to the requirements imposed on the NAB by Regulation 765/2008, the GDPR provides that the NAB needs to follow the requirements of a conformity assessment

[206] An exception is established in Art. 4(2) of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, OJ L 218/30.
[207] Art. 7 ibid.
[208] In practice, if there is no National Accreditation Body or where the rule of lead DPA is applied, there might be cases where a NAB of one Member State is competent together with a DPA from another state. Such cases may end being challenging in terms of collaboration of the two authorities but also for the applicant certification bodies.
[209] This practical challenge is more obvious in the third model, where both the DPA and the NAB provide accreditation.
[210] See previous section on Model 1 for analysis.
[211] Regulation 765/2008 setting out the requirements for accreditation.

technical standard.[212] The ISO/IEC 17065: 2012 standard[213] provides a broad range of requirements on issues such as:

- Legal and contractual matters, including liability
- Impartiality, non-discrimination, confidentiality
- Organisational and structural issues
- Evaluation process, decision, documentation and surveillance
- Complaints and appeals

The ISO/IEC 17065:2012 standard applies to certification of products, processes and services[214], but in the case of the GDPR data protection certification mechanisms, the object of certification should be read as "processing", as defined in Art. 2 GDPR.[215]

5.2.2.3. Supervision and re-accreditation

Apart from the assessment and evaluation phase, NABs are also tasked to monitor the accredited certification bodies. In cases where an accredited certification body is no longer competent to carry out the certification for which it has received the accreditation certificate, the NAB should take appropriate measures to restrict, suspend, or withdraw the accreditation.[216] Such measures can also be enforced by the NAB when the certification body has committed a serious breach of its obligations. Usually, the obligations of the accredited certification body are determined in a contractual arrangement between the NAB and the certification body. In addition, revocation of the accreditation should also take place when the accredited certification body infringes the GDPR.[217] Accreditation is valid for maximum of five years and may be renewed.

5.2.2.4. Legal effect

Accreditation is granted by the National Accreditation Bodies, which may be either public or private bodies. In the latter case, they need to be granted with formal recognition by the Member State that they conduct the exercise of the accreditation activity as public authorities.[218] The NABs also need to operate as non-for-profit organisations. The Accreditation Regulation provides that procedures against decisions of NABs and legal remedies against accreditation decisions shall be established by the Member States.

[212] See more on the static reference to the technical standard in: Irene Kamara, Paul De Hert, 'Data protection certification in the EU' (2018).
[213] See Chapter 4 p. 102 for thorough analysis of the ISO/IEC 17065:2012 standard.
[214] See Scope of ISO/IEC 17065:2012.
[215] See Chapter 2 of the Report.
[216] Art. 5(4) Regulation 765/2008 setting out the requirements for accreditation.
[217] Art. 43 (7) GDPR.
[218] Art. 4(5) Regulation 765/2008 setting out the requirements for accreditation.

5.2.3. Accreditation model 3: National Accreditation Bodies and Data Protection Authorities as Accreditors

In this accreditation model, both the National Accreditation Body and the competent supervisory authority conduct the accreditation process, presumably each of them in their field of competence and expertise.[219] This model is not elaborated on the text of the GDPR, but is derived from the wording ("both of the following").[220]

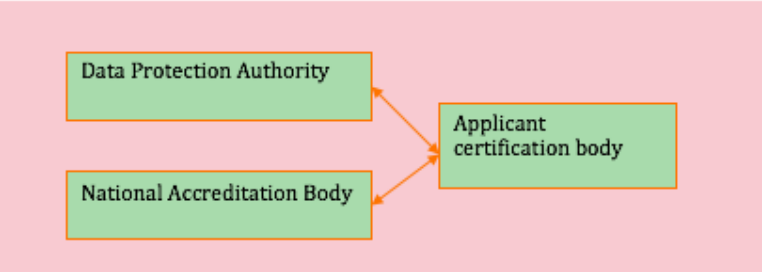


Figure 5-3 Actors of GDPR accreditation of model 3

5.2.3.1. Roles of involved actors

There are three main actors in this model: the National Accreditation Body, the DPA and the applicant certification body. This model implies a joint accreditation process. Since both NABs and DPAs are conducting a part of the accreditation process, in practice the authorities need to establish the procedures for collaboration, and guidance to applicants on issues such as where to apply, who provides the accreditation certificate and who monitors and re-news the accreditation. None of these matters is regulated in the GDPR. In practice, it would be logical if the evaluation by the NAB would focus on the procedural, organisational, and integrity requirements, as prescribed in the Accreditation Regulation and the ISO/IEC 17065:2012 standard. Followed by the evaluation by the DPA, which would focus only on the data protection competence and expertise of the applicant certification body.

5.2.3.2. Procedures, accreditation safeguards and supervision

In terms of procedures and safeguards, all the conditions of Art. 43(2) GDPR in combination with the Accreditation Regulation and the technical standard ISO/IEC 17065:2012 would apply. Again, coordination of the both authorities is necessary to establish supervision procedures.

[219] See https://services.parliament.uk/bills/2017-19/dataprotection.html accessed 13 March 2018.
[220] Art. 43(1) GDPR.

5.2.3.3. Legal effect

As for the legal effects, those depend on which authority will be determined to grant the accreditation certificate. In any case, the decision is binding and may be appealed in the competent courts, depending on the issuing authority. Another possible option is that the process is separated in two processes: the NAB grants an accreditation certificate, which is followed by, and is only valid on the condition that the DPA grants a specific accreditation certification on the basis of its accreditation requirements. In such a case, the applicant certification body could turn against the decision of the authority which is harmful to its interests.

5.2.4. Assessment of GDPR accreditation models and open questions

ENISA, in its recent report on GDPR certification, identified challenges associated with the resources of the DPAs,[221] but also the lack of experience of the DPA in relation to the procedural requirements of conformity assessments, such as checks and controls on the independence and transparency of the applicant for certification. ENISA also warned about potential implication of the function creep, when a DPA acts as an accreditation body, and at the same time is involved in the certification process. An example is where the DPA for instance should carry out periodic review of certifications in line with Art. 57(1)(o) GDPR or order the certification body to withdraw or refuse to issue certification in line with Art. 58(2)(h) GDPR.

From the above description, several open questions and challenges arise:[222]

- The meaning and content of the additional requirements in Art. 43(1)(b) GDPR
- Applicability of ISO/IEC 17065:2012 requirements in Model 1, where DPAs act as the only accreditation authority.
- Recognition of accreditation certificates granted in other Member States by DPAs or National Accreditation Bodies
- Training and expertise of auditors in the certification process
- Demonstration of independence of certification bodies and their auditors and homogeneity of the assessment methodology

[221] Also: Rowena Rodrigues, David Barnard-Wills, Paul De Hert and Vagelis Papakonstantinou, 'The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR' (2016) 30(3) International Review of Law, Computers & Technology, p. 248.

[222] The questions were addressed to the National Accreditation Bodies and the DPAs in the form of a survey. See Annex 5.

- Appropriate auditing techniques
- Function creep of DPAs being involved in both accreditation and certification activities.[223]

[223] ENISA, 'Recommendations on European data protection certification', p. 25.

5.3. Requirements for accreditation and certification bodies based on standards and EU regulations

This section presents an overview of the accreditation requirements to be met by certification bodies. The section goes beyond the GDPR, which was the focus of the previous section, and explores the practices and main sources of requirements for accreditation of certification bodies, in the field of data protection certification. In addition, the conditions to be met by the bodies providing accreditation services themselves, are also examined based on the ISO/IEC 17011 technical standard and the Accreditation Regulation.

5.3.1. Conformity assessment standards

5.3.2. EN ISO/IEC 17065:2012 conformity assessment for certification bodies

The ISO/IEC 17065:2012 on Requirements for bodies certifying products, processes and services[224] technically revises and updates an earlier standard, namely ISO/IEC Guide 65:1996. Several issues highlighted in the standard are to be taken into account by certification bodies.

- **Legal and contractual matters**

The contract between the accreditation body and the certification body should address the following matters:

- the legal status of the certification body
- liability of the certification body regarding certification activities
- minimum set and types of obligations to be imposed by the certification body on the controllers or processors to which the certification was granted, regarding:
  - the making available of access and information necessary for certification and any later updates on relevant changes
  - continuous commitment of the client to observing the certification criteria
  - arrangements for inspection, monitoring before, during and after certification
  - arrangements regarding observance of rules
  - measures regarding transparency and authorized use of conformity signage related to the certificate, once granted

[224] ISO/IEC 17065:2012 Conformity assessment - Requirements for bodies certifying products, processes and services <https://www.iso.org/standard/46568.html> accessed 12 March 2018.

- availability of measures to record and deal with complaints, disputes and various types of transgressions.

- **Conflict of interests and impartiality**

Requirements relating to impartiality relate to the measures the certification body undertakes in order to prevent conflicts of interests in all its organisational levels, measures taken to mitigate risks, and measures taken to ensure auditor independence. The standard requires a high commitment from the management level from the certification body to apply all the relevant measures for impartiality.

- **Confidentiality, non-discrimination and liability**

Issues regarding financial viability, liability insurance coverage of the certification body should be addressed in the accreditation process of the certification body. In addition, other relevant issues include how the certification body tackles equal access for all interested parties and the avoidance of discriminatory practices, such as by accepting to review the application of one data controller over another.

- **Transparency**

Transparency of criteria, assessment methods, and the status of awarded and withdrawn certifications is of paramount importance for building confidence on the certification mechanism, seals, and marks. The standard requires that information on the requirements, process, and results of certification is publicly available.

5.3.3. **EN ISO/IEC 17011:2017 requirements for accreditation bodies**

A technical standard broadly used by accreditation bodies is the ISO/IEC 17011 standard, which is adopted as a European standard. The standard is primarily aimed at accreditation bodies themselves, but can provide useful information for the assessment of other conformity assessment bodies as well. It provides a series of requirements for competence, operation, and impartiality of conformity assessment bodies which assess and accredit conformity assessment bodies, including certification bodies. The technical standard specifies general requirements, such as contractual agreements, structural and resource requirements, as well as process and information requirements.[225]

- **Content of contractual agreement**

The relationship of the accreditation body and the conformity assessment body is governed by an accreditation agreement signed

[225] For the case that certification bodies that provides services on management systems, an additional set of requirements is provided in the standard.

between the accreditation body and the certification body. The agreement should include the commitments of the conformity assessment body to fulfil the accreditation requirements and to provide evidence of its conformity. Other clauses of the agreement should address the obligation of the applicant body to facilitate the work of the assessors by providing access to the required documents and records. In addition, the accreditation body should be able to assess the performance of the certification body. To that end, the certification body needs to include a relevant clause in its agreement with the applicant controller, or processor, to allow access to the accreditation body to its site. The use of the accreditation symbols, and in general, how the granting of the accreditation and its scope is communicated should also be regulated by the commitment in order to avoid being misleading or misrepresentations. Clauses about an obligation on reporting changes in the legal ownership, organisation and scope of accreditation should also be communicated to the accreditation body.

- **Impartiality and competence of personnel**

The accreditation body is responsible for the impartiality and competence of its personnel. An obligation on the disclosure of any potential or present conflict of interest by the employees of the accreditation body needs to be disclosed. In addition, the accreditation body needs to establish processes to identify, analyse, evaluate and monitor on an ongoing basis any risks to impartiality arising from the course of its activities.[226] Similarly to the ISO/IEC 17065 standard, the policies and processes of the accreditation body should be non-discriminatory and apply as such. With the exception of fraudulent behavior, falsification of information or deliberate violation of the accreditation requirements, access to accreditation services should not be refused to an applicant. Among the responsibilities of the accreditation body is the determination of the competence criteria of its personnel involved in the performance of assessments. The competence of the personnel concerns both the knowledge and the skills required to perform accreditation activities in a specific field and the knowledge of the assessment principles, practices and techniques.[227] Outsourcing is allowed under the condition that accreditation decisions are made by the personnel of the accreditation body and the accreditation body takes responsibility for all the activities outsourced to another body.

[226] Risks to impartiality may relate to ownership, personnel, management, finances, outsourcing, marketing or other sources. ISO/IEC 17011:2017, p. 7.

[227] The following examples are provided: knowledge of practices and processes of conformity assessment body business environment, communication skills, interviewing skills, assessment-management skills and reporting skills.

- **Process and assessment**

The accreditation process starts with the application of the certification body. The certification body conveys information regarding its legal status, human and technical resources, the scope of the accreditation for which the certification body seeks accreditation and a commitment to fulfil the requirements for accreditation. The application is examined during the initial assessment process. Following a review of the documentation, the accreditation body prepares the assessment. A part of the preparation is the internal check, regarding whether the certification body has a competent assessment team to conduct the certification process, within the requested scope. The assessment may be performed remotely or on-site. When non-conformities are identified, the accreditation body provides the opportunity for the applicant certification body to take corrective actions. The accreditation body then decides and if the decision is positive, it grants the accreditation.

5.3.4. **Accreditation Regulation**

In 2010, the Regulation 765/2008 started applying directly to all EU Member States. The aim of the Accreditation Regulation, as set out in Article 1, is to lay down the rules on the organisation and operation of accreditation of conformity assessment bodies performing conformity assessment activities. The Regulation applies to both mandatory and voluntary accreditation of conformity assessment and applies irrespective of the legal status of the body performing the accreditation.[228]

5.3.5. **Requirements for Accreditation Bodies**

The Accreditation Regulation provides a series of requirements to be fulfilled by the National Accreditation Bodies themselves. The requirements are set out in Art. 8 of the Accreditation Regulation and can be grouped in three categories:

A. Relating to independence and integrity of the organisation and its personnel

- Independence from the certification bodies, commercial pressures, and conflicts of interest[229]
- Objectivity and impartiality of its activities[230]

[228] Art. 3 Regulation 765/2008 setting out the requirements for accreditation.
[229] Art. 8(1) ibid.
[230] Art. 8(2) ibid.

- Differentiation of persons that carry out the assessment and persons taking the decision to accredit a conformity assessment body[231]
- Confidentiality of the obtained information should be safeguarded through adequate arrangements[232]
- Transparency through the publication of audited annual reports[233]

B. Relating to the competence of the personnel and quality of assessment

- Competence of persons taking the decisions relating to the attestations[234]
- Identification of the competence of conformity assessment activities[235]
- Sufficiency of competent personnel for the proper performance of the tasks of the National Accreditation Body[236]
- Documentation of duties, responsibilities, and authorities of the personnel that would affect the quality of assessment and of the attestation's competence[237]
- Monitoring of performance and competence of the personnel involved[238]

C. Relating to the efficiency of procedures

- Efficiency of management and appropriate internal controls[239]
- Carrying out of the assessments giving due account to the size, structure, sector, degree of complexity of the product technology, nature of the production process[240]

5.3.6. Presumption of conformity and Peer Evaluation system

The Accreditation Regulation establishes a system of peer evaluation for the National Accreditation Bodies, which helps establish mutual trust and confidence among the NABs on the quality of the assessments. Even though room for improvement has been identified in the current

[231] Art. 8(3) ibid.
[232] Art. 8(4) ibid.
[233] Art. 8(5) ibid.
[234] Art. 8(3) ibid.
[235] Art. 8(5) ibid.
[236] Art. 8(7) ibid.
[237] Art. 8(8) ibid.
[238] Art. 8(5) ibid.
[239] Art. 8(6) ibid.
[240] Art. 8(5) ibid.

peer evaluation system,[241] peer evaluation is one of the cornerstones of acceptance of granted accreditation certificates.[242] The presumption of conformity of accreditation bodies, as provided by the Blue Guide, entails that:

"If a national accreditation body has successfully undergone peer evaluation for a specific conformity assessment activity, national authorities are obliged to accept the accreditation certificates issued by this body, as well as any attestations (e.g. test or inspection reports, certificates) issued by conformity assessment bodies accredited by this accreditation body"[243].

In practice, this means that once a certification body is accredited in one Member State, it does not have to be accredited again in another Member State by its national authority, if it expands its services to that country. The national authorities in that country accept the accreditation granted in another MS. This acceptance (or otherwise recognition)[244] saves the National Accreditation Bodies from administration burdens in having to re-accredit certification bodies in their own territory of competence. At the same time, it offers a relief to certification bodies that do not need to go through a costly and lengthy process in each MS they intend to offer services.
The GDPR does not refer to such acceptance or recognition of accreditation certificates. However, depending on the Accreditation Model each Member State adopts, there are different obligations regarding recognition of the accreditation certificates. In the case that National Accreditation Bodies conduct the accreditation process, the conditions of the Accreditation Regulation apply. As a result, the issued accreditation certificates are *de lege* recognised in other MS. An important matter in that respect, as highlighted in the Stakeholder workshop organised in the framework of the study,[245] is the issue of granting accreditation based on common requirements. Diversities in

[241] European Commission, 'Report From The Commission To The European Parliament, The Council And The European Economic And Social Committee on the implementation of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93',(COM/2013/077 final) provides that : "*The next objective is to further strengthen the peer evaluation process, to enhance the availability of trained and experienced peer evaluators and to further harmonise approaches particularly in the regulated sector".*
Available: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52013DC0077&from=en> accessed 12 March 2018.
[242] Art. 2(16) Regulation 765/2008 setting out the requirements for accreditation defines peer evaluation as the "*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*".
[243] European Commission, "The 'Blue Guide' on the implementation of EU products rules 2016' 2016/C 272/01, OJ C 272/1, 26.7.2016.
[244] See Annex 1 Glossary for the term "recognition".
[245] See Annex for the Report of the Stakeholder workshop, organised on 17th April 2018 in Brussels.

the requirements would need an additional level of assessment by the NABs to ensure mutual compatibility. Requirements stemming from the Accreditation Regulation and the ISO/IEC 17065:2012 (Art. 43 GDPR) are common, but this might not be the case with the 'additional requirements' provided by national supervisory authorities to their National Accreditation Bodies.[246] In the case that supervisory authorities act as Accreditation Bodies (Model 1), there is no explicit obligation of supervisory authorities to recognise accreditation certificates issued in other MS. The following distinction should be made: in case of accreditation certificates issued by a NAB in one MS, the supervisory authority of another MS is not obliged to recognise the accreditation certificate.[247] However, in the case of accreditation certificates issued by other DPAs, the view that there is a general obligation of recognition, deriving from Art. 63 GDPR (consistency mechanism) and Art. 64(1)(c) (Opinion of the EDPB) GDPR could be supported. In either case, such issues demand clarification and preferably a common approach, that does not allow for forum-shopping and ensures consistency in the implementation of the GDPR.

5.3.7. Relationship of the GDPR to the Accreditation Regulation

As explained in the previous sections, the GDPR provides specific rules for the accreditation of certification bodies that wish to provide services in line with the approved data protection certification mechanisms of Art. 42 GDPR. At the same time, at EU level again, the Accreditation Regulation has already been in force since 2008 and has been applicable to EU Member States since 2010. The scope of the Accreditation Regulation is not identical to the scope of the accreditation-related provisions of the GDPR. The aim of the Regulation is to lay down rules on the organisation of accreditation of conformity assessment bodies performing conformity assessment activities of products, processes, services, systems, persons or bodies.[248] The GDPR accreditation provisions - and conformity assessment more general, refer to "processing"[249] of personal data, which is more limited in scope than the Accreditation Regulation.

Whereas the Accreditation Regulation directly applies only to NABs, it does not apply as such to supervisory authorities, according to Art. 43 GDPR. It should be noted however, that the Accreditation Regulation provides procedures and safeguards to the Bodies performing the accreditation process and consequently, the accredited bodies i.e. the

[246] See variety of interpretations and approaches on the meaning of 'additional accreditation requirements' in p. 98.
[247] The EDPB argues that the GDPR is *lex specialis* to the Accreditation Regulation [See EDPB Guidelines 4/2018, p.7].
[248] Art. 1(1) and Art. 2(12) ibid.
[249] See for instance Art. 42(1) and Art. 42(6) GDPR.

certification bodies. All these procedures and safeguards, discussed in the previous sections, guarantee that the Accreditation Body can provide reliable assessments as to whether an applicant certification body does not only have the expertise to provide certification services in a specific field, but also provides for guarantees in terms of the management, resources, liability, confidentiality, and other issues.

5.3.8. **The International Accreditation Forum**

The International Accreditation Forum is an international association of organisations, which collaborate to achieve common trade objectives. The focus of the IAF is the development of principles and practices for conformity assessment, with the objective to promote a common application of requirements for certification, and also to promote and facilitate the equivalence of accreditations granted by IAF members.[250] In this framework, several mandatory and informative documents are issued from the IAF and addressed to its participant organisations. Each Accreditation Body Member is obliged to commit to provide accreditation in conformity with the relevant normative documents endorsed by the IAF.[251] Below, we discuss practices and guidance issued from the IAF that offers useful examples for the GDPR accreditation Models on the competence of the assessors of the accreditation body, sanctions for non-conformity, and accreditation of certification bodies in multiple countries.

- **Generic Competence for Accreditation Body Assessors**

The IAF has adopted guidance on the competence of accreditation body assessors in line with the ISO/IEC 17011 standard.[252] The competences of the assessors (auditors) cover general issues of accreditation (such as legal entity structures, accreditation standards, technical terms associated with accreditation), planning and scheduling (such as prioritization of assessments by risk areas, preparation of assessment plans, resources required during an assessment and others), document review, onsite assessment and reporting activities. In addition, leadership, behavioral, and organisational competences are described by the IAF.

- **Harmonisation of Sanctions**

The IAF published a document with obligations regulating the harmonisation of sanctions, which is designed to apply to Conformity

[250] International Accreditation Forum, Memorandum of Understanding, Issue 6, 26 February 2016, p.5.
[251] International Accreditation Forum, Memorandum of Understanding, Issue 6, 26 February 2016.
[252] IAF, Generic Competence for AB Assessors: Application to ISO/IEC 17011 >http://www.iaf.nu/upFiles/IAFMD202016_Issue_1_25052016.pdf< accessed 10 February 2018.

Assessment Bodies, including certification bodies.[253] Accreditation Bodies, which are members of the IAF, may initiate sanctions for certification bodies, in case:

- There is a failure to resolve non-conformities in accordance with the procedures of an Accreditation Body.
- Where a complaint has been filed against an accredited certification body and after the Accreditation Body has investigated the complaint, the outcome of the investigation was negative for the certification body.
- The accredited certification body has misused or misinterpreted an accreditation symbol
- The accredited certification body has not paid the required fees to the Accreditation Body.

The sanctions that are available to Accreditation Bodies include:

- Intensification of surveillance (monitoring)
- Reduction of the scope of accreditation
- Suspension
- Withdrawal
- Public notice of the imposed sanction(s)
- Legal actions.

Since IAF Members mutually recognise the accreditations granted to and from other IAF Members, the IAF has established an obligation of the Members to communicate sanctions, suspensions, and withdrawals of accreditations.

- **Accreditation Assessment for Certification Bodies with Activities in Multiple Countries**

An issue that arises in cases of certification bodies established in multiple countries is how to perform the accreditation process.[254] Especially in the case of certifications for data transfers, the geographical location of the accredited certification body will be of interest. The GDPR does not specify whether the certification body could be established in a non-EU country and whether the possibility for outsourcing parts of the certification process (such as pre-assessment and collection of documentation) to local collaborators of the certification bodies. Whereas specific guidance is required by the EDPB

[253] IAF, IAF Mandatory Document for Harmonisation of Sanctions to be applied to Conformity Assessment Bodies, Issue 1, Version 2, 2010.
[254] This issue is raised especially in the context of certifications for data transfers. See Chapters 8 and 9 of the Report.

on the issue specifically in relation to the GDPR data protection certification mechanisms, there is significant experience already established from the accreditation practices in other fields, which is incorporated in guidance of the IAF.
The IAF provides that[255] the Accreditation Body bears a responsibility to ensure that all the activities of the certification body under assessment conform to the relevant standards, irrespectively of the location(s) that those activities are performed.[256] Sometimes conformity assessment activities are performed using remote personnel using an IT system. The Accreditation Body needs to set up an assessment program that enables the body to confirm the conformity of the activities of the certification body within the scope of accreditation. Elements of such an assessment program include the effectiveness of the management controls of the certification body, whether the certification body is accredited by the local accreditation body, the key activities performed by the personnel established in a foreign country and others. The assessment needs to take place not only at the initial phase of application for accreditation, but also at a later stage after a period of monitoring ('surveillance'), following the issuance of the accreditation certificate.

5.3.9. **The European Co-operation for Accreditation**

The European Co-operation for Accreditation (EA) is an association of the national Accreditation Bodies (NABs) in the EU, as recognised in the Accreditation Regulation. The main mission of the EA is to ensure confidence in accredited conformity assessment results through harmonisation of the operation of accreditation activities.[257] The EA has been appointed by the Accreditation Regulation as the body responsible to provide the infrastructure to European Accreditation.

One of the main responsibilities of EA and its members is the peer evaluation process. NABs conduct peer evaluation to ensure the quality and harmonisation of techniques and conformity assessment results. The EA provides a series of mandatory (for its members) documents, alongside with informative guidance and technical and advisory reports.

5.3.10. **Other sources of guidance**

Apart from the formal accreditation fora examined above, several other sources used in practice can provide useful guidance for accreditation in the field of data protection. Examples are the Audit/Assurance Program

[255] As well as the ISO/IEC 17000 series conformity assessment standards provide guidance in such matters.
[256] IAF, Accreditation Assessment of Conformity Assessment Bodies with Activities in Multiple Countries, Issue 2, 2016.
[257] See >http://www.european-accreditation.org/mission< (accessed 12 February 2018).

provided by ISACA,[258] the IS Audit and Assurance Standard 1005 Due Professional Care, and the IS Audit and Assurance Guideline 2006 Proficiency.[259]

[258] ISACA is a non-profit, independent association that advocates for professionals involved in information security, assurance, risk management and governance. >https://www.isaca.org/pages/default.aspx< (accessed 10 February 2018) Data Privacy Audit Assurance Program: https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/data-privacy-audit-program.aspx (accessed 10 February 2018).
[259]Accessible http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Pages/Guideline-2006-Profiiency.aspx (accessed 10 February 2018).

5.4. 'Additional' accreditation requirements per 43(1)(b) GDPR

This section discusses the content of "additional accreditation requirements".[260] The Accreditation model which involves the NAB in the accreditation process, with the support of the competent national supervisory authorities or the EDPB, provides that accreditation is conducted based on the requirements of the ISO/IEC 17065:2012, and "additional accreditation requirements" provided by the DPA. However, the concept is rather vague and neither the accreditation legislation nor current practices, as identified in Chapter 3, provide information. Useful information for guidance on the interpretation and operationalisation of the "additional requirements" are to be found in the guidance for accreditation bodies on how to conduct accreditation in specific application areas. In the survey launched in the framework of this Chapter,[261] the National Accreditation Bodies of the EU Member States and the Data Protection Authorities were asked to elaborate on the potential scope of such additional accreditation requirements and provide examples. Below, we elaborate on the responses of the 23 DPAs and 20 NABs that responded to the questionnaire.

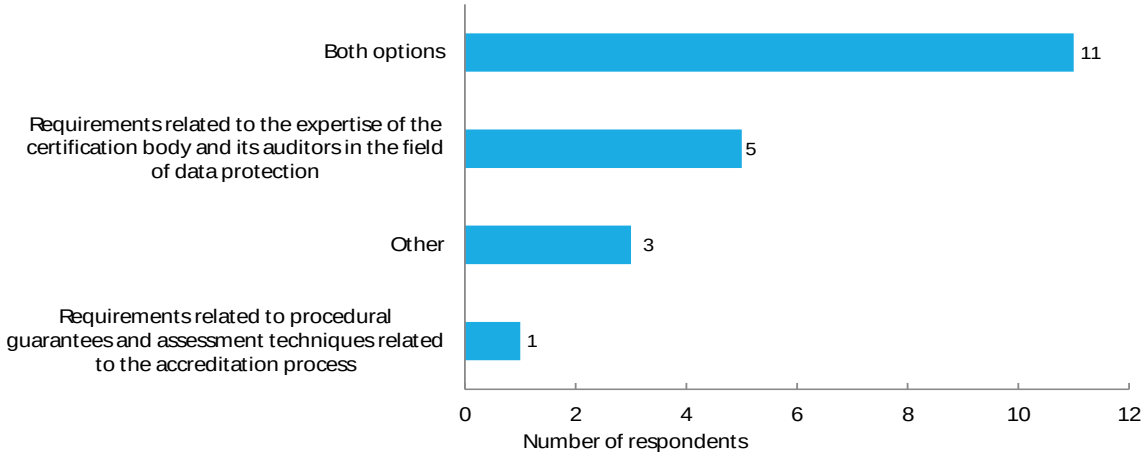
[260] Art. 43(1)(b) GDPR. The WP29 draft opinion on accreditation and the EDPB adopted Guidelines 4/2018 defined as "additional requirements" the requirements "established by the supervisory authority which is competent and against which an accreditation is performed". WP29 WP261 p.6.; Guidelines 4/2018 p. 5

[261] See Annex 4 information on the identity of the survey, the questionnaire, and the replies (separate document).

5.4.1. Stakeholder views

5.4.1.1. Data Protection Authorities and Information Commissioners

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 5-4 DPAs views on interpretation of 'additional requirements' per Art. 43(1)(b) GDPR

One of the three respondents, who selected "Other", explained that both options are under the term "additional requirements", and more specifically the expertise of the certification body, procedural issues, monitoring of the conformity of the certification body and scope of accreditation.

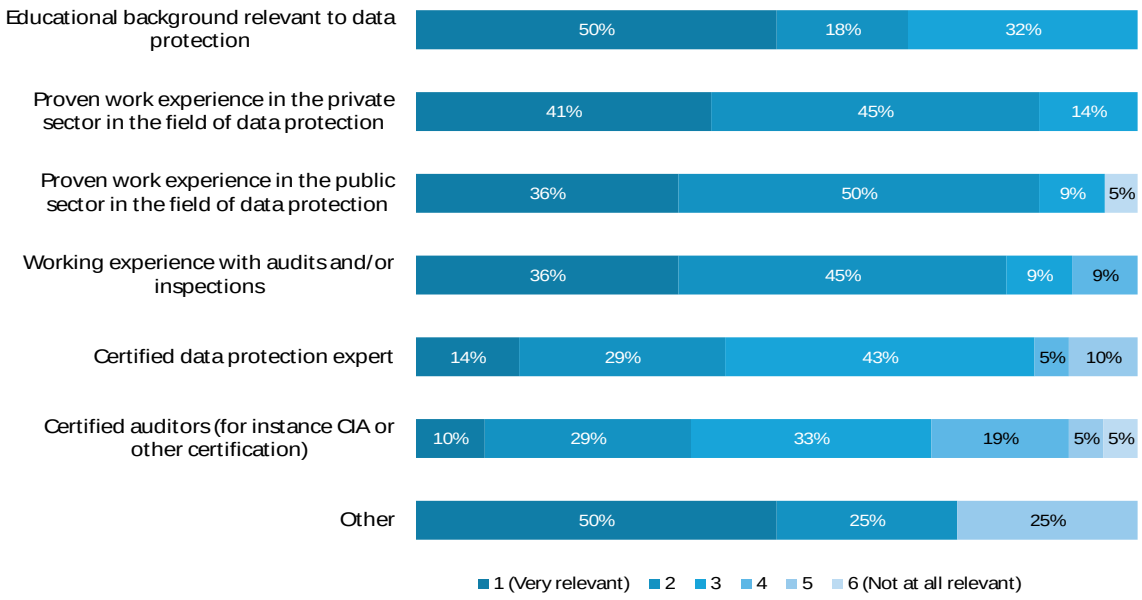
The respondents from the DPAs were requested to provide examples of additional requirements of Art. 43(1) (b) necessary for the accreditation of certification bodies in the data protection field. The responses related to:

- Knowledge & expertise in GDPR, potentially certified. For instance, specific assessment criteria of DPIAs, specific evaluation framework and tools relating to technical and organisational security measures.
- Knowledge & expertise of ePrivacy legislation, Data protection impact assessments, anonymization
- Practical experience with auditing of information security management systems
- Experience & competence as an auditor

- Knowledge & expertise in business logic or processes related to several activity sectors, etc.
- Independence
- Impartiality & conflict of interests' requirements
- Adequacy and relevance of resources

The DPAs were also asked to rate the factors relevant to assess the expertise of an auditor of a certification body.

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

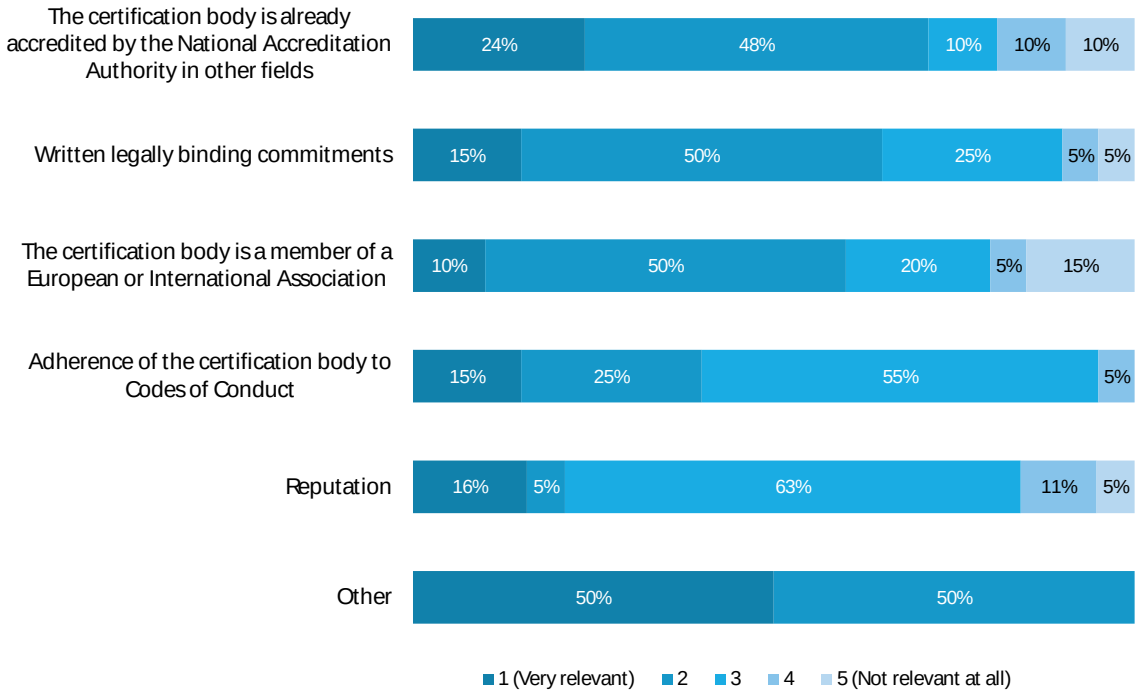
Figure 5-5 DPA views on relevant factors to assess auditors' expertise

The respondents who provided an assessment for "Other" provided a range of replies, such as:

- Proven communication skills
- Technical skills
- Adherence to a code of conduct

Regarding the independence and integrity of a certification body and its auditors, the DPAs provided the following replies:

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)*

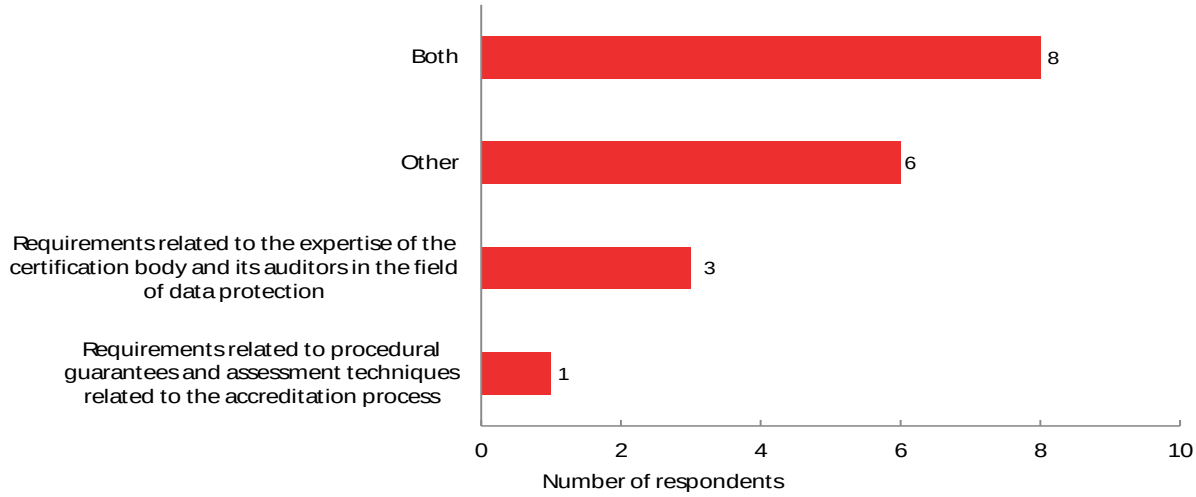


Source: Online survey on accreditation. Note: Bars denote average scores. From top to bottom, N=21, 20, 20, 20, 19, 4.

Figure 5-6 DPAS views on assessment of independence and integrity

5.4.1.2. National Accreditation Bodies

Accordingly, the NABs were also asked to provide their views on the content of "additional requirements" with a closed type question, and the opportunity to elaborate.

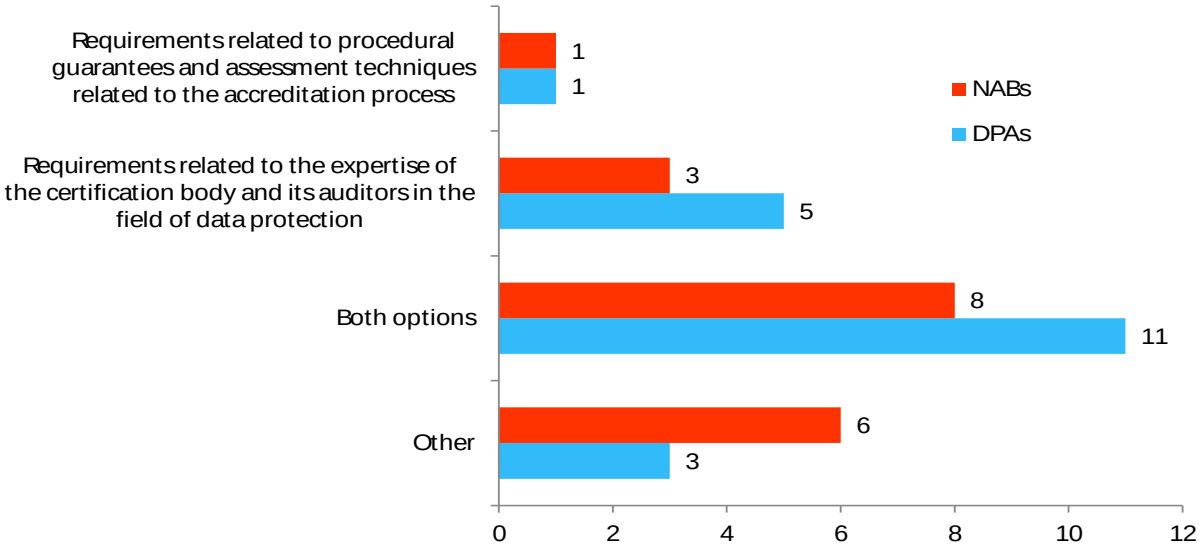


Source: Online survey on accreditation. Note: Bars denote total response count. N=18.

Figure 5-7 NABs views on interpretation of 'additional requirements' per Art. 43(1)(b) GDPR

The respondents who ticked "Other" were asked to elaborate. Those respondents pointed out requirements stemming from the ISO/IEC 17067 technical standard, as well as requirements related to the evaluation process, such as evaluation activities, depth of evaluation, sampling, expected audit times.

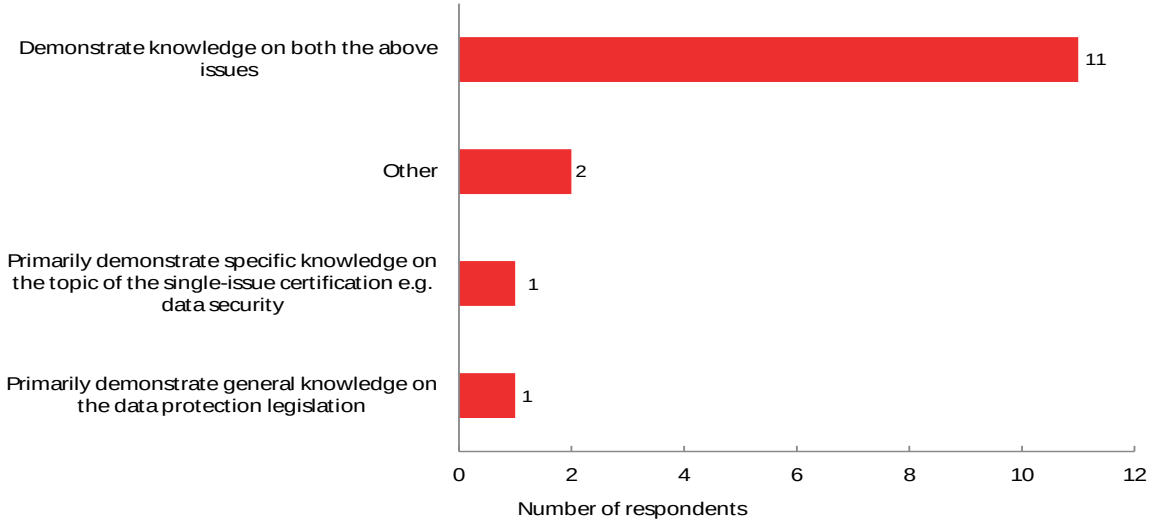
The comparative table below shows that the respondents from both groups identify as scope of the term "additional accreditation requirements" both requirements related to the expertise in the field of data protection and to procedural guarantees and assessment techniques.



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

Figure 5-8 Comparative overview DPAs v NABs views on 'additional accreditation requirements'

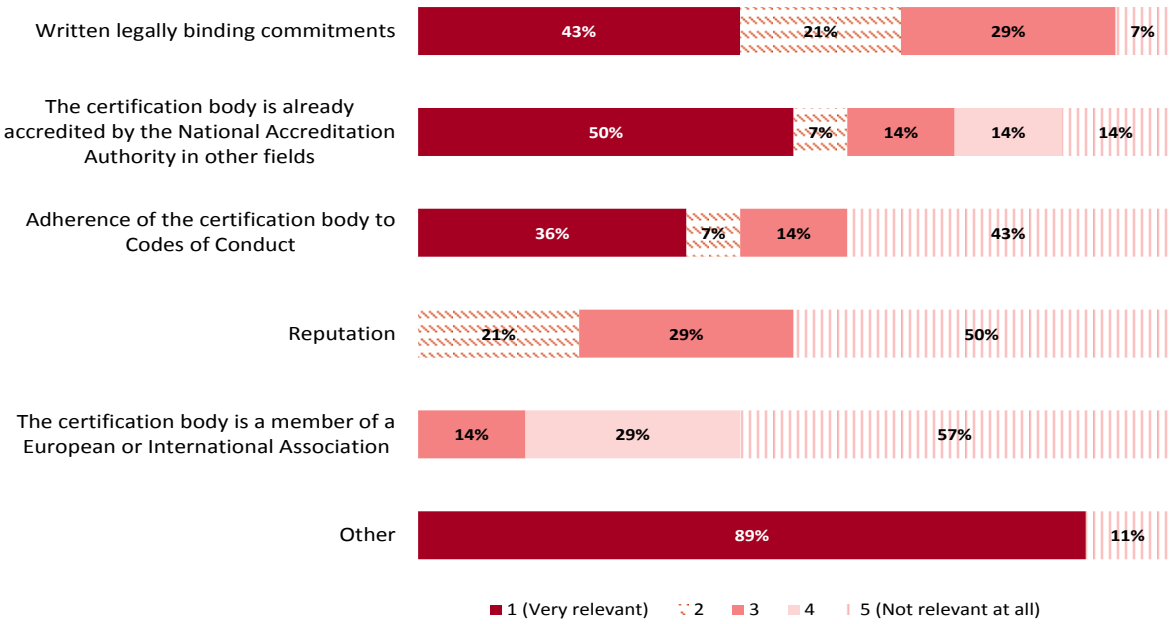
The respondents from the NABs were also asked about their views on the qualifications of the certification body (and its auditors) in the case of single-issue certifications (i.e. certifications covering only one aspect in the GDPR e.g. data security or data portability).



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

Figure 5-9 NABs views on qualifications of certification bodies for single-issue certifications

On the issue of independence and integrity of a certification body and its auditors, the respondents from the National Accreditation Bodies provided the following replies:



Source: Online survey on accreditation. Note: Bars denote average scores. From top to bottom, N=14, 14, 14, 14, 14, 9.

Figure 5-10 NABs views on assessment of auditors' independence and integrity

The respondents that selected "Other" highlighted the criteria of the ISO/IEC 17065 and ISO/IEC 17067 standards, as well as risk assessments on the existence of conflicts of interests in order to safeguard impartiality, rules and procedures of the certification body.

5.4.2. Clustering of additional requirements

The survey and literature review revealed three main clusters of requirements in addition to the Accreditation Regulation and EN ISO/IEC 17065 requirements.

- **Additional requirements related to the certification body and its auditors' expertise in the field of data protection**

Data protection authorities should provide specific requirements related to the expertise and knowledge required of the certification bodies in the field of data protection and the specific scope of the certification scheme. Both work experience and educational background in data protection law and information security are necessary competences for auditors working for accredited certification bodies. The auditors themselves could also be certified as experts in data protection law.

  - Knowledge & expertise in the GDPR, potentially certified. For instance, specific assessment criteria of DPIAs, specific evaluation framework and tools relating to technical and organisational security measures.

- Knowledge & expertise of ePrivacy legislation, Data protection impact assessments, anonymization
- Practical experience with the auditing of information security management systems[262]

- **Additional requirements related to certification body and its auditors' competence in performing audits**

Beyond the expertise in the field relevant to the scope of certification, the certification body and its auditors need to have training and skills on performing audits. Experience as a legal expert or information security expert does not entail that one knows how to perform audits, where to look for the necessary information, how to identify the appropriate methods for each case, and other skills.

- Experience & competence as an auditor
- Knowledge & expertise in business logic or processes related to several activity sectors, etc.

- **Additional requirements related to the integrity of the auditors and the certification body**

Ultimately, the supervisory authorities will need to provide 'additional' requirements to the Accreditation Bodies on issued of integrity and independence. The requirements should build on the knowledge and practices of the NABs in assessing integrity and impartiality, but further specify concrete examples on how those requirements apply in a data protection context, taking into account the relationships of the actors (controllers, processors, joint controllers, sub-processors, data subjects, certification bodies), the processing activities, the exercise of data subjects rights, and the nature of the data.

- Suitability in the information rights context
- Adequacy and relevance of resources
- Independence
- Impartiality & conflict of interest requirements

5.5. Discussion

This Chapter identified the models of accreditation as provided in the GDPR, along with a number of issues and implications they might trigger:

[262] Even though GDPR certification in line with Art. 42 and 43 does not include information security management systems *as such* in its scope, management systems might be part of the assessment for instance in relation to certification based on Art. 32 GDPR on data security of a processing activity. See EDPB Guidelines 1/2018 p. 11

- The meaning and content of the additional requirements in Art. 43(1)(b) GDPR
- Applicability of ISO/IEC 17065:2012 requirements in Model 1, where DPAs act as the only accreditation authority.
- Recognition of accreditation Recognition of accreditation certifications granted in other Member States by DPAs or National Accreditation Bodies
- Training and expertise of auditors in the certification process
- Demonstration of independence of certification bodies and their auditors and homogeneity of the assessment methodology
- Appropriate auditing techniques
- Function creep of DPAs being involved in both accreditation and certification activities.[263]

In addition, we identified a number of normative and informative sources for accreditation requirements for certification bodies and requirements to be applied to accreditation bodies themselves.

Last but not least, we delineated the concept of additional accreditation requirements, which refer to:

- Requirements related to the certification body and its auditors' expertise in the field of data protection
- Requirements related to certification body and its auditors' competence in performing audits
- Requirements related to the integrity of the auditors and the certification body

[263] ENISA (2017) 'Recommendations on European data protection certification', p. 25.

6. Technical standards for certification

6.1. Introduction and methodological approach

Standards play a substantial role for certification, as oftentimes standards form the normative basis for certification or in other words, in many cases certification proves conformity to technical standards. In the GDPR data protection certification mechanisms, standards are also explicitly mentioned in Art. 43 GDPR. This Chapter delves into the following specific requests of the Commission:

1. identification of suitable existing technical standards to be promoted by the Commission;
2. determination of factors that affect the adoption of technical standards by relevant stakeholders;

This Chapter is based on a literature study and field research. The literature study has focused on both the study of existing research reports, business reports, scientific literature, technical standards (databases) and regulatory documents. Field research has included consultation with relevant stakeholders by means of a questionnaire and a workshop. The questionnaire that was sent out to a selected group of companies, including small and medium sized companies (SMEs), as well as industry associations, standardisation bodies and certification bodies. We have received 82 responses.[264] The Workshop was held with selected representatives of (SME) associations and industry in January 2018 in Brussels.[265]

This Chapter presents the results of the survey by highlighting a number of the most interesting results.[266] These results are subsequently weighed against a brief presentation of standards that might be of relevance for the certification process but were not recognised as such by the various stakeholders.[267]

The Chapter continues with an elaboration of factors relevant for the uptake of standards. This is also based upon the results from the survey as well as the literature study. The role of the various potential uptake factors is subsequently presented, in order to further the discussion about measures that could be adopted by the Commission to promote certification and standardisation.

[264] The characteristics of the survey and respondents, as well as the full text of the questionnaire are set out in Annex 5. (separate document).
[265] Annex 6 (separate document).
[266] Due to the limited number of respondents the results of the survey are not representative for the entire field of industry associations, certification bodies, standardisation bodies, SMEs and large enterprises. They are illustrative for a number of perspectives that can be found among the stakeholders of the respective stakeholder groups.
[267] The full results of the survey are presented in the Annexes.

6.2. Identification of technical standards relevant to data protection certification

6.2.1. Survey results

Standardisation may help organisations in demonstrating compliance and in structuring processes and responsibilities within the organisation concerning specific issues, related to the processing of data. Several classes of standards are available to this end. Currently the most relevant are the international standards promoted by ISO, the International Organization for Standardisation.

ISO has developed several series of standards that are relevant from the perspective of privacy/data protection:

- the 17000 series dealing with conformity assessment
- the 27000 series dealing with information security management
- the 29100 series dealing with privacy following a privacy framework approach (29100), a privacy architecture framework (29101), a privacy impact assessment methodology (29134), privacy notices and consent (29184) and a privacy capability maturity model (29190).

The 17000 series is relevant for accreditation bodies (such as 17007: Guidance for drafting normative documents suitable for use for conformity assessment, 17011: Requirements for accreditation bodies accrediting conformity assessment bodies) and for certification bodies (17021: Requirements for bodies providing audit and certification of management systems; 17028: Guidelines and examples of a certification scheme for services; 17065: Requirements for bodies certifying products, processes and services).

The 27000 series has a broad range of standards related to all aspects of information security and information security management systems, and is relevant for organisations handling personal data (27000-27001-27003-27004-27005: various aspects on information security management; 27002: Code of practice for information security controls; 27017: Code of practice for information security controls based on ISO/IEC 27002 for cloud services; 27018: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors; 27031: Guidelines for information and communication technology readiness for business continuity; 27032: Guidelines for cybersecurity; 27033: Network security) and auditors (27008: Guidelines for auditors on information security controls).

The 29000 series encompasses privacy standards (29100: Privacy framework; 29101: Privacy Architecture Framework; 29134: Guidelines for privacy impact assessment; 29184: privacy notices and consent; 29190: Privacy capability assessment model) and thus bears relevance for organisations processing personal data.

The survey highlighted the recognition of standards that help securing information management (the 27000 series). A number of these standards are recognized as relevant and as worthy of recommendation.

The survey asked for the present level of uptake of standards and the interest in promoting standards: "What privacy/data protection related technical standards do you use (industry)/would you recommend (industry organisation)/do you base your certification on (certification standards)?"[268,269]

	27000 series	29000 series	other
SMEs	27001; 27002; 27003; 27018	29134	BS10012
Large enterprises	27001; 27002; 27003; 27017; 27018	29134; 29151; 29190; 29191	BS10012; 19941
Industry associations	27001; 27002; 27003; 27018	29134	BS10012
Certification bodies	27001; 27002; 27003; 27017; 27018	29151	

Table 6-1 Inventory of responses

The 27000 series is recognised and promoted (especially 27001 and 27002); the 29000 series is only partially recognised (by large enterprises) and hardly promoted (by industry associations) or used in the certification process.

A significant part of the industry respondents indicated that they 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[270], including:

- Requirements from the German BSI (Bundesamt für Sicherheit in der Informationstechnik);
- PCI DSS v3.2, 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.

[268] Respondents were presented with the following options: 27001; 27002; 27003; 27017; 27018; 29101; 29134; 29151; 29190; 29191; BS10012.
[269] It concerns the following questions in the survey: question 2 industry associations, question 1 industry and question 3(b) certification bodies. See Annex 5 for details.
[270] Each by one respondent only.

On top of the standards presented in the survey, industry associations recommended the following standards:

- the Cloud Security Alliance Code of Conduct for GDPR Compliance, a document aimed at specifying the application of the GDPR in the cloud environment.[271]
- 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".[272]
- 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.[273]

As regards the certification bodies, it is interesting to note that only slightly more than half of the certification bodies responded that they used technical standards in the certification process (five out of nine respondents). They identified a number of other standards that are of relevance to them:

- ISO 17065[274] 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 the RTS of PSD2.

Standards can be national, European or international. National standards could be relevant for market parties that mainly are active in national markets, while European and international standards could be preferred to parties that act on a European or international scale.

The survey[275] demonstrates that relevant stakeholders (industry associations, SMEs and large enterprise) favour European and international standards over national one's. Large enterprises favour international standards over European ones. SMEs are interested in national standards as well. These results are in line with what might be

[271] See: Cloud Security Alliance, 'Cloud Security Alliance Issues New Code of Conduct for GDPR Compliance' (CSA,2017) <https://gdpr.cloudsecurityalliance.org/news/> accessed 13 March 2018.
[272] See: Cloud Security Alliance, 'Cloud Controls Matrix Working Group' (CSA,2017) < https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview > accessed 13 March 2018.
[273] See: Bundesamt für Sicherheit in der Informationstechnik, 'Referenzierung des Trusted Cloud Data Protection Profile V 1.0 auf C5' (2017), available: <https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_ Catalogue/C5_and_Data_Protection/C5_and_Data_Protection_node.html> accessed 12 March2018.
[274] This is however an accreditation standard.
[275] Question 6 industry associations and question 7 industry.

expected. The results underscore the relevance of action on a European scale.

6.3. Standards relevant for certifications: additional options

As part of the research efforts an overview has been made 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.

That overview has been created and based on research in standards databases. We restricted our research to:

1. currently existing standards. Draft standards were left out unless it concerned promising late stage drafts that are likely to be published within the next 12 months;
2. standards focused on data protection or relevant aspects thereof;
3. formal standards (hence set by recognised bodies).

The overview provides guidance as to additionally relevant standards but is not intended to provide a full and complete overview. In this paragraph we present some highlights of this overview.[276]

6.3.1. **Additional standards for industry**

For demonstrating conformity, the following standards might be deemed relevant.

ISO/IEC 22301 specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a document management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.

ISO/IEC 25012 defines a general data quality model for data retained in a structured format within a computer system. It can be used:

- 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.

[276] See full overview in Annex 5 (Separate document) and discussion on Recommending standards in p. 158f.

ISO/IEC 25024 defines data quality measures for quantitatively measuring the data quality in terms of characteristics 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;
- guidance for organizations defining their own measures for data quality requirements and evaluation.

6.3.2. **Additional standards for standardisation and certification bodies**

For (national) standardisation and certification bodies, the following standards might be relevant, on top of those already mentioned in the survey:

- ISO/IEC Guide 17 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. The standard could also be useful as drafting guidance to ensure the auditability of standards drafted by authorities in direction of SMEs;
- ISO/IEC Guide 23 defines the information that should be displayed in a third-party certificate when referring to a standard;
- ISO/IEC Guide 27 identifies 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);
- ISO/IEC 17067 describes the fundamentals of product certification and provides guidelines for understanding, developing, operating or maintaining certification schemes for products, processes and services.

6.3.3. **Additional standards for accreditation bodies**

For (national) accreditation bodies, the following standards might be relevant, on top of those already mentioned in the survey:

- ISO/IEC 17020 specifies requirements for the competence of bodies performing inspection and for the impartiality and consistency of their inspection activities. 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/IEC 17040 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. The standard could be useful to organize a mutual recognition process between public or private certification bodies located in different Member States.

6.3.4. Standardisation sources for relevant future developments

The body of technical standards relevant to data protection certifications is rapidly evolving. To a large extent triggered by the introduction of the GDPR and in the context of the growing societal awareness of issues like data protection and cyber security, various standardisation bodies have included or expanded the development of relevant standards in their work plans. In this section, the organisations and technical committees that currently seem to be particularly relevant for monitoring the availability of relevant technical standards are presented.

International Standardisation Organisation

ISO addresses the data protection issue (often referred to as privacy in ISO's wording) within Sub-Committee SC 27 Information technology -- Security techniques under which has been established the Working Group 5 (WG5) dedicated to Privacy, Identity management and Biometrics[277]. The following standards focusing on privacy matters are currently in development at ISO:[278]

- ISO/IEC DIS 19086-4 Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 4: Security and privacy;
- ISO/IEC PDTS 19608 Guidance for developing security and privacy functional requirements based on ISO/IEC 15408;
- ISO/IEC AWI 20547-4 Information technology -- Big data reference architecture -- Part 4: Security and privacy fabric;
- ISO/IEC DIS 20889 Information technology -- Security techniques -- Privacy enhancing data de-identification techniques;
- ISO/IEC CD 27550 Information technology -- Security techniques -- Privacy engineering;

[277] Presentation of the SC 27 Information technology -- Security techniques https://www.iso.org/committee/45306.html

[278] International Organization for Standardisation, 'ISO/IEC JTC 1/SC 27' (ISO, 2017)<https://www.iso.org/committee/45306/x/catalogue/p/0/u/1/w/0/d/0> accessed 13 March 2018.

- ISO/IEC CD 27552 Information technology -- Security techniques -- Enhancement to ISO/IEC 27001 for privacy management – Requirements;
- ISO/IEC DIS 29101 Information technology -- Security techniques -- Privacy architecture framework;
- ISO/IEC CD 29184 Guidelines for online privacy notices and consent
- ISO/IEC AWI TR 20547-1 Information technology -- Big data reference architecture -- Part 1: Framework and application process;
- 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 will be revised in 2019.

The Comité Européen de Normalisation (CEN) and Comité Européen de Normalisation Electrique (CENELEC)

During January 2015 CEN/CENELEC accepted from the DG Home of the European Commission[279] the standardisation request on 'Privacy management in the design and development and in the production and service provision processes of security technologies'. The Joint Technical Committee (JTC) 8 Privacy Management in Products & Services has been established in 2015 to address the European Commission's request with the JTC 13 Cyber Security & Data Protection established in 2017.[280]

The standards focusing on privacy matters currently under development at the CEN are the following one: [281]

- CEN/CLC/ETSI/prTR 50691 (WI=65708) Cyber Security and Privacy;
- EN 419212-4:2018 (WI=00224252) Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment;
- EN 419212-5:2018 (WI=00224253) Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment. CEN/TC 2242018-02-28

[279] See Privacy section on CEN-CENELEC's website https://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Privacy/Pages/default.aspx
See also Alessandro Guarino, 'New CEN-CENELEC Technical Committees for Infosec and Data Protection Standardisation' (presentationBrussels (TC8), 19 September 2017).
Available:<https://www.enisa.europa.eu/events/enisa-cscg-2017/presentations/guarino> accessed 12 March 2018.

[280] Walter Fumy, 'Cybersecurity and Data Protection standards in support of European policy' (presentation given at Cybersecurity Act - Establishing the link between Standardization and Certification', Brussels, 13 February 2018) Available:
<ftp://ftp.cencenelec.eu/EN/News/Events/2018/Cybersecurity_ENISA_CEN_CL_ETSI_Presentations/Walter-FUMY_Chair_CEN-CLC_JTC13.pdf> accessed 13 March 2018.

[281] See CEN standards catalogue. Available:
<https://standards.cen.eu/dyn/www/f?p=204:22:0::::FSP_ORG_ID:6205&cs=1FB1CC5B5F03F85F0ECCECA7598551CFC> accessed 12 March 2018.

Two Technical reports (TR) are also being drafted[282]:

- Data protection and privacy by design and by default - Video surveillance products and services
- Data protection and privacy by design and by default - Biometric access-control products and services

The European Telecommunications Standards Institute (ETSI)

The Cyber Security group of the European Telecommunications Standards Institute (ETSI)[283] is the technical committee in charge of elaborating standards related to IT security and data protection. ETSI is currently developing the following standards focusing on privacy matters currently:[284]

- DTR/CYBER-0010 Practical introductory guide to privacy;
- DTS/CYBER-0014 Mechanisms for privacy assurance and verification.

6.4. Uptake factors for standards and certifications

6.4.1. Introduction

In this section, we present an overview of the uptake factors for standards and certifications. In the first part, the results of the survey are presented, followed by a description of selected categories for representing uptake factors (Trust, Recognition, Implementation and Drivers) and relevance thereof. Subsequently we present an overview of uptake factors for standards and for certifications, structured along the lines set out before.

6.4.2. Uptake factors of standards and certifications – survey results

This paragraph focuses on outlining the results of the survey in as far these are relevant to understanding the perspectives of the respondents in what factors will drive or impede the uptake of standards or certifications.

[282] Alessandro Guarino and Kai Rannenberg,' Cybersecurity, Data Protection, and Privacy Standardization in Support of EU Policy' (presentation given at Cybersecurity Act - Establishing the link between Standardization and Certification', Brussels, 13 February 2018) Available: <ftp://ftp.cencenelec.eu/EN/News/Events/2018/Cybersecurity_ENISA_CEN_CL_ETSI_Presentations/GUARINO_RANNENBERG_CEN-CLC_JTC8.pdf> accessed 12 March 2018.
[283] The ETSI cyber group is presented on the ETSI's website http://www.etsi.org/technologies-clusters/technologies/cyber-security.
[284] Source ETSI standards catalogue >http://www.etsi.org/standards-search#Pre-defined Collections< accessed 12 March 2018

Within the survey, a distinction was made between factors influencing the uptake of a standard and factors influencing the uptake of a certification.

Uptake factors for standards

Respondents from both industry associations and industry[285] considered the following factors to be significant or very significant in deciding about promoting/implementing standards, in particular:

- the costs for acquiring and implementing a standard;
- the extent to which implementing the standard contributes to legal compliance.

For industry associations[286], a number of other factors were particularly relevant as well in deciding about promoting standards as well:

- the quality of the standard;
- the extent to which implementing the standards provides additional cyber security for their members;
- the extent to which the standards are unambiguous and clear;
- the level of endorsement of the standard by industry associations;
- the extent to which compliance with the standard raises trust in their sector.

SMEs and large enterprises specifically considered these following factors to be especially (very) relevant:

- impact on trust raised by clients;
- business advantage;
- previous experiences with implementing standards.

In this respect, no differentiation was found in the kind of factors considered relevant between SMEs and large enterprises. Additionally, the ranking of factors of relevance was found to be similar. The level of endorsement by either the European Union, by government bodies or by industry associations scored relatively low as a driver for both SMEs and large enterprises. Industry associations[287] were asked, separately, which challenges they thought their members would encounter the most when implementing privacy/data protection related technical standards. Respondents identified many of the factors indicated[288] but particularly mentioned:

[285] Questions 3 and 4 industry associations, questions 4 and 8 industry, and question 3(b) certification bodies. See Annex 5 for details.
[286] Questions 3 and 4 industry associations. See Annex 5 for details
[287] Question 4 industry associations. See Annex 5 for details.
[288] Specific options presented in the survey:

a. Negative experiences with following standards in general
b. Lack of information about the existence of relevant standards
c. Lack of information/knowledge about the possible benefits of complying with these standards
d. Lack of information/knowledge about the costs and efforts of implementing these standards
e. Lack of information/knowledge about the way in which these standards fit in their business processes

- 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 about the added value of the standard.

Standardisation bodies[289] considered a broad range of factors[290] to be significant or very significant in deciding about promoting/implementing standards and in particular:

- implementation costs
- the level of endorsement of standards by the EU;
- the extent to which implementing the standard provides a clear business advantage.

6.4.3. **Uptake factors for certifications**

Respondents from both industry associations and the industry considered the following factors to be significant or very significant in deciding about promoting/taking out certifications:[291]

- the costs for members to obtain such certification;
- the level of business advantage;
- the effect on trust;
- the effect on legal compliance;
- the extent of recognition in other EU member states.

In deciding about promoting certifications, industry associations considered the level of endorsement by the European Union much less

f. Lack of knowledge/skills for implementing the standards
g. Costs of acquiring the standards
h. Costs of implementing these standards
i. The standards are unclear
j. The standards are only partially relevant for their business
k. It is not sufficiently clear to them what would be the added value of achieving compliance with the standard
l. Uncertainty about what their customers want
m. Uncertainty about what their competitors will do

[289] Question 5 standardisation bodies. See Annex 5 for details.

[290] This covered all specified options presented in the survey:
a. Costs of acquiring the standards
b. Implementation costs
c. Availability of material for training/education
d. The level of endorsement of the standards by Data Protection Authorities
e. The level of endorsement of standards by the European Union
f. The level of endorsement of the standards by (other) government bodies
g. The level of endorsement of standards by industry associations
h. Positive experiences with implementing technical standards in general
i. The extent to which the standards are unambiguous and clear
j. The extent to which implementing the standards provides a clear business advantage
k. The extent to which implementing the standards provides additional cyber security

[291] Question 10 industry associations and question 12 industry. See Annex 5 for details.

important than endorsement by national governments and DPA's.[292] Industry (SMEs and large enterprises) considered endorsement by the European Union and DPA's (much) more relevant than endorsement by other government bodies.[293]

The extent to which competitors take out certifications was considered moderately relevant by both SMEs and large industry. The extent of recognition of certification in other EU member states was considered moderately relevant by SMEs but very relevant by large industry. [294]

For the implementation of certifications by their members, industry associations found the following factors to be of significant to high importance:

- costs of privacy/data protection certifications;
- the level of endorsement of certifications by industry associations and by DPA's;
- the effectiveness of a certification;
- the effect on image;
- the extent to which customers or business partners value the certification;
- the extent to which competitors take out such certification;
- legal protection;
- the extent of recognition in other EU Member States.

Certification bodies[295] considered a whole range of factors to be significant or very significant:

- costs of certifications;
- the level of customer's perception of effectiveness;
- the level of enforcement of data protection legislation;
- the level of endorsement of certifications by the European Union and by DPA's;
- the level of market pressure;
- the extent to which competitors take out such certification;
- the legal (protective) effect of certifications;
- the recognition of certifications in other EU member states.

6.4.4. **Categories of Uptake factors**

In this section selected categories of uptake factors are described (Trust, Recognition, Implementation and Drivers) for both standards and certifications.

[292] Question 10 industry associations. See Annex 5 for details.
[293] Question 12 industry. See Annex 5 for details.
[294] Question 12 industry. See Annex 5 for details.
[295] Question 8 certification bodies. See Annex 5 for details.

6.4.5. **Trust**

Busch[296] identifies two types of trust. Trust as predictability, where the trust is that something or somebody is going to behave in a predictable way, and trustworthiness is when the trust is that something or somebody is going to behave in careful manner in any occasion. Trust is a central issue in certification, to the extent that this procedure is built upon trust granted to a recognised third-party who is formally declaring an observed fact or situation is true. Trust in certification is commonly based on the legitimacy of the certification issuer, the legitimacy of the requirements used in the process and on the impartiality of the process applied. Well-known certification bodies which certify hundreds of organisations every year and base the certification process on well-established procedures, may leverage a higher level of trust than small and unknown certification bodies. Adequate communication concerning the scope and functions of a certification, and its performance over time, is crucial for building and maintaining trust.

However, trust, especially in certification,[297] remains fragile. Multiple incidents have challenged the reputation of certification bodies.[298]

Trust also has a cultural dimension. Certain countries, like Germany and Japan, according to the scheme owners interviewed during the study, are more willing to trust in this procedure which for cultural reasons that have not yet been clearly identified. Furthermore, the certification procedure suffers from a fundamental ambiguity insofar as the applicant is also a client. The certification body is a service provider that must, at the same time, satisfy a paying client and scrutinise its procedures with impartiality. The certification body must thus constantly balance the need to ensure the quality of the certification process and the requirement to satisfy a client that is able to swap, at any time, from one provider to another. Trust represents a basic and crucial element in the certification uptake without which certification does not work. Trust is also fragile and exceedingly tough to rebuild once it has been lost. Many events in the lifecycle of a scheme can challenge its trust and that is difficult to monitor. Moreover, distrust can quickly become widespread going from a single scheme to the certification as a whole. Thus, trust appears to be one of the greatest challenges for those who intend to set up and manage certification schemes and should be carefully considered.

[296] See Chapter "Certified, Licensed, Accredited, Approved" in Lawrence Busch *Standards: Recipes for Reality* (MIT Press, 2012).
[297] Civic Consulting, 'A Pan-European Trustmark for E-Commerce: Possibilities and Opportunities' (2008)
[298] See for instance TÜV Rheinland role within the PIP breast implant in France. Judgment in Case C-219/15 Elisabeth Schmitt v TÜV Rheinland LGA Products GmbH. Court of Justice of the European Union, PRESS RELEASE No 14/17.

Trust in standardisation is primarily influenced by its contribution over a period of time. Business trust in standardisation is also driven by the level of its involvement in the process of drafting the standards. Formal standard setting remains a voluntary activity, theoretically[299] accessible to all businesses, authorities and consumer representatives. The drafting processes suggested by the international standardisation bodies gives the same ballot to every national committee involved in standard drafting committees. Moreover, the issuance of the final standard requires consensus amongst the stakeholders.

The globalisation of trade and the emergence of the Internet have stressed the shortcomings of traditional regulatory instruments to properly regulate the international flows of goods, money and data. The interest of businesses for standardisation contributes to the rise of transnational private regulatory[300] instruments seeking to fulfil the perceived regulatory gap created by the territorial limitation of traditional regulation. Trust in standards play a vital role in development in that regard. The accessibility of the process (inclusiveness), as well as balanced and transparent procedures, are vital building blocks in creating trust in the standardisation process and hence the results thereof. Also quality related aspects are important, including the extent to which there is an efficient system to manage derogations and change.[301]

6.4.6. **Recognition**

Two types of recognition can be identified. One is similar to the endorsement and materialises the value granted by the market, the authorities and by the public to a standard or a certification. Another type focuses on the knowledge and the understanding of the content of a standard or scheme and its purposes.

The way in which the regulator recognises the importance of compliance with a standard could encompass a range of measures, varying from creating the necessary conditions for adoption[302], to providing a

[299] As Graz underlined that- multinationals are overrepresented and consumers and the civil society underrepresented in the international standardisation bodies (Jean-Christophe Graz, 'Le Monde Des Normes' (2010) 80 Bulletin HEC, 24).

[300] Fabrizio Cafaggi, 'The Architecture of Transnational Private Regulation' [2012] EUI working papers; Fabrizio Cafaggi, 'Transnational Private Regulation. Regulating Private Regulators' in Sabino Cassese (ed), *Research handbook on global administrative law* (Edward Elgar 2016). Available at SSRN <https://ssrn.com/abstract=2615694> accessed 12 March 2018;
Fabrizio Cafaggi et. al. 'Transnational Private Regulation' (OECD 2013) Available <http://www.hiil.org/project/private-transnational-regulation> accessed 12 March 2018.

[301] The Industry Standards Group, 'Specifying Successful Standards' (Infrastructure Cost Review, 2012) <https://www.ice.org.uk/getattachment/knowledge-and-resources/best-practice/specifying-successful-standards/Specifying-Successful-Standards-July-2012.pdf.aspx> accessed 13 March 2018.

[302] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Unleashing the Potential of Cloud Computing in Europe", COM (2012) 529 final (27 September 2012), 8.

presumption of conformity, or even exerting other forms of 'pressure' on companies to adopt certain standards.[303]

In relation to certifications, various forms of government recognition, depending on the legal effect, can be distinguished.[304] The CE marking process,[305] developed as part of the New Approach offers a presumption of conformity with the European rules on safety, health and the environment, and acts as 'passport' for market entry in the EU.[306] Due to the central role of harmonised standards, the New Approach has had a huge impact in the standardisation uptake within the EU.[307]

The proliferation of brands, labels and marks that are being used in the market has created some confusion for the public, which is commonly held to be unable to properly recognise and understand the purpose of these labels.[308] The 2011 Eurobarometer survey on consumer empowerment, demonstrated that EU-wide logos present on product packaging can be unknown to a large number of consumers (e.g. the Ecolabel) or are generally known to consumers but misunderstood by them (e.g. the CE mark on electrical equipment and toys).[309]

Other surveys[310] and research reports[311] show that certification marks are generally recognized by consumers, but their purposes are not always clearly identified. People surveyed on the meaning of the CE marking, for instance, believe that the CE mark is a certificate of European origin or a European quality mark, when the CE mark in fact ensures the conformity with the European regulation on safety, health and environment. This demonstrates that the uptake of certifications

[303]For XBRL-standards. See: https://www.icaew.com/technical/information-technology/business-systems-and-software-selection/making-information-systems-work/it-standards-and-the-digital-economy. Panel four: XBRL, last accessed 9 March 2018.

[304] A study led in 2003 by Tilburg University on behalf of the Dutch government suggested to classify the authorities' recognition of certification depending upon the legal value granted to the scheme: 1. schemes with a legal value (erkenningsvariant); 2. schemes offering the only way for a regulated body to prove its compliance with the law (toelatingsvariant) and 3. schemes representing a means, amongst others, for demonstrating the conformity with the law (toezichtsvariant).
Dutch Ministry of industry 'Kabinetsstandpunt over het gebruik van certificatie en accreditatie in het kader van overheidsbeleid' [Cabinet view on the use of certification and accreditation within the governement policy] (2003).
See also Philip Eijlander et al. 'De inkadering van certificatie en accreditatie in beleid en wetgeving. Schoordijk Instituut, Centrum voor Wetgevingsvraagstukken' (2003) Universiteit van Tilburg.

[305] Council Resolution 85/C136/01 of the 7th of May 1985. A full presentation of the basics of the CE marking process can be found in the 'Blue Guide' on the implementation of EU product rules issued by the European Commission, 2014, 6. Available:
<http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=7326> accessed 12 March 2018.

[306] See Chapter 3 p. 42f.

[307] CRISP project, Consolidated report on security standards and certification CRISP project, p. 341.

[308] Mark R Barron, 'Creating Consumer Confidence or Confusion? The Role of Product Certification in the Market Today' [2007] 11(2) Marquette Intellectual Properties Law Review 427.

[309]http://www.aim.be/news/article/smarter-logos-better-informed-consumers.-aim-beuc-joint-initiative, accessed: 8 March 2018.

[310] Commission Staff Working Document on Knowledge-Enhancing Aspects of Consumer Empowerment 2012-2014, 'Consumer attention and understanding of labels and logos', (2012) (SWD, Final, 19.7.2012 4.1), 26.

[311] Paul van der Zeijden et al,'Keurmerken, erkenningsregelingen en certificaten; klare wijn of rookgordijn? Zoetermeer: EIM Onderzoek voor Bedrijf en Beleid", 2002.

aimed at European citizens requires not so much a multiplication of labels and marks, but also to regularly communicate the meaning of the existing labels.

6.4.7. **Implementation**

Technical and financial conditions for the implementation of the standards and the certification schemes widely influence their uptake.

Consortia standards are sometimes only accessible under restrictive licencing agreements and international formal standards can only be obtained against payment of a fee that is often considered burdensome by, especially, SMEs.

The quality of the standards is another important factor. The ICE's study[312] underlines that "The principal issue with standards is to determine how to make them simpler to understand, ensure that the number of standards is minimized, provide the right balance between prescription and flexibility and ensure there is an efficient system to manage derogations and change."

The lack of skilled competences available in companies for applying the standards, aligning internal processes and to eventually prepare a certification represents another challenge for companies, especially the smallest ones.[313] Certain certification schemes set the bar for the requirements so high that they stay unreachable to most of the applicants while, at the opposite, other schemes[314] offer such lax conditions they do not represent a credible option for the applicants. The correct balance in the requirements to ensure the schemes accessibility and reliability represents a key uptake factor.

Two different and additional costs influence certification uptake. The most obvious is related to the certification process, during which the applicant requests the paying service of certification auditors. In certain schemes,[315] the certification process is done and charged apart and in addition to the assessment process. However, an important portion of the costs in the process lies as well in the preparation of the certification, being the effort required by the applicant to align its internal processes with the certification requirements. This effort requires the applicant's internal resources with, sometimes, the help of

[312]Specifying successful standards. Infrastructure Steering Committee (ISC), (2012). Available:<https://www.ice.org.uk/knowledge-and-resources/best-practice/specifying-successful-standards> accessed 12 March 2018.

[313] Eliza Charlemagne et al. , 'Certification: A Sustainable Solution? Insights from Dutch Companies on the Benefits and Limitations of CSR Certification in International Supply Chains' [2015], 16. Available: <https://mvonederland.nl/sites/default/files/media/Certification%20-%20a%20sustainable%20solution_0.pdf> accessed 12 March 2018.

[314] Civic Consulting, 'A Pan-European Trustmark for E-Commerce: Possibilities and Opportunities', 11

[315] See Chapter 2. Annex 2 on existing data protection certification schemes (Europrise, ePrivacy App Privacy by Design Ryerson University).

additional external resources. The preparation can be a long and costly endeavour depending the scope and state of the preparations of the applicant.

Overall certification costs may even become prohibitive for smaller companies in the case of numerous and strict requirements. This could lead applicants to have to weigh the options between the effort to obtain a certification and the benefit of having it. Boiral et al.[316] identified behaviours in the ISO 9001 certification where applicants, only looking for the credentials, applied minimal and superficial compliance to obtain it. As mentioned, setting the right balance between the requirements ensuring schemes reliability and ensuring accessibility, is a key factor in certification uptake.

As regards the implementation costs of standards it is of importance to know what extent companies are able to define a business case to adopt a standard.[317] Other relevant implementation related elements include the extent to which national standards are harmonised with international standards[318] and the extent to which standards provides adequate flexibility.[319]

6.4.8. **Drivers**

One of the main drivers for applying standards is the belief that standardisation improves the productivity and speeds up the economic growth[320] of companies. Of related relevance is also the extent to which a standard can provide an incentive associated with the risk mitigation, financial betterment or increased workload.[321]

If the impact of standardisation on companies financial results is no longer challenged[322], the most frequently cited benefits by researchers[323] is that standardisation improves the company's

[316] Olivier Boiral, 'ISO Certificates as Organizational Degrees? Beyond the Rational Myths of the Certification Process' (2012) 33(5-6) Organization Studies 635.
[317]ForXBRL-standards. See: https://www.icaew.com/technical/information-technology/business-systems-and-software-selection/making-information-systems-work/it-standards-and-the-digital-economy. Panel four: XBRL, last accessed 9 March 2018.
[318] CRISP, Consolidated report on security standards and certification CRISP project, D.2.2. p. 341
[319]https://www.ice.org.uk/getattachment/knowledge-and-resources/best-practice/specifying-successful-standards/Specifying-Successful-Standards-July-2012.pdf.aspx, last accessed 9 March 2018.
[320]Peter Swann, 'The Economics of Standardisation: An Update' [2010] Report for the UK Department of Business, Innovation and Skills (BIS) and AFNOR, 'The Economic Impact of Standardisation: Technological Change, Standards and Growth in France, [2009] Association Française de Normalisation, Paris.
[321]https://www.ice.org.uk/getattachment/knowledge-and-resources/best-practice/specifying-successful-standards/Specifying-Successful-Standards-July-2012.pdf.aspx (accessed 9 March 2018). The full argument reads as follows: "However, it is clear that organisations and teams can react very positively to incentives associated with risk mitigation, financial betterment or increased workload. When combined with a framework that fosters collaboration, the right incentives do generate the necessary behaviors for change to occur."
[322] MartiCasadesús, et al., 'Benefits of ISO 9000 implementation in Spanish industry' (2001). 13(6) European Business Review 327.
[323] Juan José Tarí et al., 'Benefits of the ISO 9001 and ISO 14001 Standards: A Literature Review' (2012) 5 Journal of Industrial Engineering and Management 297; see also Frank Wiengarten et al., 'A Supply Chain

efficiency, customer satisfaction and relations with employees. Standards implementation will be fostered when an organisation itself sees the adoption of a standard as a particular priority.[324]

The wide uptake of ISO 9001 could be linked, Cochoy[325] interestingly argues, to the fact, that the standard implementation becomes the justification of the job of the workers in charge of managing the processes. Another relevant factor might be that the process description and the identification of its owner represents also a convenient way to monitor the workers of a company.[326]

Standardisation has also been used to secure and streamline the supply chain,[327] outsourced in countries without management background. Standardisation can also be 'enforced' through competitive pressure.[328]

With regards to certification, Bartley et al.[329] argue that this instrument is being used by multinationals as a risk management tool to ensure a minimum legal ground to which to measure their activities in countries in which the legal framework remains underdeveloped.

Conroy et al[330] argue that certification is commonly used by multinationals to manage the moral pressure placed on them by NGOs concerning the environment and labour conditions in developing countries.

Certification offers a reliable means for businesses to demonstrate their good will to the regulator. Certification is sometimes also used by companies as a signal for promoting the selective qualities of products

View on Certification Standards: Does Supply Chain Certification Improve Performance Outcomes?', *ISO 9001, ISO 14001, and New Management Standards* (Springer 2018).

[324]For XBRL-standards. See: https://www.icaew.com/technical/information-technology/business-systems-and-software-selection/making-information-systems-work/it-standards-and-the-digital-economy. Panel four: XBRL, accessed 9 March 2018.

[325] Franck Cochoy et al., 'Comment l'écrit Travaille l'organisation : Le Cas Des Normes ISO 9000' (1998) 39–4 Revue Française de Sociologie.

[326] Ibid.

[327] "Les normes internationales appartiennent à l'infrastructure de la mondialisation. Selon les estimations, elles affectent jusqu'à 80 % du commerce mondial" in Jean-Christophe Graz, 'Quand Les Normes Font Loi Topologie Intégrée et Processus Différenciés de La Normalisation Internationale' (2004) volume XXXV, no 2, juin 2004 Revue Études internationales 233. For XBRL-standards, see: https://www.icaew.com/technical/information-technology/business-systems-and-software-selection/making-information-systems-work/it-standards-and-the-digital-economy. Panel four: XBRL, accessed 9 March 2018.

[328] Temple (1997b) as referred to in Swan (2010), p. 16, for ISO 9000 standards in UK. Swan (2010), p. 16 adds: "Grindley (1992, 1995) concluded however that the competitive incentives to adopt formal standards were limited and companies seeking competitive advantage are best to seek this through establishing their product as a de facto standard."

[329] Tim Bartley, 'Transnational Governance and the Re-centered State: Sustainability or Legality?' (2014) 8 Regulation & Governance 93. See also Blair M, Williams C and Li-Win L, 'The Roles of Standardisation, Certification and Assurance Services in Global Commerce' 2.

[330] Michael E. Conroy, *Branded! How the Certification Revolution Is Transforming Global Corporations* (New society publish 2007). See as well: Tim Bartley , 'Certification as a Mode of Social Regulation' [2011] *Handbook on the Politics of Regulation* 441 and Tim Bartley, 'Certifying Forests and Factories: States, Social Movements, and the Rise of Private Regulation in the Apparel and Forest Products Fields' (2003) 31 Politics & Society 433.

or services. Article 42 GDPR makes certification an optional communication tool available for controllers aiming to demonstrate their compliance with the law. Certification informs, assures the regulator, and the end user that a claimed conformity is regularly and independently verified.

Certification distinguishes the certified products and services from the non-certified ones. Thus, it can be used as a promotion tool for communicating on the selective qualities of the certified products and services. Certification offers a collective brand[331] signalling specified requirements have been met and are regularly checked. It can be used as a substitution brand by producers unable to afford the design of their own commercial brand.[332]

Certification can however also function as an entry barrier.[333] The European CE marking process does not allow foreign manufacturers to market their goods in the unique European market without declaring their products' conformity with the European rules on safety, health and environment. European standards on safety and health have been adopted worldwide.[334]

The low uptake reached so far by data protection certification,[335] in Europe, demonstrates that a strong incentive is required to assure better uptake of the GDPR's certification.

6.4.9. Interim conclusions: overview of uptake factors for technical standards and certifications

We conclude this chapter with an overview of uptake factors for standards and for certifications based on the description of relevant factors[336] as set out in the previous paragraph, further literature

[331] Franck Cochoy, 'De l'"AFNOR" à "NF", Ou La Progressive Marchandisation de La Normalisation Industrielle' (2000) 18(102) Réseaux 63.
[332] Ibid 65.
[333] The approval process managed by the French agency ASIP-Santé studied in the selection of 15 schemes will shortly require from health data storage processors to be certified by an accredited third party before starting their storage activity.
[334] Mark Rotenberg and Daniel Jacobs, 'Updating the Law of Information Privacy: The New Framework of the European Union' (n 84) 605.
[335] Apart the JIPDEC PrivacyMark that has been widely adopted, the other 14 schemes have been adopted by less of 100 bodies.
[336] It should be noted that literature into factors influencing the uptake of standards and certifications is often sector specific and relating to certain (types of) standards (like ISO 9000, accounting standards etc.) or certificates The results of these analyses cannot automatically be deemed equally applicable to the adoption of all (types of) standards and certifications, and across all sectors in society. Some of the outcomes could be sector specific, due to for instance the level of technological sophistication in a specific sector, earlier experiences with adopting standards or certifications, economic considerations etc. etc. Even within the entire range of information technology related standards, the 'susceptibility' of standards for the effects of certain intervention mechanisms could be specific for a certain type of standard, subject matter related or otherwise specific. For instance, it could be imagined that the nature and dynamics of 'data protection' as subject matter for standards could result in a different 'uptake profile' than would apply for safety related standards. The same holds for certifications. Although the respondents almost completely validated the choices made based on literature review, conclusions about the validity of these uptake factors are still subject to the limitations following from the limited number of respondents to the survey.

review[337], the results of the survey and the practical experience in assisting companies in achieving compliance with information technology related rules and regulations, and mitigating related risks. This overview will contribute to designing policies for applying mechanisms for stimulating the use of standards and certifications.

A first conclusion is that the notions 'trust', 'recognition', 'implementation' and 'drivers' constitute effective labels to describe the main categories of uptake factors for both standards as well as certifications. We will hence present the relevant uptake factors under these headings.

Uptake factors for standards

1. The notion 'trust' extends to especially the following uptake factors for standards:
   - the extent to which the standardisation process is inclusive, balanced and transparent
   - the level of the quality of standards;
   - the extent to which standards over time prove to be a reliable tool providing effective solutions;
   - the extent to which there is an efficient system to manage derogations and change;
   - the extent to which compliance with standards raises trust in organisations.

2. The notion 'recognition' extends to especially the following uptake factors for standards:
   - the level of endorsement of the standards by government (related) institutions, in particular Data Protection Authorities and the European Union;
   - the level of acceptance and endorsement of standards by the market (customers, business partners, competitors, industry associations, …);
   - the level of compliance pressure by business partners, customers and other market actors (e.g. insurance companies);
   - the extent to which auditors attach value to compliance with a standard.

[337] Consumer Research Associates Ltd., Certification and Marks in Europe, A Study commissioned by EFTA, European Free Trade Association, January 2008. <http://www.efta.int/sites/default/files/publications/study-certification-marks/full-report.pdf>, accessed 12 March 2018; Rowena Rodrigues et al. 'EU Privacy seals project. Comparison with other EU certification schemes. Final Report Study Deliverable 2.4' (2014); BEUC, "UNICE – BEUC e-Confidence project" (2002) Available <http://www.beuc.org/BEUCNoFrame/Docs/1/BNNPBBOBFJLIJFFIDLOMCBNOPDBY9DWDPN9DW3571KM/BEUC/docs/DLS/2002-01026-01-E.pdf> (accessed 12 March 2018); Civic Consulting, A Pan-European Trustmark for E-Commerce: Possibilities and Opportunities, A European Parliament Study, IP/A/IMCO/ST/2012-04, Berlin, July 2012

3. The notion 'implementation' extends to especially the following uptake factors for standards:
   - previous experiences with implementing other standards;
   - the costs of acquiring standards/ the pricing of standards by standards bodies;
   - the costs of implementing standards;
   - the extent to which companies are able to define a business case to adopt a standard;
   - the extent to which the standards provides adequate flexibility/adaptability, e.g. in terms of recognising special sectoral needs or needs of SME's;
   - the extent to which national standards are harmonised with international standards;

4. The notion 'drivers' extends to especially the following uptake factors for standards:
   - clarity of the standards/ the extent to which standards are easy to understand;
   - unambiguity of the standards;
   - 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 supply chain pressure. This can vary from mandatory application to e.g. offering price reductions when a certain standard is adopted;
   - the level of competitive pressure;
   - the extent to which the organisation itself sees the adoption of a standard as a particular priority;
   - the extent to which a standard can provide an incentive associated with risk mitigation, financial betterment or increased workload;
   - sanctions (e.g. penalties, denial of license etc.) in case of non-compliance.

Uptake factors for certifications

1. The notion 'trust' extends to especially the following uptake factors for certifications:
   - the extent to which a certification is deemed reliable;
   - the extent to which a scheme considered as trustable;

- the extent to which the scheme owner is considered as trustable;
- the extent to which a certification contribute to the image of the organisation that obtained the certification;
- the extent to which a schema has a clear function and scope;
- the extent to which adequate communication takes place regarding (the performance of) the scheme, its scope and functions;
- the level of public awareness about privacy/data protection schemes in general and the given scheme in particular.

2. The notion 'recognition' extends to especially the following uptake factors for certifications:
   - 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 endorsement of certifications by industry associations
   - the level of acceptance and endorsement of standards by the market (customers, business partners, industry associations, …);
   - the extent of recognition of certifications in other EU member states.

3. The notion 'implementation' extends to especially the following uptake factors for certifications:
   - costs of obtaining certifications (out of pocket costs, internal resources);
   - costs of maintaining certifications;
   - availability of staff;
   - the level of flexibility/adaptability of the scheme, e.g. in terms of recognising special needs of companies operating in certain sectors or SME's;
   - previous experiences with certifications.

4. The notion 'drivers' extends to especially the following uptake factors for certifications:
   - the extent to which a certification is effective;
   - the level of compliance pressure by business partners, customers and other market actors (e.g. insurance companies);
   - the extent to which competitors take out such certification;
   - the legal (protective) effect of certifications under the GDPR;
   - the extent to which a certification provides additional cyber security.

6.5. Discussion and recommendations

Relevant standards

- In the context of privacy/data protection, currently overall most relevant are international standards promoted by ISO and IEC. Especially a number of standards in the ISO 27000 series (information security) is being recognised by the market as being relevant, and could be considered for further recommendation taking into account the constraints and scope of Art. 42 and 43 GDPR. Standards from the ISO 29000 series (privacy standards) are only partially recognised (by large enterprises) and seem to have a much lower uptake in the market.
- The survey indicates that there is a structural lack of knowledge in the market as regards the availability of technical standards relevant in the context of privacy/data protection. The body of standards relevant in the context of privacy/data protection is much larger than currently recognised by the market.
- The information to the market about the availability and significance of privacy/data protection related standards should be significantly improved. The survey results seem to indicate that especially information provided by authorities could be effective in stimulating the use of privacy/data protection related standards.

- Relevant stakeholders (industry associations, SMEs and large enterprise) seem to favour European and international standards over national ones. In promoting standardisation in the field of privacy/data protection the EU should maintain its focus on these levels.

- The body of technical standards relevant to data protection certifications is evolving rapidly. This is to a large extent triggered by the introduction of the GDPR and in the context of the growing societal awareness of issues like data protection and cyber security. Various standardisation bodies have included or expanded the development of relevant standards in their work plans, including ISO and the European standardisation organisations (CEN, CENELEC and ETSI).
  The above indicates that, although there is wide range of standards available, experts hold the view that there is still a significant amount of standardisation work to be done for establishing an adequate body of standards covering all relevant aspects in the field of privacy/data protection.

- The proliferation of standardisation activities in the field of security and other privacy/data protection related topics inherently bears the

risk of multiplication of efforts and competition between national, regional and international standard setting bodies. This calls for close monitoring and, where possible, adequate coordination. The development of privacy/data protection related standards on the international level is, although in part also stimulated by the introduction of the GDPR, not necessarily aimed at creating only 'GDPR compliant' standards. This calls for monitoring of the developments and ensuring that European interests are adequately met in the international standardisation arenas. On-going efforts will be needed to secure an adequate level of inclusiveness in the standardisation process in order to stimulate the development of standards that are recognised by all parties (including SMEs) as being relevant, as well as that these standards recognise the specific needs of companies in various sectors, and are being considered as affordable to implement.

- In this context, careful consideration should also be given to (forms of) standard setting, including development of guidelines, model implementations, recommendations and other forms of guidance, taking place on sectoral level in the industry. Recognition of the value of the guidance documents developed in these fora is expected to contribute to a higher uptake of authoritative documents, including formal standards.

Uptake factors: standards

- The notions 'trust', 'recognition', 'implementation' and 'drivers' constitute effective labels to describe the main categories of uptake factors for standards relating to privacy/data protection. In each of these categories a wide range of relevant uptake factors can be distinguished. These factors relate to both specifics of standards as such (costs, quality etc.) as well as to contextual factors, including legal value, market impact and consequences of non-compliance.

- Industry seems to consider especially the following uptake factors for standards of importance[338]:

    - *economic considerations*:
        - costs of acquiring standards (mainly SME's);

[338] The limited response to the survey does not allow for drawing further conclusions between the views of SMEs and large industry.

- costs of implementing standards, and
- level of business advantage.

- *endorsement of standards by authoritative sources*, mainly:
  - Data Protection Authorities;
  - European Union, and
  - (other) government bodies.

- *quality considerations*:
  - the extent to which standards are unambiguous and clear;

- *trust*:
  - the extent to which compliance raises trust of clients in their organisation;

- *compliance*:
  - the extent to which implementing the standard contributes to legal compliance;

- *cyber security*:
  - the extent to which implementing standards provides additional cyber security.

Uptake factors for certifications

- The notions 'trust', 'recognition', 'implementation' and 'drivers' constitute effective labels to describe the main categories of uptake factors for standards. In each of these categories a wide range of relevant uptake factors can be distinguished. These factors relate to both specifics of an individual certification (costs, available staff, expertise, effectiveness etc.) as well as to contextual factors, including legal value, supply chain impact, public awareness and the certification market.

- Industry seems to consider especially the following uptake factors of importance[339]:

    - *economic considerations*:
        - costs of acquiring (and maintaining) a certification;

    - *endorsement and recognition of certifications*:
        - Data Protection Authorities;
        - European Union;
        - (other) government bodies;
        - industry associations;
        - recognition in other EU member states; and,
        - the extent to which competitors take out such certification;

    - *quality considerations*:
        - the extent to which the certification is effective;

    - *image/value*
        - the extent to which certification contributes to the image of companies;
        - the extent to which customers or business partners value the certification;

    - *legal protection*:
        - the legal (protective) effect of certifications.

[339] The limited response to the survey does not allow for drawing further conclusions between the views of SMEs and large industry.

7. Other mechanisms to promote and recognise the GDPR data protection certification mechanisms

7.1. Introduction

In this Chapter we present an overview of other potential mechanisms to promote and recognise the GDPR data protection certification mechanisms, in view of Article 43(9) GDPR. This is done on the basis of a literature study, the survey addressing business, industry associations, SMEs, and the Workshops organised in the framework of the study.[340]

The actions 'promoting and recognising' certifications are aimed at influencing the behaviour of (in particular) companies, a significant part thereof being SMEs. Within the context of the GDPR, approved certifications are considered an important instrument for providing guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor.[341]

The possible measures that can be used to promote and recognise the GDPR data protection certification mechanisms can be quite diverse and can be categorised in various ways, including in terms of the addressees:

- the parties involved in offering and implementing data protection certifications (legal experts, consultants, auditors, certification bodies, accreditation bodies);
- EU and national legislators and enforcement authorities;
- controllers and data processors, including SMEs.

Another important distinction, also in view of the authority granted to the Commission under the GDPR, is between legislative (forms of regulation and enforcement) and non-legislative measures. The first category includes amongst others: enforcement on EU and national level, providing legal clarity as to the status of GDPR related certifications, increase in the legal protective effect of certification and ensuring mutual recognition etc.

Non-legislative measures also cover a wide range of measures, including awareness raising, information and training, financial support (including tax incentives and subsidies), public procurement, support to development of, and access to, relevant standards, certification supply side measures, impact assessment and monitoring business compliance costs.

[340] See Annex 6.
[341] Recital 77 GDPR.

In the next two sections, we present the results of the survey, followed by an overview of the measures based on a structure combining the elements mentioned above.

7.2. Survey results on certifications

In the survey, several questions related, directly or indirectly to the other mechanisms that could promote and recognise the GDPR data protection certification mechanisms. Relevant results are described below.[342]

First, we examined reasons for low uptake level of certifications:

7.2.1. **Low uptake level**

Only 10% of SME-respondents and 38% of large industry respondents have already obtained a privacy/data protection related certification.[343] The background reasons for having not (yet) obtained a certification are diverse. The main reasons given by the respondents to justify this situation are the following ones:

- prohibitive costs;
- lack of information;
- no legal or market requirement;
- no measurable/significant effect in terms of goodwill of the public;
- lack of dedicated resources;
- not ready yet/in progress;
- not yet required by customers.

The views of industry associations as regards the uptake of data protection/privacy certifications among their members are in line with the above findings.[344] It is unlikely that this will change on the short term. The vast majority of both SME's and large industry respondents have not yet decided whether or not to consider taking out a privacy/data protection related certification in the near future.[345]

7.2.2. **Investments**

Industry associations considered the factors "time", "money/costs" and "level of expertise" of comparable weight when evaluating the

[342] Due to the limited number of respondents the results of the survey are not representative for the entire field of industry associations, certification bodies, standardisation bodies, SMEs and large enterprises. They are illustrative for a number of perspectives that can be found among the stakeholders of the respective stakeholder groups.
[343] See Chapter 6.
[344] See Chapter 6.
[345] See Chapter 6.

necessary investments for achieving compliance with privacy/data protection rules and regulations.[346] Certification bodies considered both price and process as key factors for incentivising SME's to adopt privacy/data protection certifications.[347]
Certification remains costly, as stated by over two thirds of the surveyed bodies[348], and it is not likely that EU businesses are eager to invest in such a costly procedure without strong and tangible incentive(s). In other words, without any requirements from customers or authorities, or some tangible benefits for businesses, data protection certification is unlikely to develop.

7.2.3. **Sources for obtaining information**

Industry associations mainly rely on the authorities (European Union, national governments, Data Protection Authorities) for obtaining information that could improve their awareness about privacy/data protection related certifications.[349] Industry (both SMEs and large industry) additionally attach significant value to its internal experts (data protection officer, IT-department).[350] Interestingly, both groups of respondents attach much less value to (commercial) external sources (consultants, business literature, consultants, lawyers).

7.3. Survey results on standards

In the survey, several questions related, directly or indirectly, to other mechanisms to promote and recognise standards. Although the focus of this chapter is on mechanisms to promote and recognise certifications, due to the close link between standards and certifications, we also include the results of the questions that focused on standardisation in this chapter.

The main lessons from the survey are presented in the following section.

7.3.1. **Incentives**

Industry associations considered both financial incentives, training opportunities, better information (availability, market requirements) and certainty about the legal effect very significant in making the

[346] See Annex 5.
[347] See Chapter 6.
[348] See Chapter 6.
[349] See Annex 5.
[350] See Annex 5.

decision to promote compliance with privacy/data protection related technical standards amongst their members.[351]

7.3.2. **Need for information, and sources**

Industry associations mainly rely on the authorities (European Union, national governments, Data Protection Authorities) for obtaining information that could improve their awareness about the availability and effect of privacy/data protection related technical standards.[352] The role of, specifically, technical experts (IT-department, consultants) and external information sources (business magazines, websites) was considered of less significance. The role of the internal DPO was considered of moderate importance.

The feedback from industry associations interestingly highlights that data protection standardisation is something new for associations' members; they perceived a high need among their members for more information about the availability of relevant standards. Over 70% of the survey respondents[353] underlined the lack of reliable information about what the market requires in this area.

Hence, a preliminary task for the authorities to ensure an uptake in this area could be to jointly assess the business needs with the help of the industry associations.

Another interesting lesson from industry associations' feedback stresses the need for staff training about existing privacy standards and, consequently underlines the current low level of awareness in businesses on this topic.

7.3.3. **Need for leadership**

As mentioned above, the results indicate that the authorities (EU, DPA, governments) should take a leading role in raising business awareness in standardisation in the field. The survey participants did not favour any form of the authorities in this information task, perhaps considering each of them should contribute to improving information on its own scope.

The role of internal staff in companies in the process (source for information, actor) can be an important way towards the standardisation in relation to how data protection will be handled.

In our view, the endorsement by technical IT teams towards standardisation could improve its uptake. Ultimately it concerns standards that impact the technical infrastructure of a company, as well

[351] See Annex 5.
[352] See Annex 5.
[353] See Annex 5.

and the tension traditionally found in many organisations between compliance functions and business/IT should not be fuelled by addressing only one of these functions in companies. It is also important to communicate that data protection related standards are neither pure technical nor 'compliance-only'. A joint compliant/technical effort will bring forth the best results. The information actions of authorities and business organisations should thus be explicitly organized in the direction of IT departments. When aimed at decision makers, information concerning the upside of implementing privacy/data protection related standards should primarily be addressed to the top management of SMEs and in large industry companies also to the middle management.[354]

7.3.4. **Need for incentives**

Even though only one respondent noted that 'law is the only relevant incentive',[355] the results of the survey clearly indicated that industry associations and their members are waiting for concrete incentives to apply standardisation in relation to certification in the field of data protection. The results stress that the financial incentives and the level of certainty about the legal effect would help drive the standardisation uptake.

This result again highlights the special status of standardisation that is seen as technical measures aiming to help with compliance to regulations. This basic ambiguity might explain why industry representatives simultaneously expect some financial and regulatory incentives for endorsing such rules.

In our opinion, there are additional considerations for the limitations of standardisation in the field of data protection in its current form. Thus far, international standards dealing with data protection issues do not fully reflect the EU legal requirements.[356] As the WP29 has stressed in the case of the ISO/IEC 27018 cloud computing standard, the standard is a catalogue of best practices, a "good collection of non-compulsory, non-exhaustive and non-maximalist controls" that may be implemented.[357] It remains uncertain to what extent international standards will adequately address data protection obligations stemming from the GDPR.

[354] See Chapter 6.
[355] See Annex 5.
[356] Paul De Hert, Vagelis Papakonstantinou, Irene Kamara, 'The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection' (2016) 32(1) Computer Law and Security Review 16.
[357] Article 29 Data Protection Working Party, 'Opinion 02/2015 on CSIG code of conduct on cloud computing', WP232, adopted on 22 September 2015, 10 ff.

7.4. Other mechanisms: findings

In this paragraph, we highlight the different legislative and non-legislative measures that could be considered to promote and recognise the GDPR data protection certification mechanisms.

7.4.1. **Legislative measures and related instruments**

7.4.1.1. Introduction

The certification mechanism on which the GDPR builds, is a complex system shaped by (the powers and actions of) the Member States, the Commission, the DPA's and the European Data Protection Board. The formal role of the Commission relating to certifications is primarily set out in articles 42(1), 43(8) and 43(9).[358]

The formal legislative role of the Commission is delineated by articles 43(8) (delegated acts for specifying requirements to be taken into account for the data protection certification mechanisms) and 43(9) (implementing acts laying down technical standards for certification mechanisms and mechanisms to promote and recognise those certification mechanisms). The task of the Commission under article 42 (1) (encourage the establishment of certification mechanisms) is of a different nature and covers potentially a broad spectrum of (non-legislative) activities (to be undertaken in coordination with the Member States, the DPAs and the European Data Protection Board).Next to this, the Commission could – either on the basis of article 42(1) or the institutional role of the Commission - also play a role in advising, stimulating and coordinating actions to taken by other stakeholders on the basis of their powers under the GDPR. Promotion of (the use of) certification mechanisms under the GDPR can be achieved in several ways, either by legislative and non-legislative actions. Although the GDPR entrusts the Commission with certain empowerments under article 43(9) to promote (the use of) standards and certification mechanisms, it still needs to be evaluated whether in a given situation taking an implementing act is the optimal instrument for achieving this goal. Other types of actions that could be taken by the Commission under article 42(1) and/or by other actors (for instance DPA's or the EDPB) - either independently or combined with legislative steps – might in some cases be preferred. For instance, because these are more efficient, quicker to implement or provide an advantage otherwise (policy wise, political, procedural, in terms of costs ...). An example of an alternative way of promoting standards is offered by the 'CBP Guidelines for security of personal data' issued by the Dutch DPA in

[358] See analysis in Chapter 2.

2013. In these Guidelines, the DPA refers to various standards as (optional) building blocks for creating an adequate security framework, thereby providing tangible guidance for market players. The above implies that for promoting the use of standards and certification mechanism, the various stakeholders should – jointly – consider which instrument or instruments should be deployed. Consequently, our recommendations should be primarily understood as setting out desired objectives. Although we describe in more detail below which action the Commission could take under 43(9), the ultimate choice and implementation of a specific instrument requires further consultation with the relevant stakeholders, tailoring actions to authorisations, procedural scrutiny, broader policy considerations etc. Providing further guidance in this respect falls outside the scope of this study.

7.4.1.2. Starting points for a framework for selecting standards

Article 43(9) empowers the Commission to take implementing acts laying down technical standards for certification mechanisms. In the previous Chapter we provided an overview of standards relevant for the various aspects of (establishing) certification mechanisms, in particular design, accreditation, certification and monitoring.

A formal recommendation of a specific standard requires careful consideration as to the appropriateness and quality of the standard. In our view that should include amongst other things the following aspects:

- the standard should be sufficiently rich in what it covers. This in order to prevent promoting a range of standards each dealing with sub-issues;
- the standard should be consistent with the GDPR. This in order to prevent promoting standards conflicting with legal principles included in the European data protection framework;
- the standard should be sufficiently mature in that the chance that it will be overtaken by another more mature standard should be considered to be low;
- the standard should be non-ambiguous in what they it aims for, promoting broadly shared, clear purposes.
- To the extent the standard is not a European standard, the criteria of Annex II of Regulation 1025/2012[359] (Requirements for

[359] Regulation (EU) No 1025/2012 of the European Parliament and of the Council

the identification of ICT technical specifications) could be taken into consideration as well. These criteria[360] address the source, process and content of a standard.[361] According to Regulation 1025/2012, the standard issuer should be a non-profit making organisation which is a professional society, industry or trade association or any other membership organisation. As regards procedural aspects, the drafting process should conform to openness, consensus, and transparency[362]. Regarding the content of the standard specification, the criteria are maintenance, availability, intellectual property rights, relevance, neutrality and stability, and quality.[363]

7.4.1.3. Current body of relevant standards

As described in the previous Chapter and Annex 5E, there is currently a significant body of standards relevant for the certification mechanisms. The current base of relevant standards is clearly dominated by

of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council, OJ L 316, 14.11.2012.

[360] Article 3 and 4 of Annex II

[361] Formally, Annex II refers to a 'technical specification'.

[362] Article 3 Annex II: "(…)
(a) openness: the technical specifications were developed on the basis of open decision-making accessible to all interested parties in the market or markets affected by those technical specifications;
(b) consensus: the decision-making process was collaborative, and consensus based and did not favour any particular stakeholder. Consensus means a general agreement, characterised by the absence of sustained opposition to substantial issues by any important part of the concerned interests and by a process that involves seeking to take into account the views of all parties concerned and to reconcile any conflicting arguments. Consensus does not imply unanimity;
(c) transparency:
(i) all information concerning technical discussions and decision making was archived and identified;
(ii) information on new standardisation activities was publicly and widely announced through suitable and accessible means;
(iii) participation of all relevant categories of interested parties was sought with a view to achieving balance;
(iv) consideration and response were given to comments by interested parties."

[363] Article 4 Annex II: "The technical specifications meet the following requirements:
(a) maintenance: ongoing support and maintenance of published specifications are guaranteed over a long period;
(b) availability: specifications are publicly available for implementation and use on reasonable terms (including for a reasonable fee or free of charge);
(c) intellectual property rights essential to the implementation of specifications are licensed to applicants on a (fair) reasonable and non-discriminatory basis ((F)RAND), which includes, at the discretion of the intellectual property right-holder, licensing essential intellectual property without compensation;
(d) relevance:
(i) the specifications are effective and relevant;
(ii) specifications need to respond to market needs and regulatory requirements;
(e) neutrality and stability:
(i) specifications whenever possible are performance oriented rather than based on design or descriptive characteristics;
(ii) specifications do not distort the market or limit the possibilities for implementers to develop competition and innovation based upon them;
(iii) specifications are based on advanced scientific and technological developments; (f) quality:
(i) the quality and level of detail are sufficient to permit the development of a variety of competing implementations of interoperable products and services;
(ii) standardised interfaces are not hidden or controlled by anyone other than the organisations that adopted the technical specifications.

international standards in particular from ISO and IEC. This holds for all aspects of (establishing) certification mechanisms.

Some of the ISO and IEC standards have been endorsed as European standards as well[364], others are only available as international standards. Currently there is still a significant number of standardisation initiatives under way with the aim of strengthening the body of data protection related standards and GDPR related standards in particular. This both in terms of reviewing existing standards as well as developing additional standards. In the previous Chapter, we highlighted some developments currently under way in ISO, IEC, ETSI and CEN-CENELEC. Overall, the development of a coherent and adequate set of European standards fully aligned with the principles and mechanisms of the GDPR still needs substantial efforts.
Notwithstanding their added value, a significant part of the currently available international standards is not suitable for integral, unconditional recommendation in the context of promoting standards for certification mechanisms of Art. 42 and 43 GDPR. ISO and IEC publish guidelines, codes of practice, requirements, and frameworks. Not all of these types of documents are directly useable in the current setting. Codes of practice are generally oriented towards a specific community of practitioners and the elements thereof are sometimes too much content related to be of value in a broader setting. A practical example of the above can be found in the WP29 comments relating to ISO/IEC 27018[365]: *"(…) the WP29 would like to stress that ISO/IEC 27018 is a catalogue of best practices for cloud providers acting as processors. It describes a list of controls to improve privacy. This standard is only a good collection of non-compulsory, non-exhaustive and non-maximalist controls that may be implemented. Thus ISO/IEC 27018 is not built to be used as a standalone document for certification. It can be used in conjunction with ISO/IEC 27001 which allows a certification. ISO/IEC 27001 does not take into account the specificities of the protection of privacy such as impacts on the individuals, but it ensures a high level of protection of information in the organization's interest. The addition of good practices based on ISO/IEC 27018 may therefore help to ensure that privacy is better taken into account but it does not prove that privacy risks are taken into account. ISO/IEC 27018 should ideally be used only after assessing the risks on the privacy of the persons concerned, in order to treat them in a proportionate way. For now, no published standard describes the way to conduct this*

[364] For example: ISO/IEC 17065, ISO/IEC 27001 and ISO/IEC 27002.
[365] Working Party 29 Opinion on the Cloud Select Industry Group (C-SIG) Code of Conduct on data protection for Cloud Service Providers, Available at:<http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf> accessed 2 May 2018)

process. Ongoing work at the ISO may help to fill this gap in the next few years."

Some relevant international standards promote a management system approach that conflicts with the scope of certification as specified in Article 42(1) GDPR. For instance, subsection 1 of ISO/IEC 27001 reads "This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving *an information security management system* within the context of the organisation." Subsection 1 of ISO/IEC CD 27552[366] (still under development), provides "This document specifies the requirements and provides guidance for establishing, implementing, maintaining and continually improving a *Privacy Information Management System (PIMS)* in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization."
Certain ISO/IEC standards include provisions that clearly conflict with the GDPR. Subsection 6.2.2 of ISO/IEC 29101 provides "The transfer of sensitive PII (Personal Identifiable Information) should be avoided unless it is necessary to provide a service that the PII principals has requested, it fulfils a business requirement for offering the requested service, or unless it is required by law." Management of sensitive data suggested in ISO/IEC 29101 appears misaligned with Article 9 GDPR that is more restrictive than the standard.[367]

Other ISO/IEC standards do not cover the full requirements set of the GDPR. For example A.10.11 of ISO/IEC 27018 about Contract measures applying to cloud processor reads: "Contracts between the cloud service customer and the public cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data is not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor. Also, subsection A.10.12 Sub-contracted PII processing adds "Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor.' Certain requirements set in the GDPR are missing in the standard. For instance, Article 28(2) GDPR requires the processor "to not engage another processor without prior specific or

[366] ISO/IEC CD 27552 Information technology -- Security techniques -- Enhancement to ISO/IEC 27001 for privacy management -- Requirements
[367] The standard suggests avoiding whereas Article 9(1) GDPR prohibits processing of this type of personal data.

written authorisation of the controller". Article 28.3g requires a return or deletion of the data at the end of the service contract that is not covered by the standard.

7.4.1.4. Recommending standards

Any standard that would be considered for recommendation by means of an implementing act should obviously be adequately aligned with the principles, terminology, mechanisms and scope of the GDPR. The above shows that this does not yet hold for at least a substantial part of the current body of data protection related standards.
For evaluating the consequences thereof we distinguish between two categories of standards:

(1) standards covering procedural aspects, such as ISO/IEC 17065 relating to conformity assessment, and

(2) standards providing the basis for describing the certification criteria against which compliance with the GDPR will be demonstrated.

For standards *relating to the criteria for certification* the adequate alignment with especially the terminology, principles and mechanisms of the GDPR is much more critical than for standards covering primarily procedural aspects. The latter type of standards are generally to a large extent neutral towards the criteria used in the relevant certification process.

Given the above considerations as to the GDPR related adequacy of the current body of available standards we do currently not recommend taking implementing acts under article 43(9) to support implementation of these standards.
Further and much more in-depth analysis of the level of GDPR conformity of the existing (ISO/IEC) standards library could be a next step in creating the right conditions for decision making about issuing implementing acts under article 43(9). Such a next step, which is clearly out of scope of the present study, should result in a detailed overview of missing requirements and disconnects between these standards and the GDPR, on the basis whereof a strategy could be designed on how to bridge the gaps. Options would probably include contributing to international standard revision process and drafting new (European) standards.

Promoting *procedural standards* by means of implementing acts could nevertheless be considered. Potential candidates include ISO/IEC standards in the 17000 series that could ensure that the certification

procedures and accreditation are aligned with a common framework. An example could be ISO/IEC 17011:2017 (Conformity assessment - Requirements for accreditation bodies accrediting conformity assessment bodies). This standard specifies requirements for the competence, consistent operation and impartiality of accreditation bodies assessing and accrediting conformity assessment bodies. For further details regarding the ISO 17000-series we refer to Chapter 6 and Annex 5E. In taking further steps we recommend that the starting points for selecting standard as set out above will be taken into account.

It is interesting to note that in the framework of the eIDAS Regulation[368], seemingly similar concerns as to the level of alignment of a relevant ISO-standards (specifically ISO/IEC 29115) have been encountered in drafting an implementing act.[369] In Recital 3 of the implementing act it was noted that: *"International standard ISO/IEC 29115 has been taken into account for the specifications and procedures set out in this implementing act as being the principle international standard available in the domain of assurance levels for electronic identification means. However, the content of Regulation (EU) No 910/2014 differs from that inter- national standard, in particular in relation to identity proofing and verification requirements, as well as to the way in which the differences between Member State identity arrangements and the existing tools in the EU for the same purpose are taken into account. Therefore the Annex, while building on this international standard should not make reference to any specific content of ISO/IEC 29115."*

Finally, we note that promotion of standards that could support companies in demonstrating compliance with GDPR provisions (hence standards relating to *certification criteria*) seems much more effective for promoting compliance with the GDPR than promoting procedural standards. This as the latter category is primarily addressing the needs of certification bodies, accreditation bodies and the like, generally being professionals in that field or having the means to secure the necessary expertise and skills, including accessing and implementing the relevant standards. This in contrast to organisations seeking compliance with the

[368] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114. See also Chapter 4 of the Report.
[369] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, OJ L 235, 09.09.2015, p. 7-20.

GDPR for which accessing and implementing standards is often a serious challenge. This obviously holds especially for SMEs.
In view of the above, we recommend that priority will be given to ensuring development of a body of standards that can be an adequate basis for drafting certification criteria under the GDPR. This preferably in the form of European standards, and potentially with the procedure of standardisation requests issued by the European Commission to the ESOs, based on Art. 10 of the Standardisation Regulation.[370]

7.4.2. **Non-Legislative measures and related instruments**

In addition, certain non-legislative measures could be promoted by the authorities to help effectively steer the behaviour of companies in applying data protection certification mechanisms.

On the basis of 15 schemes studied, literature[371] and practical experience with guiding companies in ensuring compliance with legislation, the research team recommends the following positive and negative 'rewards'. With the notion of negative "rewards", the research team intends highlighting the measures encouraging or requiring a certification to leverage a right or a privilege.

7.4.2.1. Positive rewards

In describing the positive rewards we will categorise the relevant factors as follows:
1. Direct economic incentives;
2. Certification supply side measures;
3. Supporting the developments and access to relevant standards;
4. Awareness raising;
5. Providing information and training; and,
6. Provide other forms of support to implementation and achieving compliance.

A. Direct economic incentives to foster the uptake of certifications:

- adopt appropriate measures in support of SMEs, such as affordable access to data protection-related legal advice / know-how (e.g. making available vouchers for obtaining services from qualified

[370] See Chapter 2 p. 29
[371] We refer as well to the literature for Chapter 6.

consultants and certification bodies. See for instance the innovation voucher programs[372] in the Netherlands);

- consider reduced taxes/levies for companies that have obtained an approved certification;

- engage with insurance companies to foster accessibility of GDPR related liability insurance (including for SMEs), building on obtaining an approved certifications.

B. Certification supply side measures:

- stimulate an open market for commercially operating certification bodies;

- limit publicly owned schemes to certain activities or markets (SME's) to prevent unfair competition market for private schemes;

- engage with insurance companies to foster availability of liability insurance for certification bodies;

- launch a competition for innovative, low cost approaches;

- act as a launching customer for certification bodies;

- act as a launching customer for innovative solutions (e.g. aimed at SMEs);

- maintain a fair level playing field in the market of data protection certifications, (including ensuring enforcement against fraudulent certification providers);

- active monitoring of the quality of issued certificates (to prevent risk of race to the bottom);

- effective whistleblowing mechanisms for reporting of concerns or wrong doings in the certification market and complaint handling.

C. Support the development of, and access to, relevant standards underlying certifications:

[372] See: www.oecd.org/innovation/policyplatform/48135973.pdf. (Accessed 15 March 2018) OECD: Innovation vouchers are small lines of credit provided by governments to small and medium-sized enterprises (SMEs) to purchase services from public knowledge providers with a view to introducing innovations (new products, processes or services) in their business operation.

- provide (further) support to especially SMEs to foster participation in the development of relevant standards and to stimulate the recognition of the effectiveness, relevance and affordability of implementing standards;

- engage with industry associations and sectoral bodies to explore the options for more effective use of model implementations, recommendations and other forms of guidance developed on sectoral level. These forms of guidance could not only provide a basis for stimulating an uptake of as well formal standards but could also be a starting point for 'fast track' types of standard setting building on existing authoritative documents established in a sector.

- engage with standards bodies and certification bodies via the creation of a dedicated expert group on GDPR certification;

- make key standards available for SMEs for a reduced or zero fee. The current practice of free access at the offices of national standardisation bodies is not considered adequate by especially SMEs;

- improve access to standards databases covering all relevant standards. The current level of accessibility is an obstacle as is also recognised by standardisation experts.

D. Awareness raising:

- launch awareness campaigns in which in particular authorities promote the importance of compliance with data protection legislation (incl. media campaigns);

- launch awareness campaigns in which in particular authorities supporting the value of certifications (both for companies and data subjects);

- Provide pre-assessment tools. An example could be checklists for other data protection related topics as made available by the UK's Information Commissioners' Office or the Self-assessment Privacy Toolkit offered for free by Ryerson University and Hewlett Packard[373] or the CEN CWA 15499-2.[374]

[373] Hewlett Packard/Privacy by Design Centre of Excellence "Privacy Toolkit" http://h41111.www4.hpe.com/privacy-toolkit/overview.html

[374] CWA 15499-2: Personal Data Protection Audit Framework (EU Directive EC 95/46) - Part II: Checklists, questionnaires and templates for users of the framework.

E. Provide information and training:

- ensure accessibility of information on approved certifications, criteria, accredited certification bodies etc. Establish links to the EDPB page and additional documents/laws/procedures at national level;
- support sectoral implementations fostered by industry association or otherwise;
- stimulate training programs
- introduce (funding for the development of) a EU recognition scheme for data protection related training programs.

F. Provide other forms of support to implementation and achieving compliance:

- Compare the EU Cybersecurity Act aiming at establishing data security related certifications[375];
- align to the extent possible with other certifications in the field (facilitate building block approach);
- support the development of structured 'pathways' to achieving compliance that are aligned with the needs and capabilities of SMEs.

7.4.2.2. Possible negative 'rewards'

With regard to 'negative incentives' we differentiate between direct and indirect enforcement.

A. Direct enforcement, either by or on behalf of EU, governments or supervisory authorities:

- applying penalties/sanctions, especially combined with publicity;
- introducing approved certification as pre-condition for validity of data processing agreements;

B. Indirect enforcement by EU/governments:

- relate EU market access to adherence to approved certifications.

[375] Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'') COM(2017), https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en, accessed 10 March 2018.

- include certification as a requirement in public procurement procedures of the EU and of national governments.

8. Certification as an instrument for data transfers

8.1. Introduction

Flows of personal data within the EU Member States and from the EU to other countries are necessary for international trade.[376] The GDPR modernised the provisions on data transfers to controllers and processors in third countries, outside the EU. The rationale remained the same: the transfer of the data should not lower the standards of protection the data subjects enjoy within the EU. In other words, the level of protection should not be undermined.[377] At the same time, while maintaining the Commission Adequacy Decision as legal ground for data transfers to third countries (or international organisations), the legal grounds for transferring data by means of appropriate safeguards were significantly expanded. One of those novel means aiming to provide appropriate safeguards is the approved data protection certification mechanisms of Art. 42, together with legally binding and enforceable commitments.[378]

Article 42(2) of the GDPR provides for a specific incentive for companies to seek certification. Due to the novelty of certification in the GDPR and as a legal basis for data transfers, this chapter sheds light at specific aspects of the role of the data protection certification mechanisms as providing appropriate safeguards for data transfers.

The Chapter proposes high-level/generic safeguards, necessary to be included in a data protection certification mechanism, which qualifies as a data transfer mechanism according to art. 46(2)(f) GDPR. To this end, we analysed other existing 'data transfer mechanisms' such as Standard Contractual Clauses for Transfers to third countries, Binding Corporate Rules and the requirements set by the WP29 under the Data Protection Directive regime and recently endorsed by the EDPB.[379] During the exercise, the limitations of this analysis were considered regarding first, the differences of certification and the other transfer mechanisms, and second, the different legal basis of existing data transfer mechanisms (Directive 95/46/EC and national laws, instead of the GDPR). Next, the chapter presents an analysis of APEC CBPR, as an established certification system used for cross-border data transfers.

Building on the findings of Tasks 2 and 3, and the identified safeguards in this Task, we also discuss the strengths and weaknesses of a stand-alone certification mechanism for data transfers in relation to generic certification mechanisms.

[376] Recital 101 GDPR.
[377] Recital 101 GDPR.
[378] Art. 46(2)(f) GDPR.
[379] European Data Protection Board, Endorsement 1/2018, available: https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents.pdf (accessed 1 July 2018).

8.2. Scope and purpose of Art. 42(2) certification

In the absence of a Decision of the European Commission on the adequacy of the level of protection in a third country or international organisation, the GDPR provides other legal bases for transfers of personal data to third countries or international organisations (IO) by means of appropriate safeguards. Adequacy Decisions concern the overall assessment of a third country's legal order in reference to the protection offered, including the implementation and enforcement of the protection. The instruments for data transfers provided by Art. 46 GDPR (approved data protection certification mechanism, binding corporate rules, standard contractual clauses, or other as in Art. 46(2) GDPR), however, should shield the data transfer even in the case that the data is transferred to a third country where the legal order does not provide adequate data protection guarantees. An assessment of the legal order of the third country is neither formally part of the obligations of the controller or processor in Art. 46 GDPR nor part of a prior authorisation by the competent DPA.

Certification based on Art. 42(2) for the purpose of demonstrating appropriate safeguards presents certain differences in relation to certification for the purpose of demonstrating compliance with the GDPR (Art. 42(1)), as shown in this Chapter.[380] One of the significant differences is the applicant for certification: while the applicant controller/processor in the Art. 42(1) certification mechanisms is subject to the GDPR, the applicant controller/processor in the Art. 42(2) certification mechanism is the data importer established in a third country and not subject to the GDPR, or at least, is not subject when applying for certification.[381] This difference has impact from both substantive and organisational perspectives, such as:

- The certification criteria aim to show that the controller/processor has taken all the necessary measures to provide the appropriate safeguards for data transfers, instead of how a controller/processor complies with legal obligations stemming from the GDPR. The certification criteria of the certification of Art. 42(2) need to reflect mainly the essence of the relevant GDPR provision.

- The certification bodies need to ensure that the certified controller/processor provides all the necessary documentation,

[380] This view is also implied by the Guidelines adopted by the EDPB 1/2018 which will publish separate guidelines to address the identification of criteria for certification mechanisms as transfers tools. (p.4)

[381] See Art.3 (2) GDPR for territorial scope of the Regulation in cases of controllers/processors not established in the Union.

access to its premises, and continues to conform to the certification criteria after certification is granted. While this is the case also for certifications of Art. 42(1) GDPR, the establishment of the certified entity in a third country requires planning, processes, and commitment of resources of the certification body.

Accordingly, the supervisory authority/NAB need ensure that the accredited certification body is in the position to monitor the controller/processor in the third country.

8.2.1. **Applicant for certification: data importer**

As mentioned in the previous section, Art. 42(2) GDPR provides that controllers or processors that are not subject to the GDPR may adhere[382] to data protection certification mechanisms, seals, and marks in the context of personal data transfers to third countries. Controllers and processors established in third countries or the international organisations (data recipients/importers) may, by means of adherence to a data protection certification mechanism, demonstrate the existence of appropriate safeguards to controllers or processors that are subject to the GDPR and wish to export personal data (data exporters). It is thus *the controller or processor in the third country or the I*O that needs to have its processing certified according to Art. 42(2). This is a novelty of the Regulation, which gives entities not being subject to the GDPR the possibility to conform nonetheless to its principles, when importing data from a controller/processor subject to the Regulation. Even though the importer controller/processor does not need to comply with the entirety of the GDPR, it needs to process personal data in a way compatible with the GDPR. This is the task of the data protection certification mechanism of Art. 42(2) GDPR: to ensure that the data importer has taken all the necessary measures to provide appropriate safeguards to personal data it has received. As explained later in this chapter, the adherence to data protection certification mechanisms have to be coupled with legally binding and enforceable commitments of the data importer to apply the appropriate safeguards.

8.2.2. **Object of certification: processing**

As with certification for demonstration of compliance of Art. 42(1) GDPR, the object of certification for the purpose of demonstrating appropriate safeguards of Art. 42(2) GDPR is the *processing* of a controller or processor.[383] For example, a call centre or a company

[382] The term 'adherence' used in Art. 46 implies that a controller or processor in a third country has applied for and successfully been granted the data protection certification of Art. 42(2) GDPR. Adherence in the context of Art. 46 GDPR should not be confused with a unilateral decision to conform to a set of criteria.
[383] See analysis in Chapter 2 of the Report p. 18 f

providing IT services established in a non-adequate country may opt to apply for data protection certification in line with Art. 42(2) GDPR. The object of certification will be a processing operation or a set of processing operations. This means that after a successful certification process, the company established in a third country or the international organisation will receive a certification (and the right to use a seal and/or mark) that attests that the processing operation(s) of personal data in the company conforms to the (approved) certification criteria of the data protection certification mechanism. Management systems or products cannot *as such* be certified in the context of Art. 42 GDPR certification, as explained in Chapter 2 of the Report. However, it is often the case that such elements and other assets are also examined in the course of the evaluation stage, in so far necessary to assess the main object of certification, namely the processing operation under evaluation. When for example, a data storage centre in the non-adequate country applies for certification, it would have to demonstrate *inter alia* that the level of security measures undertaken does not lower the protection of the personal data, as required by the GDPR. In making the assessment on the security measures, the certification body (or supervisory authority when providing certification) will have to also include control points relating to the IT management system of the organisation.

8.2.3. **Certifying entity**

The provisions of Art. 43 GDPR apply to the certification mechanisms for data transfers. The certifying entity therefore is either a certification body, accredited in line with Art. 43, or a supervisory authority. Considering territorial competence limitations of the EU supervisory authorities in combination with the practical difficulties the certification of a data importer in a third country would entail, it is most likely that accredited certification bodies will mostly conduct certification in the case of Art. 42(2) certifications. As explained earlier in this section, the location of the controller/processor in a third country carries administrative and resources' burdens, since it entails that the accredited certification body needs to have the ability to conduct the certification process and effectively monitor the issued certification in that third country. The certification bodies need in turn to be accredited by either an EU MS supervisory authority and/or an EU MS National Accreditation or both. The following scenarios are possible:

- **The accredited certification body is established in the EU and provides cross-border certification in the third country.**

The certification body should ensure that it is able to conduct its work effectively in the third country. Usually, this is possible with the

collaboration of a local certification body in the third country. The local certification body (sub-contractor) performs its activities on behalf of the CAB and is a separate legal entity and organisation. In establishing a collaboration with a local certification body, the certification body established in the EU should seek warranties that the local collaborator lives up to the high standards of the GDPR accreditation requirements of Art. 43, the requirements of the Regulation 765/2008, and the ISO/IEC 17011. In addition, the local certification body should be able to provide certification on the basis of the ISO/IEC 17065. A safe way to ensure high standards is the accreditation of the local certification body (in the third country) by the national accreditation authority of that country participating in the International Accreditation Forum.[384] Accordingly, the accreditation of the certification body established in the EU needs to examine, among other issues, how the certification body established in the EU will carry out and manage its activities in the third country and the certification body needs to provide convincing evidence to the accreditation authority.

- **The accredited certification body has establishment(s) in the EU and/or in a third country.**

In this scenario, the certification body has establishments in an EU MS and several other locations and offers multi-site certification services. We consider the establishment in an EU MS –along with any other potential locations- as a necessary component for the accreditation process of the certification body, especially for reasons of territorial competence of the EU MS supervisory authority when acting as an accreditor. In the case of NABs providing accreditation, their competence is established by the fact that a certification body operates in the EU market and the certification body is in turn required to seek accreditation in the MS of establishment.[385] In the latter case, there is however the possibility, in general, that a certification body, accredited in a third country by an accreditation authority signatory to IAF, requests an EU NAB to issue a declaration of equivalence.[386]

In line with the above, there are two possibilities for the accredited certification body offering multi-site certification services:

[384] The International Accreditation Forum (IAF) establishes cooperation agreements between accreditation bodies accrediting certification and provide for multilateral mutual recognition arrangements (MLA) with the aim to establish confidence concerning the reliability of the results of the signatories. See more on IAF in Chapter 5.
[385] Recitals 19 and 20, Art. 7(1) Accreditation Regulation, see also: European Commission, CERTIF 2013-02– Requirement to seek accreditation in the Member State of establishment - IMP N006, http://ec.europa.eu/DocsRoom/documents/6259/attachments/1/translations (accessed 25 July 2018) p.22f
[386] European Commission, CERTIF 2013-02– Requirement to seek accreditation in the Member State of establishment - IMP N006, http://ec.europa.eu/DocsRoom/documents/6259/attachments/1/translations (accessed 25 July 2018) p.22f

A. It has its main establishment in a third country and/or an establishment or branch in an EU MS, or

B. Its main establishment is in the EU and operational branches in one or more third countries (where data importers are located).

According to IAF, a considerable factor for the accreditation process is the 'critical location(s)', which is the site or sites where the certification body performs its key activities.[387] Usually, it is the head office that receives the accreditation certificate and the local sites perform accreditation within the scope of the granted certificate.[388]
In case of a certification body, accredited in line with Art. 43 GDPR, that has its main establishment in the third country, the certification process and the surveillance of the granted certification are easier than in the alternative scenario. Difficulties might arise in terms of how the accreditation and coordination with the EU supervisory authorities is organised. Examples from other fields offer useful lessons:[389]

- *1st approach: Non-EU certification bodies are notified to the COM under Mutual Recognition Agreements.*[390]

Mutual Recognition Agreements in relation to Conformity Assessment (MRA) and the Protocol on European Conformity Assessment (PECA) are government-to-government agreements according to which the importing country accepts certification of compliance to its legal/regulatory requirements performed in the exporting country.[391] The PECA principles were defined in the Internal Market Council meeting of 13 March 1997 and the negotiating guidelines adopted by COREPER on 4 June 1997.[392] The authorities of the importing country accept conformity certificates delivered by a Conformity Assessment Body located in the exporting country (i.e. a domestic certification body that is designated by the authorities of one Agreement Partner and

[387] According to IAF, key activities include: Key activities include: policy formulation; process and/or procedure development; process of initial selection of inspectors and, as appropriate; contract review; planning conformity assessments; review and approval of conformity assessments. IAF/ILAC-A5:11/2013, https://www.iaf.nu/upFiles/IAFILACA5MutliLateral_Mutual_Recognition_ArrangementsPub_Nov2013.pdf (accessed 20 July 2018)
[388] DAKKS, Accreditation of conformity assessment bodies with several locations, 71 SD 0 014, Revision: version 1.3, 02. August 2016, https://www.dakks.de/sites/default/files/dokumente/71_sd_0_014_e_multi-site_critical-location_20160802_v1.3.pdf (accessed 20 July 2018)
[389] The examples from different domains are only an indication of how certification systems in other fields are organised. We do not imply the direct applicability of such different systems to the case of Art. 42(2) certification mechanisms.
[390] European Commission, Implementation of Mutual Recognition Agreements on Conformity Assessment and Protocol on European Conformity Assessment, DG III/B/4/GM D(98), 24 July 1998
[391] MRAs are mentioned in the Council Resolution of 21 December 1989 on a Global Approach to conformity assessment
[392] http://europa.eu/rapid/press-release_PRES-97-75_en.htm

recognised by the other), without need for additional technical evaluation/administrative intervention. Designating Authorities must ensure that suitable CABs are identified, designated and can operate according to the requirements and the procedures of the other party's regulations as indicated in the text of the Agreement. The general requirements and procedures for designation are indicated in the Framework part of the Agreement and tend to be the same for all countries and all sectors in coherence with the general objectives of the MRA. To ensure a proper implementation of the agreements, a Joint Committee is established, composed by representatives of the contracting parties. Among other responsibilities, the Joint Committee is responsible in particular to give effect to the designation or withdrawal of CABs.[393]

- *2nd approach: Non-EU certification bodies directly approved by dedicated COM agency.*

Since January 2009, certification bodies (CBs) with activities outside the EU (whether based or not in the EU) with organic products destined for EU markets must demonstrate that they implement a control system and use a production standard which has been assessed as equivalent to the rules applied inside Europe.[394]
The Regulation 834/2007 on organic production and labelling of organic products lays down rules for the approval of control bodies (certification bodies) within Member States which requires accreditation to ISO/IEC 17065 and compliance with the production standards and control measures set out in the regulation.[395] The Regulation 1235/2008 requires that any organic product entering the EU must originate from a country system that has been deemed equivalent by the European Commission or be certified by an individual control body that has subjected itself to equivalence assessment and been approved by the Organic Unit of the Directorate General Agriculture (DG AGRI) of the European Commission.[396] The production standard used outside of the European Union may not be the text of the regulations as such but must be one designed for implementation in the third country. Control bodies

[393] Procedure for designation of CABs by non-Member countries http://ec.europa.eu/DocsRoom/documents/6417/attachments/1/translations (accessed 5 July 2018)
[394] https://ec.europa.eu/agriculture/organic/eu-policy/eu-rules-on-trade/control-bodies_en (accessed 5 July 2018)
[395] Council Regulation (EC) No 834/2007 of 28 June 2007 on organic production and labelling of organic products and repealing Regulation (EEC) No 2092/91, OJ L 189, 20.7.2007
[396] Commission Regulation (EC) No 1235/2008 of 8 December 2008 laying down detailed rules for implementation of Council Regulation (EC) No 834/2007 as regards the arrangements for imports of organic products from third countries, OJ L 334, 12.12.2008

must therefore issue to their operators applying for EU equivalence program a production standard of their own or a common standard designed for the purpose. This must be separately assessed as equivalent against the production standards contained in those same regulations.

To maintain the accreditation over time, the CAB issues a technical dossier sent every year to the COM. The dossier must contain:

- control activities carried out in each third country during the previous year
- results obtained, irregularities and infringements observed, and the corrective actions taken (within 30 days following the discovery)
- changes in the production standards and control measures applied
- other relevant changes
- the results of the on-the-spot evaluations,
- surveillance and multi-annual re-assessment by the assessment body.

8.2.4. **Presumption of existence of safeguards**

There is a presumption that once a data protection certification mechanism is approved by a supervisory authority in a MS or the EDPB in line with Art. 42(5) GDPR, the controller or processor adhering to such certification mechanism, provides the safeguards required for a data transfer pursuant to Art. 46 GDPR. Thus, the certification process needs to be thorough, since granting the certification entails that the data importer qualifies in principle to receive and process personal data from an EU data exporter.

The presumption of existence of safeguards offered by the adherence to an approved certification mechanism shifts a substantial burden both onto the supervisory authorities and the certification bodies. The approval of data protection certification criteria by supervisory authorities or the EDPB determines whether a certification mechanism provides all the necessary criteria to ensure that the certified controller/processor may *in principle* provide appropriate safeguards for data transfers. The certification body bears the burden to apply the criteria and determine whether they are respected and conformed to by the applicant data importer.

The exporter controller, who is subject to the GDPR remains liable towards the competent EU supervisory authorities to demonstrate the existence of the safeguards provided by the importer controller or processor, including that the certification is not revoked or withdrawn throughout the processing of transferred personal data.

8.2.5. Relation to other transfers tools of Art. 46(1) and added value of certification mechanisms

8.2.5.1. Binding Corporate Rules, Standard Contractual Clauses and certification mechanisms

The instruments of Binding Corporate Rules, Standard Contractual Clauses, and Data Protection Certification Mechanisms provide alternative tools for the transfer of personal data to controllers or processors in third countries or international organisations. In terms of substance, the three instruments embody a common underlying purpose, which is to ensure that data are being treated in a manner compatible with the GDPR after having been transferred to a third country. The issues therefore addressed in each instrument are not substantially different, as discussed later in this Chapter.

However, the three instruments also show distinctive characteristics in terms of target group, review layers of processing activities, and organisational issues.

Target group of certification: entities in the third country. While BCRs and SCCs are primarily addressed to the controller or processor that exports personal data, the 'selling point' of certification for the purpose of data transfers is the fact that it is addressed to entities established in third countries or international organisations, which are not subject to the GDPR. The entity that may apply and receive the certification is not data exporter, but the data importer established in the third country.
Any organisation in a non-adequate country or any international organisation that wishes to submit its processing to a certification body for the purpose of demonstrating the existence of appropriate safeguards is in principle free to do so. Data protection certification as a data transfer tool therefore does not necessarily require a pre-existing relationship between the data importer and the data exporter. This sort of de-coupling – at least at the certification stage – of the two actors offers significant advantages to both parties:

- data exporters may be assisted in their selection of controllers or processors who have already been audited by an independent accredited certification body and were granted certification, thus demonstrate the existence of safeguards.

- data importers planning to enter the EU market may submit their processing for certification and receive a data protection seal, as a means to show reliability and due consideration to data protection principles and rights in line with the GDPR.

Certification of the entities not subject to the GDPR are invited in this manner to apply the high protection standards of the GDPR, making the GDPR a point of reference in other jurisdictions.

Review layers of processing. Certification, as a third-party conformity activity, requires evaluation and decision-making by an independent body. This means that in relation to BCRs, certification includes an additional *external* control level: first the certification criteria are approved by EU DPAs or the EDPB. Upon application for certification, an accredited certification body (or an EU MS supervisory authority) evaluate the processing activity of the applicant controller or processor (importer) against the approved criteria (Art. 42(5) GDPR). Similarly, SCCs introduce an approval layer, as they are adopted by the supervisory authorities[397] or the Commission[398], but no additional layer of independent review, such as the review by the certification body or the dpa in the case of data protection certification mechanisms.

Organisational issues. The location of the data importer (applicant for certification) in a third country outside the Union and the need for review by the certification body requires structures for certification that are different from BCRs and SCCs. Being primarily linked to entities subject to the GDPR, BCRs and SCCs procedures are *managed* by the supervisory authorities from within the Union.
Data protection certification mechanisms however, require structures that enable accredited certification bodies to provide services to organisations established outside the Union. In fact, data protection certification mechanisms, as opposed to single approval processes, require regular monitoring after the certification is granted. The post-certification monitoring ('surveillance') is necessary to ensure that the conditions for granting the certification continue to be met, and thus the appropriate safeguards guaranteed with the certification continue to exist. Such organisational matters, while they require preparatory work in setting up a network of support, but they are deemed necessary for the success of certification as a data transfer tool.

8.2.5.2. Codes of Conduct and certification mechanisms

In terms of the relationship of Codes of Conduct as introduced in Art. 40 and 41 GDPR and data protection certification mechanisms, one can identify more commonalities than with the other transfers tools of Art.46 (1) GDPR. Both instruments are targeted to controllers and

[397] Art. 46 (2)(d) GDPR.
[398] Art. 46(2)(c) GDPR.

processors in third countries, they both involve an accredited entity providing assurance of the conformity to the criteria of the instrument and entail organisational issues for the accredited entity with regard to managing conformity to the transfer tool criteria outside the borders of the Union. The difference between the two instruments lies in their substance: Codes of Conduct of Art. 40 aim at offering a tool specifically tailored for the needs of specific sectors.[399] Codes of Conduct are drafted by trade Unions or associations representing controllers or processors and aim at calibrating the obligations of controllers or processors to the specificities of sectors.[400] Certifications on the other hand, do not need necessarily be targeting sectors, even though nothing in Art. 42 prohibits such mechanisms. This practically means that Codes of Conduct as a transfer tool are better suited for companies (controllers/processors) with sectoral, instead of multi-sectoral activity, given that there is already an approved Code of Conduct for that sector. In the case of companies with multi-sectoral activities, there would be substantial difficulty to adhere to multiple Codes of Conduct. Certification mechanisms as a transfer tool on the other hand have the potential to be a more flexible instrument, as the content – although needs address all the necessary issues to provide guarantees for the transfers – is not limited to the specificities of a sector, but can be sector-neutral and applicable to a broader range of controllers and processors.

8.3. Overview of roles of actors involved

The processing operation of data transfers adds complexity to the already complex certification landscape,[401] as it introduces new actors, namely data controllers or processors ("recipient" controllers or processors) in a third country or international organisation. One should not only think of a single recipient controller or processor in one third country, since there is a possibility of further onward transfers.
The graph below identifies the scenario of a single data transfer to a non-EU country and one onward transfer to another non-EU country. Certification is granted by an accredited certification body.

[399] Art. 40 also refers to the specific needs of SMEs, which is a common element with Art. 42.
[400] Recital 77 GDPR.
[401] See Figure 2-1 Overview of data protection certification under Art. 42 and 43 GDPR.

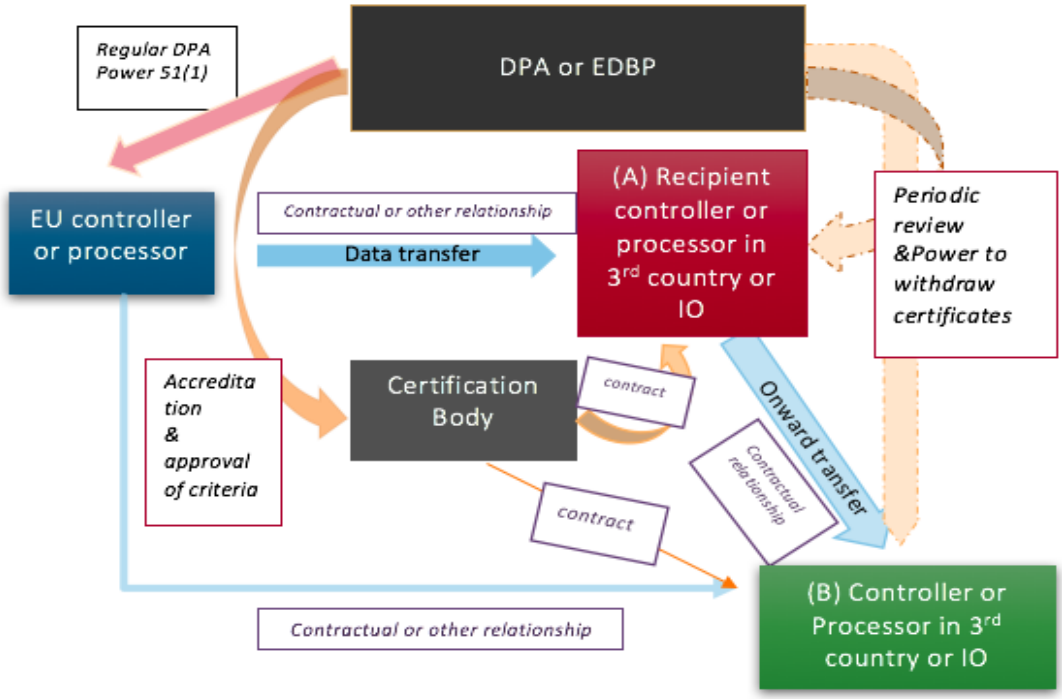


Figure 8-1 Overview of legal relationships in data transfers to certified controllers/processors in non-EU countries

In the graph above, the following relationships are identified:

- **Controller/processor established in the EU (exporter) and controller/processor established in a third country (recipient/importer):** This is the backbone relationship of the data transfer. The type of the relationship may vary depending the qualification of the actors as controllers, joint controllers, or processors. In any case, a contractual relationship will most likely, but not necessarily, be established.[402]

- **Recipient controller/processor (importer) and certification body granting the GDPR certification:** The controller or processor in the third country or IO needs to be certified in line with Art. 42 and 43 before he/she starts processing personal data. The data importer also needs to provide legally binding and enforceable commitments.[403] Usually, the certification body and the applicant for certification enter a contractual agreement which describes the conditions for granting the certification, obligations

[402] This is the case with data processors for example line with Art. 28(3) GDPR.
[403] See later in this Chapter.

of both parties and other relevant issues pertaining to the certification, as seen in Chapter 4 of the study.[404]

- **DPA/EDPB and controller/processor established in the EU (exporter)**: This relationship is not particular to certification or transfer. The data exporter is subject to the investigation powers of the competent supervisory authority in terms of the data processing carried out by the exporter itself and the data processors who are processing data on behalf of the data exporter or in collaboration with the data exporter.

- **DPA/EDPB and Certification Body:** As explained in a previous chapter,[405] a certification body needs to be accredited by the supervisory authority or a National Accreditation Body.[406] The DPA has the power to revoke accreditation when the conditions for which it was granted are no longer met. The DPA also approves the certification criteria.

- **Recipient controller/processor (importer) and competent DPA of an EU Member State or the EDPB:** This is an indirect relationship, not formally established in the GDPR, as the recipient controller or processor in the third country is beyond the jurisdiction of the DPA. The DPA is competent to oversee the data transfer, which is a processing activity itself. When it comes to the awarded certification, however, the DPA has the task and power to carry-out (periodic) reviews of certifications which have been issued[407] and order the certification body to withdraw certification when the conditions for its issuance are no longer met.[408] Thus, such powers of the DPA imply that – at least for the awarded certification – the recipient certified controller or processor is subject to the oversight of an EU DPA.[409]

- **Recipient controller/processor (importer) (A) and onward controller/processor (B):** The onward controller or processor needs to comply with the conditions for transfers.[410] If the country

[404] See p. 70f.
[405] See Chapter 5 on Accreditation.
[406] As provided in Art. 42 and 43 GDPR, it is also possible that the supervisory authority itself provides certifications, without a certification body. In this Chapter we focus on the scenario that involves a certification body due to 1. Its complexity 2. Its likelihood. It is more likely that certifications of non-EU controllers or processors serving the purpose of Art. 46 will be conducted by a certification body under the supervision of the DPA, rather than the DPA itself, for reasons which include resources and capacity.
[407] Art. 57(1)(o) and Art. 58(1)(C) GDPR.
[408] Art. 58(2)(h) GDPR.
[409] The agreement between the certification body and the certified entity may contain the agreement of the certified entity to be subject to the oversight of an EU DPA for issues pertaining to the granting, issuance, maintenance, and withdrawal of the granted certification.
[410] Art. 44 GDPR.

of the onward controller, or processor, offers an adequate level of protection, as decided by the Commission with an Adequacy Decision, there is no need for certification of the onward controller/processor. However, if that third country does not ensure an adequate level of protection, one of the safeguards of Art. 46 GDPR needs to be provided for.

- **Onward controller/processor and competent DPA of an EU Member State or the EDPB:** The same applies, as in the relationship between recipient controller/processor and DPA of an EU Member State.

- **Onward controller/processor and controller/processor established in the EU (exporter):** This relationship might be formalised with a bilateral contract, or be covered by a general authorisation of the EU data controller towards the recipient processor. In any case, since the onward processor is processing personal data on behalf of the EU controller, the latter is liable for any infringements of the GDPR.

8.4. Certification criteria and "appropriate safeguards"

The approved certification criteria are the backbone of the data protection certification mechanism. As discussed in Chapter 4, the certification criteria address substantial issues such as the legal grounds for the processing operation, the legal requirements of for example Art. 32 and how they are met by the applicant for certification. It is through conformity to the certification criteria that the data importer ensures that its processing does not undermine the level of protection guaranteed to data subjects in the Union. The topics of the criteria need therefore be informed by all those necessary elements in the GDPR that guarantee such protection.[411]

The GDPR replaced the term 'adequate safeguards' found in Art. 25 Directive 95/46/EC with 'appropriate safeguards'. Since the legal bases of Art. 46 GDPR allow transfers of data to countries that do not ensure an adequate level of protection, the safeguards provided need to correspond to elements of the type(s) of processing activities carried out by the applicant for certification.

Useful examples in that regard are provided by other instruments of Art. 46, that is the BCRs and the SCCs. We further consider the examples valuable for another reason: approved certifications such as data transfers mechanisms are introduced under the same provision in the GDPR as alternative (to each other) appropriate safeguards. Notwithstanding the scope of each instrument of Art. 46(2) GDPR, the *level of protection* offered by the Art.46 instruments should not differ. Each of the instruments of Art. 46(1) leads to the occurrence of data transfers, without prior authorisation by the supervisory authority, and is subject to the conditions and restrictions of Art. 46 GDPR.[412]

8.4.1. **Binding Corporate Rules**

Binding Corporate Rules (BCR) are a tool intended for transfers within the same corporation or in a group of enterprises engaged in a joint economic activity. Even though not explicitly foreseen in the Directive 95/46/EC, BCR are a tool that was developed under the Directive. The GDPR formalised BCR as a data transfer mechanism in Art. 46 and 47.[413]

Guidance from the WP29 on the content and key safeguards required in the BCR has been invaluable. The primary elements to be addressed in

[411] See Chapter 9 on the different certification models for data transfers.
[412] Together with the general principles for transfers, as provided in Art. 44 GDPR.
[413] See list of companies with concluded BCR procedures and the lead DPAs: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en

the BCR,[414] which are submitted to the supervisory authorities for approval, are the following:[415]

- **Information and transparency requirements**

The BCR needs to provide information about the structure and contact details of the group of undertaking or the group of enterprises engaged in a joint economic activity. It also needs to include the scope of the BCR, including the geographical and material scope. It also needs to provide an overview of the processing and data flows, the third countries where the data are intended to be transferred, as well as the purposes for processing, the type of data processed, and the types of data subject affected.[416]

- **Data Protection safeguards**

The BCR needs to specify the application of the general data protection principles apply to the group of companies that are subject to the BCR and the measures taken for the application of the principles. Under the general data protection principles Art. 47(2)(d) emphasises ("*in particular*") to purpose limitation, data minimisation, limited storage periods, data protection by design and by default, legal basis of processing, processing of special categories of data, measures to ensure security, and special safeguards for the onward transfers to controllers or processors not subject to the BCR. Particular attention is paid to the means provided by the group of undertakings to enable the exercise of the rights of the data subject. Article 47 GDPR requires both substantive and procedural rights to be safeguarded.[417]

- **Binding nature requirements**

The company or IO needs to explain in its BCR how its rules are both internally (within the group of undertakings or enterprises engaged in a joint economic activity) and externally binding.[418] Art. 47(1)(b) requires the companies to expressly confer enforceable rights on data subjects regarding the processing of their personal data. The companies need also accept liability for paying compensation to remedy breaches of the BCR by companies not established in the Union.[419] In addition, it should be clear that the burden of proof lies with the company instead of the individual. The WP29 has also advised the companies to introduce

[414] Art. 47 GDPR. Article 29 Data Protection Working Party "Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules" 2017, WP256.
[415] Article 29 Data Protection Working Party "Working Document Setting-up a framework for the structure of Binding Corporate Rules", 2008, WP 154 and Article 29 Data Protection Working Party "Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules", 2008, WP153.
[416] Art. 47 (2)(a)(b) GDPR.
[417] Substantive rights: Art. 12-22 GDPR, procedural rights: Art 77, 79 GDPR.
[418] Art. 47 (2)(c) GDPR
[419] Art. 47(2)(f) GDPR

information about the existence of sufficient assets of the company to cover potential compensation claims of individuals.[420]

- **Accountability**

There are several requirements in Art. 47 GDPR aiming at ensuring accountability of the group of undertakings or enterprises. Those include training programmes for the personnel with access to the personal data,[421] complaint handling processes, methods for verification of compliance such as audits, and description of tasks and qualifications of the data protection officer designated to internally monitor the application and compliance of the BCR.[422]

- **Cooperation with the supervisory authorities**

The group of companies or undertakings with joint economic activity should describe in its BCR the cooperation mechanism with the competent supervisory authority in order to ensure compliance with the BCR program of each of the companies.

- **Mechanisms for reporting and recording changes**

Another aspect already suggested by the WP29 and introduced in the GDPR is the reporting of changes.[423] The BCR should have mechanisms in place to deal with any changes that might arise, without compromising the function and effectiveness of the BCR programme. Examples are changes in the composition of the group, change of the Data Protection Officer, change in national legislation in one of the countries of the establishment of the companies.

8.4.2. **Standard Contractual Clauses**

Another way of making sure adequate protection is offered in data transfers is the adoption of the Standard Contractual Clauses (SCC). The SCC, which are drafted and published by the Commission, do not require prior notification to the DPA. The SCC impose obligations on both the exporter and importer (recipient). The Commission has published the following Models for SCC: 1. For EU controller to non-EU controller[424] 2. From EU controller to non-EU processor[425]

---

[420] Article 29 Data Protection Working Party "Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules", 2008, WP153.
[421] Art. 47(2)(n) GDPR
[422] Art. 47(2)(j) GDPR
[423] Art. 47(2)(k) GDPR
[424] Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC *OJ L 181, 4.7.2001,* http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32001D0497 and 2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32004D0915&from=EN
[425] See amendments to the Models after the Schrems case: Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard

The necessary elements included in the SCC relate to:

- Scope, description, and details of the transfer.
- Data processing principles applicable to the data transfer and the processing of the transferred data.
- Obligations of the exporter relating to among other issues the lawfulness of processing, technical and organisational measures to ensure security and confidentiality
- Obligations of the data importer (recipient)
  - The adoption of technical and organisational measures relating to data security (risk-based approach).
  - The adoption of procedures to ensure confidentiality and security of the personal data, including for persons under the authority of the importer controller.
  - To respect the principles and purposes of processing determined in the SCC.

In addition to the above necessary elements in terms of the range of obligations, several contractual clauses are introduced in the SCC to ensure implementation and enforcement of the obligations undertaken with the contract (for the recipient) or the data protection legislation (for the exporter).

- Third-party beneficiary clause and right of the data subject to be represented by an association.
- Liability clause, compensation for damages, including provision of evidence to the financial exporter of financial resources sufficient to fulfil its responsibilities.
- Indemnification.
- Dispute resolution (mediation and/or judicial redress) and jurisdiction.
- Duty of cooperation with the authorities.
- Governing Law.
- Appointment of contact point for complaint handling.

The standard contractual clauses, for the transfers from controllers to processors established in a third country and to sub-processors also established in a third country, contain a prohibition on the recipient processor from sub-contracting the processing without the prior written consent of the data exporter.[426] Such a clause maintains and in fact

contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council, *OJ L 344, 17.12.2016, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016D2297&from=EN*

[426]Art. 11 of European Commission "Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive

reinforces the overall accountability of the data exporter from all the activities and processing taking place on its behalf.[427]

8.4.3. Appropriate safeguards provided for by adherence to certification mechanisms

The overall aim of the certification criteria should be to demonstrate that the data importer has taken all the necessary measures to ensure that he/she provides appropriate safeguards for the data transfer. The GDPR provides that the safeguards of Art. 46 should *in particular* relate to compliance with the general principles relating to personal data processing and data protection by design and by default.[428] Beyond the processing principles of Art. 5, the safeguards in the certification mechanism reflect legal obligations of controllers and processors (Art. 24, 28 GDPR), security of processing, and a range of other legal requirements.

8.4.3.1. Timing of adherence to certification

The timing of establishing the contractual relationship between the certification body and the controller/processor in the third country is significant with regards to the content of the agreement and the scope of certification.

If we focus on the linear relationship[429], there are three main actors: the data controller/processor in the EU (exporter), the controller/processor in the third country or the international organisation (importer) and the certification body.

The relationship of the certification body with the data importer needs to develop before the data can be transferred, since the safeguards demonstrated with the granted certification need to be in place prior to any data transfer. It is possible that the relationship of the data recipient with the certification body exists even before the data recipient plans to conduct business with its EU based counterpart.

Certification may also take place after the EU controller/processor has come to a conditional agreement with the data recipient, but has to

95/46/EC of the European Parliament and of the Council" 2010, OJ L39/5, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010D0087&from=EN

[427] It should be noted that there is a pending case regarding the validity of the Standard Contractual Clauses as means of transfers providing appropriate safeguards under the Data Protection Directive regime. https://www.alstonprivacy.com/wp-content/uploads/2018/04/ref.pdf (accessed 15 June 2018). See Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 – Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Case C-311/18). http://curia.europa.eu/juris/document/document.jsf?text=&docid=204046&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12202343 (accessed 15 February 2019).

[428] Recital 108 GDPR.

[429] See Graph in p. 130

take place before the transfer occurs. However, certification may be a lengthy process, and the outcome may be negative for the applicant or corrective actions might need to be undertaken before the certification is granted. This should always be considered when certification is intended to be used as a transfer tool.

8.4.3.2. Certification criteria and appropriate safeguards

Building on the topics included in Art.47 GDPR for the BCRs and Recital 108 GDPR, we consider the following safeguards should be the minimum elements for a certification mechanism for the purposes of Art. 42(2) and Article 46(2)(f) GDPR in relation to processing operations.[430]

1. Certification criteria related to the conditions of processing

The certification criteria in this category should address the principles of processing (Art. 5 GDPR) and the legal grounds of processing (Art. 6 GDPR). As the cornerstones of the data protection legislation,[431] the lack thereof in the certification scheme would risk undermining the level of protection of the transferred personal data. The certification scheme should also look into how the data importer applies to the object of certification, namely processing operations,[432] the principles of data minimisation, purpose limitation and the other principles of Art. 5 GDPR to its processing.[433]

The specific scope of certification (e.g. data storage of HR data by an IT company offering services as data processor) determines which processing activity (-ies) is within the scope of certification. Accordingly, the evaluation of the processing of the data importer should be performed in relation to the specific scope of certification. Beyond the measures taken and policies adopted for specific types of processing, the auditor should also look at the overall structure and mechanisms of the data importer in place and its ability to provide the appropriate safeguards not only at a specific moment in time – when the evaluation takes place – but throughout the validity period of the granted certification.

The approved certification criteria should include a definition and brief description of the aim of each criterion, rather than proposing ways to fulfil the criterion, which is an element, open to the applicant of certification to demonstrate and the auditor(s) of the accredited certification body to assess. It should be noted that some of the topics require knowledge of the details of the data transfer such as for

[430] See also approach followed by the WP29 in the case of Adequacy Decisions. Article 29 Data Protection Working Party "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EC Data Protection Directive" Working Document, 1998, DG XV D/5025/98 and Article 29 Data Protection Working Party "Adequacy Referential (updated)"

[431] In the Schrems case, the CJEU provided that the regime of data transfers is complementary to the general rules established by the data protection law on lawfulness of processing. Case C 362/14 para 95.

[432] See p. 18

[433] For guidance on how the certification criteria should be formulated, see Chapter 4 of the Report.

instance the legal grounds for processing, which is not present when certification is granted prior to the data importer – exporter agreement. A certification body cannot determine in advance for example whether a data importer processes data in conformity with the grounds of Art. 6 GDPR, if the context and details of the data transfer are not known. The certification body can only assess the stated intention and the subsequent measures and policies of the applicant controller or processor to process personal data in line with one of the grounds of Art. 6 GDPR. When the context and type of transfers is known, if necessary, as mentioned before, the scope of data protection certification might be broadened.

2. Certification criteria related to data subjects' rights

The third cluster of topics to be addressed by certification criteria concerns data subjects' rights. The scheme should examine how a data importer enables both substantive and procedural data subjects' rights (right to an effective remedy). This requirement is stressed in both Art. 42(2) and 46 GDPR and has also been stressed by the CJEU in relation to the right of Art. 47 CFEU.[434]

3. Certification criteria related to responsibilities of actors

The approved criteria should also include control points stemming from the responsibilities of the applicants as controllers or processors. Data protection by design and by default (Art. 25 GDPR), data security (Art. 32 GDPR), records of processing activities (Art. 30 GDPR), data breaches (Art. 33 and 34 GDPR), data protection impact assessments (Art. 35 GDPR) and others. It should be noted here, that the fact that the certification applicant is not subject to the GDPR, and thus not subject to the above obligations, needs to be considered when determining the stringency of the certification criteria and developing the assessment methodology. At the same time, the certification scheme owner, when developing the certification criteria, should keep in mind that the level of protection of personal data should not be lower or incompatible with the level offered by the Union.

The *appropriateness* of the safeguards to a large extent will be determined by the nature and context of the data transfers. The appropriateness therefore of the safeguards, for which the exporter

[434] The Court provided that "The individual should be provided – by law – with the possibility to pursue legal remedies in order to have access to the personal data relating to him/her, so as to rectify or erase such data in line with Art. 47 Charter" Case C 362/14

controller/processor is responsible, is an open legal standard determined for each *type* of data transfer. The conditions of the transfer should, in general, ensure that the level of processing isn't lower than the processing of data within the Union.[435]

4. Assessment by the certification body

The certification body is responsible to assess whether the data importer conforms to the certification criteria provided in the data protection certification mechanism of Art. 42(2) GDPR. The auditor of the certification body should conduct a thorough audit of the processing activities under scrutiny in the certification process. The elements of the assessment could include:

- Documentation such as policies, commercial and employment contracts, Terms & Conditions, user manuals, document management and/or archiving systems, consent forms, privacy statements and policies.

- IT security measures, such as pseudonymisation and encryption, IT software and infrastructure, including back-up systems and storage systems.

- Work processes and procedures such as personnel access rights and authorisations to documents containing personal data, complaint handing and dispute resolution, processes for the exercise of data subject rights, review and facilitation of data subjects' requests.

In addition, the data importer should inform the certification body of any legal requirements or other commitments that might compromise or pose a risk to the conformity of the organisation to the certification criteria.

The exact methodology of assessing conformity to the certification criteria is a matter of determination by the entity drafting the certification scheme, pending the approval of the supervisory authority. Although no certification criteria have been yet approved in line with Art. 42 (1) or 42(2) GDPR, we should learn from practices in usual privacy or data protection certification practice as highlighted in Chapter 4 of this Report. EuroPrise for example, depending on the scope of certification and the entity to be certified, looks into technical aspects such as:

[435] Recital 108 GDPR.

- Physical access control
- Access to media and mobile devices
- Access to data, programs, and devices
- Identification and authentication
- Use of passwords
- Organisation and documentation of access control
- Network and transport security
- Incident management
- Temporary files
- Disposal and erasure of data
- Appointment and duties of a security officer
- Documentation and inventories, and others[436]

In general, there are several types of assessment methods, as prescribed by international conformity assessment standards, that a certification body may use to assess the conformity of the object of certification in a given assessment. An initial inspection for example is more suited for a product certification, while an auditor may also opt for assessment of a process and the quality control of an organisation, audit testing, field investigation/on spot audit and others.[437] The assessment methodology in a certification mechanism for data transfers may include a combination of methods.

8.5. Legally binding and enforceable commitments

Data transfers of personal data on the basis of certification are allowed only coupled with "binding and enforceable commitments."[438] Due to the lack of an obligation for the specific authorisation of the data transfer from the supervisory authority or an adequate level of protection in the third country (or international organisation), the GDPR requires additional commitments from the controller or processor in the third country, thus the recipient of the data. The additional commitments aim to facilitate the enforceability and binding effect of the safeguards as provided for by the granted certification. This section explores the concept of the commitments and the means and possible options for rendering the commitments of the data recipient binding and enforceable.

[436] See Public certification report (re-certification) of European Privacy Seal for VALid-SSD: https://www.european-privacy-seal.eu/EPS-en/Valid-ssd/ accessed 10 October 2018
[437] Breitenberg, Maureen A. The ABC's of the US Conformity Assessment System. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, Office of Standards Services, 1997.
[438] Art. 46(1)(f) GDPR.

8.5.1. **Content and types of commitments**

The data importer is obliged to commit to that he/she will apply the appropriate safeguards embedded in the approved certification (Art. 42(2)). It is common for certification agreements to include conditions for the maintenance of the granted certification. Such conditions are in practice commitments of the certified entity to continue to respect the certification criteria and to report to the certification body any change that might affect certification. In the case of certification as a tool for data transfers, commitments of the data importer to respect the criteria and overall conditions of the certification mechanism (including for example how to use the certification mark and others) may be part of the certification agreement between the certification body and the certified controller/processor in the third country.

However, it is also recommended that legally binding and enforceable commitments are given to the data exporter (EU controller or processor). Such commitments might at first come across as redundant, since the certified controller/processor has already committed to the certification body to respect and conform to the certification criteria and the requirements for the granted certification. However, due to the accountability principle applicable to the EU data exporter, the overall duty of responsibility for the data transfer and especially for the existence of appropriate safeguards, lies with the data exporter. Thus, the data exporter may either rely on the fact that commitments are made to the certification body (would need to confirm nevertheless to which extent those commitments are fulfilling the requirement of Art. 46(1) and 42(2) GDPR) or require from the data recipient, apart from providing evidence about the granted certification, to also commit towards the exporter to apply the safeguards.

The provision of Art. 46(1)(f) read jointly with Art. 42(2) entails that the types of commitments are "contractual or other legally binding instruments".[439] Prior to distinguishing various options for the aforementioned commitments it is important to note that in principle each legal instrument designated to provide such commitments should as a minimum meet the following requirements:

1. The instrument should be recognised by the relevant court as being valid;
2. The instrument should provide a legal basis for relevant claims;
3. The claims should be recognised by a court or arbitral panel as being valid;

[439] Art. 42(2) GDPR.

4. The court's or arbitrator's decision can be effectively enforced in a third country.

When analysing 'the contracts and other legal instruments' as referred to in the GDPR the following instruments are discussed: (1) bilateral contracts, (2) multilateral contracts, (3) unilateral contracts/commitments and (4) treaties.

8.5.1.1. Bilateral, multilateral, and unilateral contracts/commitments: overview

Bilateral contracts are a private law instrument that is commonly use to lay down rights and obligations of parties with a view to certain 'transaction'. Contracts can cover a wide range of data protection related rights and obligations as is also demonstrated by article 28(3) GDPR setting out the topics a contract between a controller and a processor shall entail as a minimum.

Contracts in general should meet a number of criteria in order to be valid. Although the requirements may vary over jurisdictions it commonly requires: (1) offer and acceptance, (2) intention to create legal relations, and (3) competency or capacity (the authority or ability to make contracts). In common law jurisdictions generally 'consideration' (an economically measurable detriment or benefit) is a requirement for validity as well. In some cases a contract will only have binding effect on the parties when formalities are met such as being in the form of a signed, dated written document. In principle, a bilateral contract will only confer rights or impose obligations upon persons or legal entities being a party to the contract ('privity of contract').[440] It should be noted that the use of the instrument of *multilateral* contract deserves specific attention for aspects like the requirements for validity, condition for termination or suspension, liability etc. This since the multiplicity of contract parties creates a large number of mutual relationships[441] that all have to be addresses properly in the contract. In practice multilateral contracts are being used far less than (sets of) bilateral contracts.

A *unilateral contract* is conditional instrument, often taking the form of a reward or incentive. A unilateral contract can be described as contract in which only one party makes an express promise, or undertakes a performance without first securing a reciprocal agreement from the other party.

In a unilateral contract, one party makes a promise (the offer) that is only binding when certain conditions (as set out in the offer) have been met. Unilateral contracts often take the form of an incentive or reward

[440] See however the possibility to introdcuce third party beneficiary clauses Section 8.5.4

[441] For example: a four-party contract gives rise to six mutual relationships that need to be addressed adequately in the contract.

and do not seem adequate per se in the context of securing personal data processing related rights and claims.

8.5.1.2. Bilateral, multilateral, and unilateral contracts/commitments: conditions and boundaries

Above we identified four criteria that should (minimally) be met for a legal instrument to be effective as a basis for providing the commitments required by Art. 42(2) GDPR: (1) validity of the instrument, (2) scope (claim should be within the scope of the instrument), (3) validity of the claim (enforceability) and (4) effective enforcement.
The extent to which the first three criteria are being met is largely up to the contracting parties. Contract law is generally very flexible with relatively few mandatory elements, offering a solid basis for drafting valid contracts that can constitute a basis for enforceable claims. Contracts can however not set aside mandatory statutory requirements (like e.g. the elements of article 28(3) GDPR when the data importer is a data processor). Next to respecting mandatory statutory obligations, the validity and legal effect of a contract will largely depend on the level of clarity and consistency of the language used in the contract, the level of detail and legal nature of the obligations set out in the contract (best effort/result), the way violations of key performance obligations are being sanctioned (e.g. effective warranties), choice of forum and choice of applicable law. Drafting contracts that meet the three criteria set out above obviously requires adequate skills and expertise of the parties involved or their advisors.
The fourth criterion (effective enforcement in a third country) is more complicated and to a significant extent governed by mandatory rules (usually in the form treaties). Effective execution of – by way of example – a EU court's decision relating to a contract between a EU based controller and a third country-based processor, first requires local recognition of the judgment in the third country. In general, this recognition takes place based on bilateral or multilateral treaties for the recognition and enforcement of judgments.[442] The recognition is either (1) automatically, meaning that no special procedure is necessary, and the judgment can be enforced as if it were a local domestic judgment or (2) requires local court intervention. In the latter case in principle no elaborate review of the merits of the case will be required.
In case no treaty for recognition and enforcement for court's decisions is in place, arbitration could constitute an effective alternative. This

[442] Examples relating to (non-EU) third countries include the Convention on International Access to Justice 1980 and bilateral treaties between EU countries and third countries.

based on the Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention).[443]
If either way no recognition is obtained, a new procedure will have to be initiated in the third country.
Once the judgement is found to be enforceable, still a number of circumstances will influence the actual result thereof. First of all, it is obviously required that the defendant's legal entity is in existence. As the IT-sector is usually rather dynamical, this is an in our view underestimated aspect in the context of securing data processing related rights. Secondly the entity should be economically strong enough to offer adequate redress. This is obviously important when financial compensation is sought. When the entity is not willing to cooperate the claimant will have to obtain (further) courts' orders such as a warrant of execution allowing for seizure of assets, third party debt order to freezes money held in the defendant's bank account or maybe even a bankruptcy order. Contractual penalty provisions might also be instrumental in these circumstances. It should be noted that in ensuring effectiveness of data export related contracts or certification agreements, reliance on traditional insurance instruments for international trade (like export credit insurances) does not automatically provide for a solution as these instruments in principle only cover purely financial risks.
In case no financial compensation is sought, like when exerting rights to erasure, rectification of data or the right to object, the factual cooperation of the controller or processor (defendant) is necessary. The extent to which in case of defendant's refusal to comply effective legal remedies (like penalties or in some cases maybe even imprisonment) are available is a matter of local law in the relevant third country. Finally it should be noted that effective enforcement also requires adequate access to justice. Due to high costs (fees for initiating a procedure and attorney fees), complexity and duration of legal procedures this is a serious concern for especially data subjects and SMEs. Alternative dispute resolution methods might mitigate some of these concerns.[444]

When discussing the options for using contracts as a means for strengthening the effect of certification mechanisms in personal data transfers to third countries the following two contracts are key: (1) the contract between the Certification Body and the data importer (certification contract) and (2) the contract between the EU based and non-EU based controller or processor (data processing contract).

[443] Accessible at: http://www.uncitral.org/pdf/english/texts/arbitration/NY-conv/New-York-Convention-E.pdf
[444] See section 8.5.3

The *certification contract* is the basis for issuing a certification but also governs the lifecycle of the certification (renewal, withdrawal, audits). The commitments of the (to be) certified body relating to obtaining a certificate can be strengthened by inserting adequate warranties, penalties and other sanctions in the certification contract. Regarding the lifecycle of a certification, the right to withdraw or suspend a certification constitutes in principle a strong weapon for the Certification Body in ensuring compliance with the scheme requirements. The way the certification agreement is drafted will however ultimately largely determine its effectiveness (enforceability).

The *data processing contract* can strengthen the effect of the certification contract by stipulating the obligation to obtain/retain a valid certification and support this by warranties and sanctions (penalties, liabilities, termination). This implies that the certified entity has not only an obligation to comply with the scheme requirements towards the certification body but to the EU controller/processor as well. Complying with the certification requirements thereby becomes directly linked to the business of the relevant party and is substantiated with commercial interest to comply. This will in principle create a significant additional leverage for ensuring compliance with scheme requirements.

In securing effectiveness of obtaining monetary compensation (penalties, compensation for damages), an instrument like a bank guarantee could furthermore strengthen the position of the claimant.

8.5.1.3. Treaties

International law could also provide an effective basis for creation of the commitments sought after under the GDPR. This especially in the form of treaties, formal agreements between two or more states.[445] Treaties create obligations between states with for instance recognition of court decisions as their objective. Treaties can however also confer rights on individuals for instance aimed at the protection of minorities. Examples of relevant treaties in the context of data protection include the European Convention on Human Rights[446], the International Covenant on Civil and Political Rights (1966)[447] and the Convention 108 for Protection of Individuals with Regard to Automatic Processing of Personal Data (1981).[448]

[445] Other potentially relevant sources of commitments by states include could include case law, legal doctrine, custom or unilateral acts. Another example is the Universal Declaration of Human Rights that was proclaimed by the U.N. General Assembly in 1948. The Declaration is not legally binding but many principles have been incorporated in treaties, national constitutions etc.

[446] Accessible at: https://www.echr.coe.int/Documents/Convention_ENG.pdf accessed 20 September 2018

[447] Accessible at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx accessed 20 September 2018

[448] Accessible at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 accessed 20 September 2018

Treaties are tangible form of international cooperation. The importance of such cooperation is also recognized in article 50 GDPR (International cooperation for the protection of personal data) on the basis whereof the Commission and supervisory authorities shall take specific steps facilitating effective enforcement of legislation, including by means of mechanisms as notification, complaint referral, investigative assistance and information exchange. In 2017, the Commission announced it would explore the possibilities offered by Art. 50 GDPR, and more specifically the development of a framework agreement for cooperation between EU data protection authorities and the enforcement authorities in third countries.[449] International enforcement cooperation could be fostered in already existing networks or structures such as in the framework of the Convention 108,[450] the Global Privacy Enforcement Network (GPEN) [451] or the International Conference of Data Protection and Privacy Commissioners.
The importance of treaties as a basis for preventing loss of rights for EU data subjects in case of personal data transfer outside the EU is also recognized by the EDPS. Relevant areas in which the EDPS offers expertise on EU proposals include trade, law enforcement (e.g. on PNR agreements with non-EU countries) and administrative cooperation.[452]
For relevant parties, the existence of treaties facilitating recognition and enforcement of decisions of courts and supervisory bodies in principle provides a very significant advantage in terms of duration of proceedings, costs and the level of uncertainty involved. For data subjects a treaty can take away a significant part of the barriers for effectively enforcing their rights under the GDPR. Similarly, it can effectively support controllers or processor in enforcing their rights under data processing contracts aimed at achieving compliance with the GDPR. This is especially important for SMEs who are vulnerable (in terms of access to justice) when it comes down to judicial enforcement of their rights in agreements with contracting parties in third countries.

As such a treaty can also be an effective instrument assuming a dedicated framework is created, adequately taking into account the specifics of data protection related recognition and enforcement matters. This framework could be created either in the form of a dedicated treaty or amendment of existing treaties for recognition and

[449] European Commission, Communication from the Commission to the European Parliament and the Council "Exchanging and Protecting Personal Data in a Globalised World" COM (2017) 7 final, 13.
[450] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
[451] GPEN is an informal network for the collaboration of Privacy Commissioners with the aim of enforcing privacy rules worldwide. Read more: https://www.privacyenforcement.net accessed 12 March 2018.
[452] See: https://edps.europa.eu/data-protection/our-work/subjects/international-agreements_en

enforcement of judicial decisions with data protection specific aspects.

8.5.2. **Binding character and validity of commitments**

Building on the above discussion, the binding effect means that the data importer can be held liable based on its commitment and that the commitment is in principle irrevocable. The clarity, precision, detail of the commitment and scope of obligations of the parties must be clearly outlined in the contract or other binding instrument. The quality of the commitment plays a role into holding the data importer liable in terms of its commitments. It could be desirable that explicit warranties are included in the contractual agreement of the data importer with the certification body and/or the data exporter with the aim to strengthen the position of the data exporter, since when dealing with warranties, the recipient controller/processor is required to provide evidence of results, instead of efforts. In the same rationale of the data exporter's responsibility for the data transfer, the data exporter may also introduce additional contractual measures, such as a right to audit the processor in a third country (via the accredited certification body or another auditor), a right to receive information and monitoring reports from the certification body, contractual penalties or liquidated damages.

Another aspect of the binding character of the data recipient's commitments is the validity thereof. The commitments are binding, if they are not void in terms of the domestic legislation and the legal order in the country of the data recipient. Reasons for a contract being void could be the lack of capacity to contract or that the content of the contract is against public interest. In addition, a common understanding, which is also in line with the EU legislation and the GDPR, of the two parties should be reached in terms force majeure, breach of contract or withdrawal from the contract.

8.5.3. **Enforceability between contractual parties**

The element of enforceability relates to the choice of jurisdiction, applicable law and execution of judicial decisions. The location of the data importer in a third non-adequate country raises the issue of enforceability of the undertaken commitments. There are several options available for the exporter controller/processor or the certification body. Further to what discussed in the previous section,[453] we note the following options for enforceability of commitments between contractual parties.

[453] See p. 154f

Option #1: EU 'repatriation' clause

The data exporter (or the certification body, if established in the EU) and the recipient may choose to agree on EU law as governing law of the contract, that is the law that applies to the Member State where the data exporter is established. Assuming a choice for EU forum and jurisdiction, key aspects in evaluating the level enforceability of both the data processing agreements as the certification agreement extend to (1) validity and enforceability under EU law and (2) enforcement in a third country. As discussed before, the first aspect will, next to respecting mandatory statutory obligations, largely depend on the level of clarity and consistency of the language used in the contract, the level of detail and legal nature of the obligations set out in the contract (best effort/result) and the way violations of key performance obligations are being sanctioned (e.g. effective warranties). This option strengthens the enforceability of the data importer's commitments, but also the exercise of the data subject's rights. For the data importer, however such a solution is the least favourable option, as the data controller or processor established in the third country would agree to submit itself to the competence of unfamiliar courts and legislation. In addition, litigation costs would be considerably higher than the other options.

Option #2: Alternative Dispute Resolution Mechanisms (ADR)

Clauses allowing arbitration or mediation for parties to resolve differences stemming from the undertaken commitments are usually beneficial in contractual commitments involving parties in different jurisdictions. Dispute resolution, for example, by means of arbitration, is relevant in the case of international organisations as well. It should be noted that the scope (e.g. relating to commercial or civil law relationships)[454] of such instruments, the authority of the independent party[455] and varying binding effects might be limiting their applicability to all cases of data transfers on the basis of approved certifications.[456]

In specific, there are several ADR instruments that may be used as a measure for parties to solve disputes that may arise in the conclusion and execution of the certification agreement or the data processing agreement.

The authors would like to thank Hosna Sheikhattar for her research assistance on the alternative dispute resolution mechanisms (TILT).

[454] However, the CJEU in the Schrems case ruled that "Effective legal protection should be established against interferences with fundamental rights originating not only from commercial relationships, but also from the State. Case C 362/14 para 88 ff.

[455] For example in some jurisductions an arbitrator may not be allowed to create, modify, or terminate a legal relationship but his/her powers are limited to declaratory judgements and orders to pay. Rubino-Sammartano, Mauro. International arbitration law and practice. Juris Publishing, Inc., 2014. p. 185, p.189f

[456] Read for example the model contract for arbitration with alternative options for clauses: Patocchi, Paolo Michele. "UNCITRAL Model Law on International Commercial Arbitration 1985 with amendments as adopted in 2006." United Nations Publication, 2016, http://www.uncitral.org/pdf/english/texts/arbitration/ml-arb/07-86998_Ebook.pdf [accessed 7th May 2018]

- **Arbitration**
  Arbitration is generally initiated through an arbitration clause included in a contract. Pursuant to this clause, an arbitral tribunal will be constituted, which will contain one or more appointed or selected arbitrators. [457] The award in international arbitration is binding in the place of arbitration, and may be recognised as such by court order. In some jurisdictions, state courts have the authority to order interlocutory injuctions and conservatory measures during arbitral proceedings.

- **Mediation**
  Mediation is a voluntary process under which a mediator, who is a neutral third party attempting to resolve a dispute between parties, in an amicable way. The mediator assists the parties in reaching a settlement agreement on their own, without ever imposing a decision on them.[458] Thus one cannot strictly speak of enforceability of commitments since mediation is a voluntary process, unless there is a settlement. The mediation settlement may be enforceable either by means of a court order or by recording the settlement agreement as an arbitral award. [459] Mediation may have added value in the context of data transfers, as a first effort towards solving a dispute before initiating costly cross-border litigation.

- **Other mechanisms**
  Increasingly, in the fields such as electronic commerce and consumer protection, online dispute resolution is introduced.[460] Other mechanisms include Ombudsmen, initiated by trade organisations. In the Netherlands for example, the Foundation for Consumer Complaints Board handles a number of cases between companies members of the trade associations and attempts non-binding settlements of disputes.[461]

All ADR measures, are best suited for business to business relationships, while additional measures should be foreseen for the exercise of data subjects' rights, as discussed in the following section.[462]

[457] Gaultier, Thomas. "Cross-Border Mediation: A New Solution for International Commercial Settlement?" INT'L L. PRACTICUM 26 (2013): 38-42.
[458] Gaultier (2013)
[459] ibid
[460] OECD in its guidelines on consumer protection in electronic commerce recommends the establishment of alternative dispute resolution mechanisms with the employment of information communication technologies. OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (1999) p.18
[461] https://www.degeschillencommissie.nl/over-ons/ accessed 15 October 2018.
[462] See Section 8.5.4.

Option #3: Enforceability guarantees provided in national legislation of the third country

Alternatively, the parties may decide to agree on another governing law, for instance of the country where the data importer is established. In that case, the data exporter or the certification body needs to make sure that the commitments and safeguards as included in the granted certification are valid and enforceable in the selected non-EU jurisdiction. This option, although it lacks the guarantees of the EU law has an advantage in terms of the execution of judgements, since the third country will likely be the country where the assets of the data importer are located. In addition, the law of the third country would have to recognise third party beneficiary rights.

8.5.4. **Enforceability of data subjects' rights**

In terms of data transfers to data recipients in a third country or international organisation, given the limitations of EU DPA competences, [463] the data subject rights are only indirectly protected via the safeguards introduced in the granted certification and any undertakings of the data recipient to facilitate the exercise of such rights.

Since Art. 42(2) and 46(2)(f) GDPR both require particular attention to the data subject rights, the legally binding and enforceable commitment needs to introduce relevant clauses for data subjects. A data subject not being party to a data processing contract between a controller and third country processor or a certification contract between a certification body and the certified data importer, cannot exert any rights under the contract (nor be bound by it). Designation of the data subject in said contract as a 'third party beneficiary' will however confer certain rights (as set out in the contract) on the data subject and constitute binding

[463] The issue of oversight of the DPAs in the case of bilateral agreements between private parties in non-EU countries and the limits of the powers of the EU DPAs has been raised by several prominent scholars (See Kuner 2017), but also stressed by the Court of Justice, in two instances. In the Weltimmo case, the Court ruled that the supervisory authorities are able to exercise their effective powers of intervention, based on complaints submitted to them, only within the territory of its own Member States. The Court continued that the DPAs cannot impose penalties on the controller who is not established in their territory, but should request the competent authority of the Member State whose law is applicable to take action (but also stressed by the Court of Justice, in two instances. In the Weltimmo case, the Court ruled that the supervisory authorities are able to exercise their effective powers of intervention, based on complaints submitted to them, only within the territory of its own Member States. The Court continued that the DPAs cannot impose penalties on the controller who is not established in their territory, but should request the competent authority of the Member State whose law is applicable to take action. In the Schrems case the Court, in interpreting the Directive, also found that: *"It is, admittedly, apparent from Article 28(1) and (6) of Directive 95/46 that the powers of the national supervisory authorities concern processing of personal data carried out on the territory of their own Member State, so that they do not have powers on the basis of Article 28 in respect of processing of such data carried out in a third country."* Case C-362/14, ECLI:EU:C:2015:650. The Court however acknowledged the powers of the DPAs with regard to the transfer as such, which is a processing operation by itself. Para 54 provided: "Neither Article 8(3) of the Charter nor Article 28 of Directive 95/46 excludes from the national supervisory authorities' sphere of competence the oversight of transfers of personal data to third countries which have been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46."

commitments. A third party beneficiary is in principle not a party. Insertion of third party beneficiary clauses in the contract could in some jurisdictions however result in the third party's accession to the contract.
When using *multilateral contracts*, a data subject or for instance a sub-processor could be designated as (primary) contracting parties and hence execute their rights under the contract on the basis thereof directly.
Clauses introducing rights for data subjects as non-parties to the contractual commitments should include both:

- substantial rights against controllers in the third country or international organisation such as the right to information, access, rectification, restriction, erasure and objection.
- procedural rights and remedies such as the possibility to lodge a complaint before the competent DPA and the courts.[464] Particular attention should be given to the introduction of the rights to an effective judicial remedy against a controller or processor, the representation of data subjects and the right to compensation and liability.

Additional clauses to facilitate the exercise of the rights of the data subjects such as the reversion of burden of proof (not on the data subject to prove the violation or harm) should also be considered.

Although, certification of Art. 42(2) is a data transfer tool for cases there is no adequacy decision for a third country, it is possible that national legislation in the third country provides some instruments for the enforcement of data subject rights. The WP29 opinions exploring different redress mechanisms in third countries in the context of Adequacy decisions offer useful lessons on how national legislation on data protection, civil and liability law, criminal and criminal procedural law may support enforcement of data subject rights and redress mechanisms.[465] It should be noted that since a thorough review of the legal system of a third country has not been conducted, reliance on instruments of national legislation of the third country where the data importer is established, could only be complementary to other measures and commitments, such as in the framework of the

[464] Article 29 Data Protection Working Party "Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules".
[465] The different types of redress mechanisms are discussed here by means of example. The WP29 opinions were issued, as mentioned, in the context of Adequacy Decisions, which is a different legal basis for data transfers.

certification agreement and third party beneficiary rights, as discussed.[466]

[466] Article 29 Data Protection Working Party, 'Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay' WP177, adopted on 12 October 2010, 20., Article 29 Data Protection Working Party, 'Opinion 4/2002 on the level of protection of personal data in Argentina' WP63, adopted on 3 October 2002, 16., Article 29 Data Protection Working Party, 'Opinion 7/2009 on the level of protection of personal data in the Principality of Andorra' WP166, adopted on 1 December 2009, 13, Article 29 Data Protection Working Party, 'Opinion 8/2007 on individuals with regard to the processing of personal data in Jersey', 11, Article 29 Data Protection Working Party, 'Opinion 6/2009 on the level of protection of personal data in Israel'' WP165, adopted on 1 December 2009, 17.

8.6. Example of cross-border transfers mechanism: APEC CBPR

8.6.1. The APEC Privacy Framework: overview

The Asia-Pacific Economic Cooperation (APEC) is an economic intergovernmental forum established in 1989 that currently gathers 21 participating countries around the Pacific Rim[467]. In 2004, APEC Ministers endorsed the *APEC Privacy Framework* for encouraging "the development of appropriate information privacy protections and ensuring the free flow of information in the Asia Pacific region."[468] The APEC Privacy Framework has defined nine privacy principles based on these included in the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal first published in 1980 and updated in 2013[469]. Part III[470] of the APEC Privacy framework defines the following principles:

1. **Preventing Harm**: The controllers must prevent misuse of personal data.
2. **Notice**: The collection of personal data must be documented and data subjects informed of the collection and its purpose(s)
3. **Collection Limitation**: The collection must be limited to the data relevant to the purpose.
4. **Use**: The data must be collected with the consent of the data subjects and used in relation to the purpose
5. **Choice**: The data subjects have the right to exercise choice in the data collection and use
6. **Integrity**: The data must be complete, accurate and kept up to date
7. **Security/Safeguards**: Data must be protected against risks of loss and unauthorized access. Security measures must be adapted to the data sensitivity
8. **Access and Correction**: The data subjects have the right to access their own data and request the data is corrected

[467] See Member Economies on the APEC website https://www.apec.org/about-us/about-apec/member-economies.aspx (accessed 10 November 2018)
[468] Preamble Recital 4 of the APEC privacy Framework http://publications.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf (accessed 10 November 2018)
[469] Preamble Recital 5 of the APEC privacy Framework http://publications.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf (accessed 10 November 2018)
[470] See Part III of the APEC Privacy framework 2015 updated version. https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)(accessed 10 November 2018)

9. **Accountability**: The controller must ensure the compliance of processors it works with. It must be able to demonstrate its compliance with the privacy framework.

8.6.2. **APEC CBPR**

The APEC Cross Border Privacy Rules (CBPR) system[471] is a mechanism that facilitates transfers of data among the participant organisations, while respecting the Privacy principles of the APEC Privacy Framework.[472] To participate in the system organisations need to implement legally enforceable privacy policies and practices, which are in line with the CBPR Program requirements for all the personal information collected or received, which is subject to cross border transfer to other participating economies. The policies and practices of the organisations are evaluated and monitored by public or private sector 'accountability agents', who also certify the compliance of the participant organisations.[473]

Accountability Agents

The Accountability agents are responsible for the monitoring and certification with relation to the APEC Privacy Framework and not domestic regulations and any legal obligations that could stem thereof. Once accredited, the Accountability Agent is entitled to assess and attest the conformity of candidate organisation with dedicated requirements, the CBPR Program Requirements, derived from the APEC privacy framework. The APEC CBPR system has defined a process in five steps[474] for accrediting the AA. The program has also drafted a set of dedicated criteria[475] assessing that the candidate body is:

- Free of conflicts of interest,
- Has defined internal safeguards and a disclosure policy in order to prevent potential conflicts of interest,
- Possesses a structured conformity assessment process,
- A monitoring and re-certification process,
- A complaint and dispute resolution process,
- A sanction policy to apply to certified bodies in case of persisting non-compliance

[471] See Annex 3 (separate document).
[472] The APEC Privacy Principles are: Preventing Harm, Notice, Collection Limitation, Uses of Personal Information, Choice, Integrity of Personal Information, Security Safeguards, Access & Correction and Accountability.
[473] To date only two Accountability Agents exist: TrustArc Inc. for the United States and JIPDEC for Japan.
[474] See the process for becoming an APEC CBPR system Accountability Agent on the CBPR's website. http://www.cbprs.org/Agents/NewAgentProcess.aspx (accessed 10 November 2018)
[475] See accreditation requirements for becoming an APEC CBPR system Accountability Agent http://www.cbprs.org/Agents/CBPRsRequirements.aspx (accessed 10 November 2018)

The Joint Oversight Panel, following the accreditation process it manages, issues a non-binding recommendation to the APEC country from where the Accountability Agent originates. The country keeps the final decision to accredit or not the Accountability Agent. The accreditation is then granted for one year and must be renewed according to the same process by the Joint Oversight Panel.

Applicability, certification criteria and assessment

APEC CBPR sets a minimum standard for privacy protection requirements. In case of conflict between the domestic law and the APEC CBPR system, APEC economies should adapt their national laws and regulations to be in line with the requirements of the APEC CBPR program, in order to be able to participate. The APEC CBPR System only applies to data controllers established in APEC participating countries[476] insofar as the scope of the APEC Privacy Framework to which the CBPR refers is limited to data controllers. In 2015, a dedicated framework, following the same process, the *Privacy Recognition for Processors*[477] (PRP), has been endorsed to help processors to demonstrate their compliance with privacy principles derived from the Privacy Framework.

The assessment procedure, as provided by the Accountability Agent for the US, TrustArc, encompasses the following stages:

- Initial assessment of applicant's compliance with the Privacy Certification requirements of TrustArc, which reflect the APEC Privacy Framework requirements. The initial assessment is performed through a document review and technical assessment. The applicant is provided with a self-assessment questionnaire, which is reviewed by the Accountability Agent, together with any associated documentation, such as:[478]
    - Applicable privacy statements and/or hyperlinks
    - Information security policy.
    - Policy for secure disposal of personal information.
    - Risk assessments reports.

[476] The USA, Mexico, Japan, Canada, Singapore and the Republic of Korea.
[477] A presentation of the Privacy Recognition for Processors (PRP) is available on the CBPR's board website https://cbprs.blob.core.windows.net/files/PRP%20-%20Purpose%20and%20Background.pdf

[478] APEC cross-border privacy rules system, policies, rules and guidelines: https://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx; (accessed 10 November 2018)Accountability Agent APEC Recognition Application ANNEX C, https://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-AccountabilityAgentApplication.ashx (accessed 10 November 2018)

- Statement of the applicant confirming compliance with the requirements of the legislation that governs the collection of personal information, and that it is collecting information by fair means, without deception.
- Written policies and documented procedures to ensure that all collected personal information is in accordance with the purposes for which it was collected.
- Description of how individuals provide consent for third party disclosure (online point of selection, via email, profile page, telephone, other).
- Description of mechanism for correcting inaccurate, incomplete, and out-dated personal information.
- Complaint handling procedures.
- Internal guidelines, contracts, compliance with codes of conducts, or other to ensure compliance with APEC Information Privacy Principles.
- Self-assessments to conform compliance to internal guidelines, contracts, codes of conduct and others.
- The certification is issued for one year at the end of which the organisation must attest "to the continuing adherence to the CBPR program requirements".
- The Accountability Agent is required to review possible changes occurred in the certified situation during the validity period and perform comprehensive reassessments on a regular basis. [479]

- The Accountability Agent, in this case TrustArc, then provides a comprehensive report to the applicant, by outlining the findings regarding compliance and proposing necessary changes to the applicant in order to comply with the APEC principles.
- The applicant controller makes the requested changes and TrustArc verifies that the changes have been properly implemented
- Following a successful compliance assessment, the Accountability Agent awards the certificate to the applicant.

8.6.3. **Cross-border Privacy Enforcement Arrangement and Joint Oversight Panel**

The implementation and enforcement of commitments that have been undertaken is one of the building blocks of the data transfer

[479] Section 8 of Accountability Agent Recognition Criteria.

mechanisms of Art. 46 GDPR. The APEC CBPR, working to ensure the enforcement of its privacy framework, in cross-border information flows, has established the APC Cross-Border Privacy Enforcement Arrangement ("CPEA").[480] CPEA creates a framework for cooperation in the enforcement of the Privacy legislation of the APEC economies. The administration is handled by the US Federal Trade Commission.

The CPEA sets out the fundaments for the enforcement of commitments of controllers undertaken in the APEC CBPR framework, which will also correspond to legal obligations of the national law of the APEC country to which the controller is subject.[481]

The obligations and commitments that go beyond what is legally required from a controller in term of the domestic law of an APEC country, are treated as commitments undertaken between private parties, namely the certified controller and the Accountability Agent.

The Joint Oversight Panel (JOP) carries out the administration of the CBPR system. The JOP also handles the Accountability Agents' applications and evaluates whether an organisation should be recognised as Accountability Agency. Although the JOP does not in itself decide whether to recognise an Accountability Agent or to revoke its recognition, the JOP issues recommendations that have an advisory but more or less informally binding nature for the APEC economies.[482] The concept of an oversight panel which monitors the activity of the certifiers may be loosely linked to accreditation of certification bodies, even though there are substantial differences in the two systems.

8.6.4. **Key take-away features**

Due to the different normative basis of the CBRP and the GDPR certification, the CBPR program is not of interest with regard to the transfers as such, but it presents an interesting case in terms of the guarantees and safeguards in a country other than the one of the data exporter.

- **Certification of the importers**

APEC CBPR certification is certification of the importer/recipient of the personal information, not the exporter organisation, as the Art. 42(2) certification.[483].

- Certification criteria

[480] https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx (accessed 10 November 2018)
[481] For the data processors, APEC has adopted the APEC Privacy Recognition for Processors System. See https://www.apec.org/~/media/Files/Groups/ECSG/2015/APEC%20PRP%20Rules%20and%20Guidelines.pdf (accessed 12 March 2018)
[482] Economies voluntarily participate in the APEC system.
[483] This element resembles to Art. 42(2) GDPR.

The CBPR system suggests an interesting approach in the drafting of certification criteria that slightly differs from the drafting commonly used in certification standards.

The CBPR criteria offers a guided approach where the preliminary Intake Questionnaire completed with the CBPR Program Requirements precisely detail the results expected for each criterion. [484]

This approach has two benefits. First, it contributes to prevent the potential inconsistencies in criteria interpretation. Second, by making these detailed criteria available for free, it helps organisations prepare for the certification and structure their processing in line with the certification criteria.

Question	Assessment Criteria
1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.	If **YES,** the Accountability Agent must verify that the Applicant's privacy practices and policy (or other privacy statement) include the following characteristics: • Available on the Applicant's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified). • Is in accordance with the principles of the APEC Privacy Framework; • Is easy to find and accessible. • Applies to all personal information; whether collected online or offline. • States an effective date of Privacy Statement publication. Where Applicant answers **NO to question 1**, and does not identify an applicable qualification subject to the Qualifications to Notice set out **below**, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.

Figure 8-2: Example of criterion from the CBPR Program Requirement.

- **Short validity period of granted certification**

The CBPR system grants a one-year validity period for certification. This feature promotes a close monitoring of accountability agents and certified organisations. It contributes to the reliability of the CBPR system by preventing the risk of complacency in the certification process.

- **Cross-border-monitoring**

[484] See Figure 8-2.

The roles of the Joint Oversight Panel and the Cross-border Privacy Enforcement Arrangement give an example of how to set up oversight and control mechanisms in certifications for cross-border transfers.[485]

8.7. Components of certification mechanisms for transfers

Building on the analysis in this Chapter on the purpose, elements, criteria, enforceability of the data protection certification mechanisms for data transfers, the analysis of previous Chapters (Chapters 3, 4, and 6), and the analysis of other mechanisms of Art. 46 GDPR, we identified a number of key components for the data protection certification mechanisms of Art. 42(2) GDPR. The components reflect different issues that should be addressed in a certification mechanism in order to assure that the data importer provides appropriate safeguards to receive personal data from the EU controller/processor. The structure is based on the ISO/IEC 17067 standard.[486]

Component		Explanation
Scope of the certification		The scope of the certification provides the aim and specific object of certification (which type of processing operations are covered)
Information & Supporting documentation		The information about the organisation and its activity (full name, establishment, mapping of data processing activities, etc.) that the applicant needs to provide to the certification body. This section also lists all the supporting documentation necessary to provide evidence of the applicant for conformity to the criteria and other elements of the certification mechanism.
Certification criteria[487]	**Data protection principles**	Policies, processes, and organisational and technical measures, to implement, respect and apply data protection principles of Art. 5 GDPR.
	Ground for processing	Specification of ground of processing and justification.
	Data Protection by	Policies, processes, and organisational and technical measures, to implement, respect

[485] The Article 29 Data Protection Working Party has identified several common blocks between the APEC CBPR and the Binding Corporate Rules, but also a number of topics that are not or not commonly addressed between the two instruments for data transfers. Article 29 Data Protection Working Party "Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents" WP212, adopted on 27 February 2014.
[486] ISO/IEC 17067 standard
[487] Based on Art. 47(2)(d) on the content of Binding Corporate Rules, which is one of the other grounds of Art. 46 GDPR for transfers on the basis of appropriate safeguards.

	Design and by Default	and apply data protection by design and by default.
	Data Security	Technical and organisational measures to handle access to data prevent loss, alteration, manipulation, of personal data, data breach reporting protocol for communication with the data exporter and the data subject, if necessary.
	Processing of special categories of data	If applicable, specification of ground for processing and technical and organisational measures.
	Substantive data subject rights (Art. 12-22 GDPR)	Policies, processes, and organisational and technical measures, to facilitate the exercise of the rights to information, access, rectification, restriction of processing, erasure, portability, object and not to be subject to automated decision-making.
Evaluation methodology against the certification criteria		The mechanism should provide a detailed description of the methodology to be used by auditors.[488]
Methods and procedures to ensure integrity and consistency of the process		The mechanism needs to set out methods and procedures to ensure that the results of the certification process are consistent and have not been compromised. For example it needs to describe mechanisms to identify integrity issues of the employees of the certification body.
Use of certification seal and/or mark		This section describes the permitted use of the certification seals and/or mark once the certification is granted to the data importer.
Resources		The estimated resources necessary to carry out an evaluation of the applicant for certification.
Non-conformities with criteria (major, minor) and corrective actions		The mechanism should explain what is considered to be major and minor non-conformity (for example that non-conformities with data protection principles criteria are major, while missing documentation for one of the security measures is minor, and maybe corrected within a given period of time).
Surveillance procedure and cooperation with the		The certification mechanism should describe how the certification body will ensure that the conditions of granting the

[488] See Chapter 4 p. 74f on Conformity assessment.

certification body	certification continue to be met.
Complaint handling mechanisms & appeals	The applicant should have the right to complain against the certification procedure and appeal.
Reporting mechanisms	The mechanism should describe how the applicant reports changes in its processing, or status, or other that affect certification.
Content of contract between the certification body and the certified entity	The mechanism needs also to provide the content of the contract between the certification body and the certified entity. The contract should at least include: ▪ Governing law (EU MS law or of the third country) ▪ Commitment of the data importer to respect the certification criteria. ▪ Grounds for revocation or withdrawal of the certification. ▪ Obligation to disclose conflicting national laws that prevent the certification criteria from being respected or complied with. ▪ Description of how the data importer undertakes to respect and facilitate data subjects' rights (both substantive and procedural) and how the commitments are made binding and may be enforced against the data importer by the certification body, or third party beneficiaries, such as the data exporter and data subjects. ▪ Description of available remedies in case of damages from breach of the certification or the contractual agreement. ▪ Conflict resolution mechanisms.

Table 8-1: Components of certification mechanisms for data transfers

9. Positioning of data transfer certification in view of generic certification

The GDPR specifically requires that the needs of SMEs need to be considered regarding the data protection certification mechanisms.[489] Beyond SMEs, the analysis of existing certifications revealed that a certification process may be both lengthy and costly for any company.[490] Besides, it is true that not all certified controllers or processors may wish to transfer data to third countries or if they do, the recipient country might already be covered by an Adequacy Decision. In such cases, data protection certification mechanisms that are designed to include requirements and criteria for data transfers might impose an undue burden on such controllers or processors or might even render certification unappealing for them.

Considering such issues, this Chapter is devoted to the question of whether certifications in light of Art. 46(2)(f) GDPR should be part of every data protection certification mechanism or a stand-alone mechanism, independently of a certification regarding compliance with the GDPR.

9.1. Models of certification for data transfers

In the previous Chapter, it was explained that certification as a data transfer mechanism is addressed to the controller or processor in the third country or the international organisation. Adherence of the data importer to such a data protection certification mechanism, with the procedures of Art. 42 and 43 GDPR, are a means for the exporter controller or processor to be assured of the appropriate safeguards and be therefore allowed to transfer personal data to the certified importer controller or processor.

In practical terms, the components identified in the previous Chapter may be provided in different models that can be identified for the purpose of data transfers. The certification scheme owners, when developing the data protection certification mechanisms, should consider the available options and whether it is meaningful to combine the certification for the purpose of demonstrating compliance with the GDPR with the certification for data transfers in one mechanism or a stand-alone certification mechanism for data transfers is a better option. We identify the following models:

[489] Art.42(1) GDPR.
[490] See also Rodrigues Rowena et al., 'Inventory and analysis of privacy certification schemes Final Report Study Deliverable 1.4' EU Seals project (2013), 44 and 144. Available: <http://www.vub.ac.be/LSTS/pub/Dehert/481.pdf> accessed 15 February 2018.

Model A is the stand-alone data transfer certification. The data protection certification mechanism of Model A entails that the scope of the certification mechanism is to provide safeguards for the transfer of personal data to a third country or international organisation.[491]

Model B can be described as following a modular, flexible approach: this certification includes the elements of the generic certification, and an additional module (and set of approved criteria specific to the purpose of data transfers), which is applied only when the applicant controller or processor is established in a third country or organisation and intends to receive data. The rationale of a modular certification is that a scheme owner does not need to establish different certifications for the purpose of demonstrating compliance (Art. 42(1) GDPR) and for the purpose of data transfers (Art. 42(2) GDPR).

Model C is the generic data protection certification, which makes no differentiation in its scope for processing activities related to transfers.[492] The appropriate safeguards for data transfers are embedded in the approved criteria. As explained in Chapter 4, certifications based on Art. 42 GDPR may be either all-encompassing (otherwise 'comprehensive'), namely covering the whole spectrum of the GDPR principles, rights and obligations or focus on a particular issue, such as data protection by design ("single-issue certifications"). Single-issue certifications are by definition not fit for purpose, since they address the GDPR provisions partially.

Model	Description	
A	Stand-alone data transfers certification	
B	Modular generic certification	
C	Generic certification	C1: Comprehensive certification
		C2: Single-issue certification

Table 9-1 Optional models for certification of data transfers

9.2. Assessment of certification models for data transfers

The research team assessed the strengths and weaknesses of the models against a set of key criteria. The criteria, while not being exhaustive, aim at capturing the main issues that might arise in each of the three models, in relation to data transfers, namely to maintain or to risk lowering the level of protection (Criterion 1: "safeguards"), to

[491] The development of such certification mechanisms, seals, or marks is provided in Art. 42(2) GDPR.
[492] Generic in this context means non-specific to data transfers.

facilitate or cause undue burden to the authorities and the certification bodies (Criterion 2: "organisational aspects"), increase or reduce the market incentives for data protection certification mechanisms (Criterion 3: "costs & fit for purpose") and to offer clarity or confuse the data subjects (Criterion 4: "transparency").

	Criteria	Strength	Weakness	Concerned entity
1	Safeguards as reflected in approved criteria	Maintain high level of protection	Lower protection	*Data subject & DPA*
2	Organisational aspects	Facilitate	Undue burden	*DPA & Certification body*
3	Costs & fit for purpose	Increase market incentives	Decrease market incentives	*Applicant controller or processor*
4	Transparency	Clarity on offer	Confusion on offer	*Data subject*

Table 9-2 Matrix of assessment criteria of data transfers certification models

9.2.1. **Model A: Stand-alone certification for data transfers**

A stand-alone certification for data transfers would be fit for purpose and able to ensure appropriate safeguards. Since the stand-alone data transfers certification will have to be designed with the sole purpose to facilitate data transfers, several elements would have to be different than with the regular national data protection certification mechanisms or the European Data Protection Seal. First, as with the assessment for the Adequacy Decisions, the formulation of the requirements and criteria would not have to be identical on a one-to-one scale compared to the GDPR provisions, but will aim at fulfilling the essence of each provision. In addition, GDPR topics relevant only for the EU, such as for instance the derogations of Article 89 GDPR on processing for archiving purposes, scientific, historical research or scientific purpose would not be part of the data transfers certification mechanism. Other topics that have a strong EU law element in the GDPR, would be maintained but neutralised in a way that would be relevant to other jurisdictions. An example is the derogation of Art. 22(2)(b) in automated decision-making, in which the data subject does not have the right not to be subject to such a decision, when mandated by European Union or Member State law. Obviously, the certification body and its auditors would need to ask the applicant controller or processor for information

about the national law (or international norms, in the case of International Organisations) to which they are subject, and afterwards assess whether the spirit of the national law reflects the meaning of the Art. 22(2)(b) derogation. Such a process is not an easy task for auditors and assessors. It demands specific guidance on how to apply and assess the certification criteria and a very good understanding of EU law and EU data protection law.[493] In terms of the transparency of the certification towards the data subject, the stand-alone certification would fulfil this criterion, provided that all the necessary conditions of the ISO/IEC 17065 standard are met. A data protection certification mechanism that is destined to allow cross-border flows would be advertised and communicated as such (transparency). The main weakness of the stand-alone Model would be identified from an organisational perspective, as the existence of stand-alone certifications for transfers – along with any other generic or single-issue certifications that might be developed and approved- add an operational burden to the work of DPAS, and NABs.

Model A	Criteria	Strength	Weakness
1	Safeguards	✓	-
2	Organisational aspects	-	✓
3	Costs & fit for purpose	✓	-
4	Transparency	✓	-

Table 9-3 Scoring of Model A in terms of transfers assessment

9.2.2. **Model B: Modular certification**

This model adopts a more flexible approach. Data transfers as a sub-set of the criteria of the certification scheme are developed in the framework of a generic (all-encompassing) data protection certification mechanism, and consequently approved by the competent authority. The modular element relates to the application of the criteria. Once the applicant is a controller or processor in a third country or IO, then the sub-set of criteria would be part of the audit and transfers would be included in the scope of certification. If the applicant is already subject to the GDPR and aims to use certification to demonstrate compliance,

[493] Some certification scheme owners or/and Conformity Assessment Bodies, but also the European Accreditation forum provide such documents, sometimes called "certification manuals" or guidance. See for instance:
<https://cris.vub.be/files/25487413/CRISP_D6.2_Final_certification_manual.pdf> accessed 12 March 2018.

then the scope of certification would be limited to the generic certification, without the data transfers module. In practical terms, modular certification is a model that primarily saves effort and organisational costs for certification scheme owners and certification bodies. Some of the modules are common. independently of the intended purpose of certification (Art. 42(1) or Art. 42(2(2)). This means that its auditors are already trained to conduct their evaluation on those common modules, such as for example the facilitation of the exercise of the right to rectification of inaccurate data.

In terms of safeguards and level of protection, such a certification model as with Model A, is likely to ensure that all the appropriate safeguards specific to risks that might arise from data transfers to a non-EU country are in place. From an organisational point of view, DPAs and certification bodies have an extra burden only when transfers are in the scope of certification. This seems to be the optimal solution among the available models in terms of organisational burden. Next, the flexibility of this model makes the costs and fit for purpose criteria its strong elements. The main weakness of the modular approach is its potential miscommunication or creation of confusion to the data subject as to when the transfers module is part of the scope of the granted certification. Data protection marks have a significant role to play here in indicating the difference in scope, but given the plethora of certification marks in the market, the expectations on achieving full clarity and transparency should be low. For the data subjects or others actively seeking for information on an issued certification of such kind, the registry kept by the EDPB, may offer such the necessary information on the scope of the certification.

Model B	Criteria	Strength	Weakness
1	Safeguards	✓	-
2	Organisational aspects	✓	-
3	Costs & fit for purpose	✓	-
4	Transparency	-	✓

Table 9-4 Scoring of Model B in terms of transfers assessment

9.2.3. **Model C: Generic certification**

The generic certification model, in this context, is the one that does not differentiate in scope for transfers to third countries or within the Union. The Model C1 assessed in the section is an all-encompassing data

protection certification mechanism, destined to assess a processing activity against approved criteria on the full spectrum of the GDPR provisions. Such certification mechanism is based on Art. 24 and 28 GDPR, and its scope is not limited to one issue, but aims to demonstrate compliance with the legal obligations of the applicant controller or processor. This certification mechanism would follow the model of EuroPrise, which was analysed earlier in the report[494] or the ePrivacy Seal.[495]

Since the certification mechanisms under this Model are all-encompassing (or else: comprehensive), criteria and requirements that address data transfers safeguards, are by default embedded in the criteria and requirements of the certification scheme.[496] This element creates the potential for a high level of protection offered by the certifications of this Model, in terms of data transfers, as well as clarity and transparency as to what is covered by its scope. This certification mechanism would require that the (applicant) data importer would have to conform to certification criteria, as if it would be subject to the GDPR. Even though the legal standard for data transfers is not as high as full compliance with the GDPR, the applicant would need to demonstrate compliance of its processing with the stringent criteria of a data protection certification mechanism of Art. 42(1) GDPR.[497]

The very same element of all-encompassing GDPR legal obligations may however increase the costs and bring an administrative burden to the certifying entity, especially when the applicant should go through stringent requirements as if the applicant would be subject to the GDPR. When the applicant is a controller or processor in a third country, or the recipient of the personal data in an onward transfer, then the stringent transfers-related safeguards should be embedded in the approved criteria of the certification.

Model C1	Criteria	Strength	Weakness
1	Safeguards	✓	-
2	Organisational aspects	-	✓

[494] See Annex 3 (separate document).
[495] See https://www.eprivacy.eu/en/privacy-seals/eprivacyseal/. See also ENISA (2017) 'Recommendations on European data protection certification'.
[496] This statement refers to the substantive/normative criteria, not to the legally binding and enforceable commitments, which are additional requirement to the adherence to approved certifications per Art. 46 GDPR.
[497] Art. 44 GDPR requires that "All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined"

3	Costs & fit for purpose	-	✓
4	Transparency	✓	-

Table 9-5 Scoring of Model C1 in terms of transfers assessment

The last Model examined for data transfers is the single-issue certification. As discussed earlier in the report,[498] single-issue certification focuses on a particular issue such as data-security. In terms of safeguards for data transfers, certifications in this Model are in principle not providing the appropriate safeguards required by Art. 46 GDPR. One cannot think of a certification demonstrating how secure a processing operation is for qualifying for the transfer of data to a third country, for the simple reason that the data security of the processing is only one of safeguards which the recipient controller or processor needs to demonstrate. In addition, this impacts the criterion fit for purpose and costs. An applicant controller or processor would need to go through multiple single-issue certifications to ensure that he or she provides appropriate safeguards. Lastly, single-issue certifications have a limited scope. The seal and mark of such certification needs in general to be advertised and communicated as covering the specific issue, instead of giving the impression of an all-encompassing certification. Adding data transfers in the scope of such certifications would only encumber the already blurred lines of what the seals offer.

Model C2	Criteria	Strength	Weakness
1	Safeguards	-	✓
2	Organisational aspects	✓	-
3	Costs & fit for purpose	-	✓
4	Transparency	-	✓

Table 9-6 Scoring of Model C2 in terms of transfers assessment

9.2.4. **Overall assessment and discussion**

This section assessed 3 Models of data transfers certifications against a set of key issues. The assessment revealed the different strengths and weaknesses. The aim was not to identify the strongest or weakest

[498] See Chapter 3 analysis of identified certification models p. 29f

Model, but to discuss the different implications of adopting or promoting the one Model over the other. From a quantitative perspective, the stand-alone certification and modular certification appear to have more strengths than weaknesses. From a qualitative perspective, one cannot say which model is better than the other, since such a decision would depend on which criterion is of higher importance, or priority, for the scheme owner and developer, and of course the DPA (or the EDPB) that approves the certification criteria. The table below presents an overview of the strengths and weaknesses of the different Models.

	Safeguards	Organisational aspects	Costs & fit for purpose	Transparency
Model A	+	-	+	+
Model B	+	+	+	-
Model C1	+	-	-	+
Model C2	-	+	-	-

Table 9-7 Overview of strengths and weaknesses of Models of certification for data transfers

10. Key Findings

This Chapter aims at presenting the main conclusions and findings of the study as discussed in the previous chapters. The main target audience is the European Commission, even though the information provided in the study and this Chapter in particular can be of benefit also to other stakeholders involved in the GDPR certification mechanisms.

The findings of the study present an overview of the main issues identified and discussed. These key issues are then grouped in four themes that are complementary to each other. Those themes were also apparent in the feedback sessions during the various workshops and meetings where the study was presented.[499]

Overall, although the GDPR entrusts the Commission with certain empowerments under Article 43(8) and 43(9), it still needs to be evaluated whether in a given situation adopting a delegated or an implementing act is the optimal instrument for achieving this goal. Other types of actions that could be taken by the Commission under article 42(1) and/or by other actors (for instance DPA's or the EDPB) - either independently or combined with legislative steps – might in some cases be preferred. For instance, because these are more efficient, quicker to implement or provide an advantage otherwise (policy-wise, political, procedural, in terms of costs ...)." In particular, when it comes to Art. 43 (9) and technical standards, given the considerations as to the GDPR related adequacy of the current body of available standards we do currently not recommend taking implementing acts under article 43(9) to support implementation of these standards. We do see as a priority the clarification of aspects of the new system, before delving into issues of implementation.
Consequently, our recommendations should be primarily understood as setting out desired objectives. Although we describe in more detail below which action the Commission could take under 43(8) and 43(9), the ultimate choice and implementation of a specific instrument requires further consultation with the relevant stakeholders, tailoring actions to authorisations, procedural scrutiny, and broader policy considerations.

[499] Article 29 Data Protection Working Party – Technology Sub-group meeting (September 2017), Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 meetings (October 2017, December 2017, and March 2018), Workshops organised by the Study consortium (January 2018 and April 2018).

10.1. Overview of findings

The study for this report aimed at supporting the newly introduced instrument of certification in the EU data protection legislation by exploring the existing landscape, legal framework, and ultimately facilitating the Commission in its decision to exercise its power to adopt delegated and implementing acts.

The data protection certification mechanisms, seals, and marks as established mainly in Art. 42 and 43 GDPR, despite their novelty -both in terms of their formalisation with a legal provision and their set-up – are not new as an instrument in data protection. The study revealed a multitude of active certifications in the broader field of data protection, privacy, and information security with a diversity of attributes: origin, public/private ownership, normative basis, sector, territorial scope and others. The broad range of certifications already active in the field already flags one key message: notwithstanding the particularities of the mechanisms of Art. 42 GDPR, the accumulated experience, best practices, and knowledge of the existing certifications should be valued and taken on board, to the extent allowed by the conditions of Art. 42 and 43 GDPR, in the development and establishment of the new data protection certification mechanisms.

The study analysed to this end a number of active data protection certifications on the basis of a matrix of selection criteria including among others the owner (public authority, certification body, other), the concerned entity (controller or processor), sector specificity or neutrality, normative basis (regulations, technical standards, or other), subject matter, and the maturity of certifications. The analysed certifications, both EU or EU MS-based and non-EU based, were grouped in certification models according to their scope in terms of sector, SME-relevance, territorial coverage (EU-wide, international, national, sub-national), normative criteria, and certification scheme arrangements (e.g. internally managed v. outsourced certification process, monitoring by public authorities). The identification and analysis of all the different models provides an overview of all the available options for entities aiming at developing certification schemes, benchmarks for supervisory authorities when reviewing and assessing certifications, and background information for the European Commission, should it decide to exercise its powers.

Next to the lessons of existing certifications, the study delved into the specifics of the data protection certification mechanisms of Art. 42 and 43 GDPR. The study looked into the certification mechanisms in terms of certification criteria and certification process. The certification criteria are the backbone of the certification and both their formulation and

content are of paramount importance for the success and reliability of the instrument of certification as a means to demonstrate compliance with the GDPR. Given the silence of the GDPR on the specific content of the certification criteria and the parameters of the task of the supervisory authorities to approve such certification criteria on the basis of Art. 42(5) GDPR, the study provides a comprehensive set of conditions that need to met by certification criteria submitted for approval to supervisory authorities. The set of conditions, which is based on case studies (New Legislative Framework and harmonised standards, eIDAS Regulation, and the proposal for Cybersecurity Act), technical standards on conformity assessment, and the relevant GDPR provisions is provided as: a. Pre-conditions b. Subject-matter of certification c. Formulation of the certification criteria and d. High-level considerations and boundaries. The analysis showed that despite the fact that best practices can be observed from other fields, the supervisory authorities or the European Commission (via the exercise of its implementing powers or the issuance of a standardisation request to the European Standardisation Organisations) utlimately need to agree on a common assessment methodology and benchmarks that is specific to particularities of the legal framework at hand, as explained in the Chapter.

The study also analysed the certification processes as determined in the ISO/IEC 17065 standard and examined existing certifications. Again, as with the certification scope models, the certification process provides a multitude of diverse practices as per conformity assessment models with the collaboration with external auditors and the conditions for such a collaboration, the conditions for issuance of certification, the practice of gradual sanction policies, dispute resolution mechanisms and the conditions for renewal of certification (full re-assessment, partial re-assessment, etc.). Particularly useful are the practices for monitoring the granted certifications ('surveillance'), since those include a combination of methods that can be adopted by certification bodies and supervisory authorities. There is a role identified here for the European Commission, as discussed in the Recommendations of the study: the role of facilitating harmonised implementation of the provisions.

Another important issue which required a closer look is Accreditation. The study analysed the different models of Art. 43 for accreditation of certification bodies, the different roles of the players, procedures, safeguards, and the legal effects of each accreditation model. A clear finding is that while the National Accreditation Bodies already have procedures, policies, and expertise in place to start providing accreditation services to certification bodies, whereas the supervisory authorities – only with a few exceptions – have the know-how. This was revealed in the survey on accreditation launched in the framework of

the study, which showed that supervisory authorities are not familiar with the conformity assessment standard(s), while the opposite is true for National Accreditation Bodies. In addition, the application of the Accreditation Regulation to NABs imposes a series of significant obligations and conditions to those bodies (which is not necessarily the case for DPAs) such as the acceptance of each other's issued accreditation certificates, the peer evaluation system, and the requirements for independence, integrity of the organisation and its personnel, together with requirements for quality assessment, competence, and efficiency of procedures. Best practice examples can also be drawn by the fora to which the NABs participate such as the International Accreditation Forum and the European Co-operation for Accreditation. Either via guidance or as mandatory documents, those organisations already provide solutions for issues that are likely to arise in the field of data protection certification such as the competence of assessors, accreditation of bodies with activities in multiple countries, and others. The survey also provided answers to the question on the exact meaning of the term 'additional requirements' of Art. 43(1)(b) GDPR, as relating to requirements for expertise in the field of data protection, competence in performing audits in data protection processing operations, and integrity of the auditors.

Considering the significance of technical standards in the field of certification, Chapters 6 and 7 present and elaborate on the results and findings of a stakeholder survey launched in the framework of the study, as well as two workshops held in order to gather the views of controllers/processors, supervisory authorities, National Accreditation Bodies, certification bodies, standardisation bodies, SMEs and civil society, on several issues relating to standards and certification, including uptake factors and incentives. The results show that trust, recognition, technical and financial implementation issues, as well as contribution of the standard and/or certificate to legal compliance, influence the desirability of certifications, seals, and marks in the field of data protection. Through an analysis of existing technical standards, the study provides an overview of relevant technical standards useful as a basis for conformity assessment, drafting and formulation of certification criteria and requirements, normative basis for certification criteria, and other issues pertaining to the development and operation of certification mechanisms, seals, and marks. The Chapters also provide a catalogue of mechanisms to promote certification, as provided in Art. 43(9) GDPR, both with positive rewards and negative incentives. Such measures, although primarily intended to inform the actions of the European Commission, can also be useful for Member States that are tasked to encourage the uptake of data protection certification mechanisms in Art. 42(1) GDPR.

The last two Chapters of the main body of the study are devoted to certification mechanisms of Art. 42(2) GDPR, namely certifications as a tool for international data transfers. The study showed that although the certifications of Art. 42(1) – which aim to demonstrate compliance with the provisions of the GDPR- and of Art. 42(2) – which aim to show that all necessary measures are implemented to provide appropriate safeguards for a data transfer to a non-adequate third country – have the same legal basis, their content and set-up is likely to differ to a certain extent, both in terms of substance and organisation. Binding Corporate Rules and Standard Contractual Clauses can form a good starting point for the elements to be addressed in a certification mechanism of Art. 42(2) GDPR: information requirements, data protection principles, effectiveness requirements, enforcement of commitments, reporting and collaboration mechanisms, are all elements to be addressed in certification schemes of Art. 42(2) as well. However, the fact that certification involves a third party audit and an additional relationship next to the one of the data exporter and data importer, namely the one of the certification body and the data importer, introduces an additional layer (to the one of the data exporter) of responsibility to monitor and review the measures to the certification body. The study ultimately proposed a set of components necessary to form part of a certification mechanism for data transfers. Following the proposed content of the certification scheme of Art. 42(2) GDPR, we analysed and assessed the potential models of certification, and in particular whether certification of Art. 42(2) GDPR should be a stand-alone certification mechanism or form part/merged (either as modular certification or comprehensive certification) of the certifications of Art. 42(1) GDPR. The findings tend to show that, whereas not optimal for organisational purposes for the certification bodies, the mechanisms of Art. 42(2) are fit for purpose, and fulfil the criteria of provision of appropriate safeguards and transparency when presented as a stand-alone certification, developed for the purpose of data transfers with all the specificities addressed in the scheme (addressed to data importers, that are located in a third country, not subject to the GDPR, etc.).

10.2. Clustering findings in themes: clarity, transparency, implementation, and accessibility.

Theme 1: Clarity of the new certification system

Clarity relates to the certainty of meanings, obligations, and distribution of roles in the GDPR certification under articles 42 and 43.

Theme 2: Transparency of the data protection certification mechanisms, seals, and marks.

Transparency is an essential component for a certification to achieve its purpose to demonstrate compliance in line with Art. 42(1) GDPR and ultimately allow data subjects to quickly assess the level of data protection offered by a controller or processor.[500] Besides, transparency of the certification process in specific is a legal obligation in the GDPR.[501]

Theme 3: Implementation

The data protection certification mechanisms under the GDPR include a variety of novel elements in relation to existing certifications in other fields, such as for example the three accreditation models, the use of certifications for demonstration of appropriate safeguards and others. Proposals under implementation deal with practical organizational and co-ordination issues in rolling-out the new certifications under Art. 42 and 43 GDPR.

Theme 4: Accessibility

Accessibility related to the access of certifications to a broad range of controllers and processors, including SMEs and start-ups. Accessibility also deals with the actual possibility for controllers and processors, as well as data subjects, to gain access to the key components of the certification mechanisms, which ultimately reveals what a seal or a mark stands for both in B2B and B2C relations.

10.3. Possible actions based on Art. 43(8) & 43(9)

As explained in Chapter 2, Art. 43(8) and 43(9) empower but do not oblige the Commission to adopt acts. Where reference is made to the adoption of a delegated or implementing act in the possible actions outlined in the themes below, this points to possible elements to be taken into account in a possible delegated or implementing act by the Commission. The following findings and types of possible actions aim to address the issues relevant to the above themes primarily in relation to the powers of the Commission should it decide to adopt delegated or implementing acts where and when necessary. Where action instead or

[500] Recital 100 GDPR
[501] Art. 42(3) GDPR

in parallel can be taken by the EDPB in the identified areas, this is noted.[502]

10.3.1. Theme 1: Clarity

10.3.1.1. Clarification of relationship between certifications and other GDPR instruments for demonstrating compliance

Even though not strictly within the scope of the study, a topic that the research team came across often during the feedback sessions in the various workshops was the differentiation of certification from other instruments, namely codes of conduct and data protection impact assessments. Furthermore, as highlighted in Chapter 2 of this Report, but also stressed during the workshops, the lack of definitions in the GDPR on the following terms leads to a lack of clear distinction of the terms: data protection certification mechanisms, certifications, criteria, requirements, seals, and marks. In order to allow for the full potential of certifications to develop, the intended use and relationship of the instruments which can be used to demonstrate compliance and allow the data subjects to quickly assess the level of protection of relevant products and services should be clear to controllers/processors and conformity assessment bodies. Commission action in these areas will contribute to improve clarity by stipulating the requirements to be taken into account for certification mechanisms.

Type of possible actions	Options
Adoption of binding act	Adoption by the Commission of binding acts in accordance with Art. 40(9) and (10) and 43(8) and (9)
Policy/Guidance	Guidelines on codes of conduct (art. 40-41 GDPR), data protection impact assessments (art. 35 GDPR) and certifications (art. 42-43 GDPR) to be adopted by the EDPB.

Table 10-2: Clarification of relationship between certification and other instruments

10.3.1.2. Clarification of relationship between national certifications under the GDPR and the European Data Protection Seal

The matter of clarification of the relationship between the certifications approved at a national level by a DPA pursuant to Art. 42(5) GDPR and the European Data Protection Seal approved by the EDPB should be

[502] The order of presentation of each possible action (adoption of binding act, policy/guidance, and other) does not imply prioritisation.

clarified. What happens with incompatible auditing techniques of seals with the same scope at a national and European level? What happens if legal norms are interpreted differently and thus assessments lead to different results? The exercise by the Commission of its powers under Article 43(8) and (9) as described above will bring the basis for such clarifications. National certification mechanisms should not include conflicting criteria and requirements to any approved European ones.[503]

10.3.1.3. Clarity on different national accreditation models adopted in Member States

Following the diversity permitted by the GDPR in relation to bodies offering accreditation under Art. 43 GDPR and certification, the certainty of the options available to each interested certification body (for accreditation) or controller/processor (for certification) is important. Certainty can be achieved by centralizing the information and making it publicly available. This could be in a form of a register providing:

- the name of the Country
- the Name(s) and address of authorities providing accreditation under Art. 43 GDPR in each MS
- URL to websites

The GDPR already provides that a similar register should be maintained by the EDPB for accredited certification bodies, certified controllers or processors in a third country[504] and approved certification mechanisms, seals, and marks.[505] We propose to extend the register already provided by the GDPR to include the above category.

Type of possible actions	Options
Other	Expansion of the public register to be maintained by the EDPB as to include accreditation authorities providing Art. 43 accreditation in each MS.

Table 10-3: Clarity on different accreditation models across EU MS

[503] This would be similar to the adoption of European and national standards, even though in that case there is a legal obligation for standards organisations under Art. 3(6) Regulation 1025/2012.
[504] Art. 70(1)(o) GDPR
[505] Art. 42(8) GDPR

10.3.1.4. Clarity on establishment of accredited certification body in case of data transfers

Following the discussion in Chapter 8 of the Report on certification as a tool for transfers, and the fact that the GDPR does not determine where the accredited certification body should be established– namely only the EU, EU main establishment, or third country- this issue should be clarified. In addition, the ability of the accredited certification body to perform its activities in another EU MS country, the possibility and conditions of outsourcing and establishment of local collaborators and the conditions of such collaboration (accreditation by an EU DPA or NAB) should also be clarified.

10.3.2. Theme 2: Transparency

10.3.2.1. Transparency of certification criteria and assessment methodology

As seen from the analysis of existing certifications, the certification criteria and/or the methodology for assessment conformity to the scheme are not always available. While we hold that the certification criteria should in their entirety be published to ensure transparency and safeguard the reliability of the certification, seal, and mark, it is true that there are proprietary rights over assessment methodologies which feed concerns over sharing publicly the methodologies. Another solution would be publication and unhindered access to the main rationale of the assessment methodology. For example, the Ryerson Privacy by Design certification publishes an extensive list of control points, which the auditors use to assess the certification requirements. Other certifications use other methodologies such as Protection Goals or Control Goals, which they summarise on their websites.

The requirement for transparency over the assessment methodology can in any case be derived by the responsibility of certification bodies for a proper assessment. In addition, if a data protection certification mechanism is interpreted to include the assessment methodology, apart from the certification criteria and other organisational or procedural issues, then such methodology should be included in the register of the EDPB (Art. 42(8) GDPR).

Type of possible actions	Options
Policy/Guidance	Guidance providing a template for publication of the criteria and the assessment methodology or a summary thereof by the EDPB.

Table 10-4: Transparency on certification criteria and assessment methodology

10.3.2.2. Transparency of certification assessment results

Certification is granted to an applicant controller or processor once the evaluation of its processing in line with the certification criteria is successful. However, an awarded seal does not automatically entail transparency over a controller's or processor's certified processing activity (-ies). It is advisable to instruct the certification bodies to also publish a brief report summarising the scope of assessment and granted certification, the applicable certification criteria against which the processing was audited, the areas for improvement, the validity period of certification and any ongoing process on renewal of certification. A good practice in this respect is the ULD Datenschutzaudit register which includes a 10-page condensed overview of the evaluation scope, assessment, and results.[506]

Type of possible actions	Options
Adoption of binding act	Adoption of delegated act by the Commission in line with Art. 43(8) GDPR determining the minimum content of the public version of evaluation reports.
Policy/Guidance	Guidance on the content of such publicly available evaluation reports could be provided by National Accreditation Bodies in line with the ISO/IEC 17065:2012 standard. Development of evaluation reports templates could be provided by the EDPB.

Table 10-5: Transparency of certification assessment results

10.3.2.3. Transparency on scope and expiration of a granted seal

Apart from the publication of evaluation reports, additional measures should be implemented to enhance transparency of the granted certification. Not all companies or data subjects are likely to take the effort to visit a website and read the, quite often, of technical nature, evaluation report. For this reason, the seal should also already provide indications on at least the scope of the granted certification and the expiration thereof. A good example is the CNIL seal for safe boxes which includes a name of the seal which already provides information about its scope ("Label CNIL Coffre-Fort"), the date of issuance and the expiration date. Another manner to provide an indication of the scope of the granted certification, or the 'maturity level of compliance' as is

[506] See https://www.datenschutzzentrum.de/audit/register/ [accessed 30 April 2018] Another example is EuroPrise: https://www.european-privacy-seal.eu/EPS-en/awarded-seals accessed 30 April 2018

currently done in the MYOBI scheme, is by providing seals of different colour.[507] In addition, it is advised, to follow the example of eIDAS seals, and introduce data protection seals that are electronically verifiable.

Type of possible actions	Options
Adoption of binding act	Adoption of an implementing act by the Commission in line with Art. 43(9) GDPR to support the recognition of seals by colour coding types of data protection seals determining the minimum features of a seal being date of issuance, object of certification, and expiration date.
Other	On the basis of experience, launch of a study by COM with the aim to identify and measure the success rate, including preferences of data subjects regarding visual representation, of seals and marks.

Table 10-6: Transparency on scope and expiration of the seal/mark

10.3.2.4. Transparency of pricing policies

As the in-depth analysis of existing certifications and the surveys conducted in the framework of this study showed, organisations offering certification services follow very diverse pricing policies, ranging from no fee, to per hour payment or pricing policy depending on the object and complexity of assessment, or fixed prices. Some of the certification bodies do not provide information on their websites on their pricing policies. Such diversity and practices might lead to unintended results, namely exploitation or forum shopping. It is therefore recommended that transparency of pricing policies is encouraged by the Commission and Member States in line with Art. 42(1) GDPR.

10.3.3. Theme 3: Implementation

Due to the currently growing market on GDPR data protection mechanisms, and the fact that, as mentioned earlier, Art. 42 and 43 introduce a new system with several characteristics unique to the GDPR (such as allowing DPAs to act as certification bodies and accreditation bodies, both single-issue and comprehensive certification, and others) new certifications based on different models and techniques are likely to develop. In addition, the GDPR does not address all issues that usually arise throughout a certification and an accreditation process. There is

[507] This is a practice followed in the energy sector. https://ec.europa.eu/energy/eepf-labels/ accessed 30 April 2018

thus a foreseeable risk of development of practices that do not fully align with Art. 42 and 43 GDPR or that the diversity of the practices will negatively impact the aim of the data protection certification mechanisms, seals, and marks to provide a tool for controllers and processors to demonstrate compliance of their processing activities with GDPR provisions, and to offer transparency to data subjects on such certified activities.

10.3.3.1. Common or comparable approach on the matter "to the satisfaction of the competent supervisory authority"

Supervisory authorities, both when providing accreditation themselves and when providing additional accreditation requirements, have the power to reject the application of a certification body that does not demonstrate expertise, independence[508] or that there is no conflict of interest in the exercise of their activities *to the satisfaction of the competent authority.* The vague term allows supervisory authorities to follow different approaches, which could result to varying degrees of strigency in the approaches and thresholds in different Member States, while implementing the same European Regulation.

Type of possible actions	Options
Policy/guidance	Opinion or guidelines of the EDPB on the meaning of demonstration of expertise, independence and lack of conflicting interests '*to the satisfaction of the competent authority*', adoption of a common approach via the consistency mechanism, communication of benchmarks and different examples/scenarios.
Other	EDPB to follow the developments on different cases encountered in MS and update of the benchmarks.

Table 10-7: Adoption of a common approach on thresholds for accreditation

10.3.3.2. Certification criteria

As analysed in Chapter 4 and stressed by the workshop participants (January and April 2018) [509] the content of the certification criteria is of utmost importance and should meet certain high standards as provided by the GDPR. The Commission may adopt a delegated act to lay down a general framework specifying all requirements for the data protection

[508] Art. 43(2)(a) GDPR.
[509] See Annex 6.

certification mechanisms, to be further operationalised by the criteria approved by DPAs/EDPB.

Type of possible actions	Options
Adoption of binding act	Adoption of a delegated act by the Commission in line with Art. 43(8) GDPR to lay down the general framework for certification mechanisms.
Policy/Guidance	EDPB to work on guidelines and on keeping up-to-date the procedures and assessment criteria for approval of the certification criteria (Art. 42(5) GDPR) by the DPAs.
	The EC to follow closely the developments at international standard setting organisations and European standard setting organisations on the drafting and development of new technical standards relevant to GDPR.

Table 10-8: General framework and minimum content of certification criteria

10.3.3.3. Common benchmarks for certification procedures

As stressed in the study, [510] there is a diversity of certification models in the market, which is likely to render difficult the task of supervisory authorities to approve certification criteria and keep an oversight over the granted certifications. The supervisory authorities may be assisted in their tasks by using common benchmarks for certification procedures in data protection certification mechanisms. Such benchmarks may be provided by conformity assessment standards, thus standards relating to procedural and organizational issues on conformity assessment. As discussed in Chapter 7, promoting *procedural standards* could be considered by means of delegated or implementing acts.[511] Potential candidates include ISO/IEC standards in the 17000 series that could ensure that the certification procedures and accreditation are aligned with a common framework. One of the elements that need to be benchmarked is the assessment methodology. As seen in the case studies in Chapter 4, as well as in the analysis of existing certifications, certification bodies use a broad range of methodologies to assess how certification criteria are met by the applicant entity. Apart from the issue of transparency of assessment methodologies, the soundness and quality of the methodologies is of paramount importance for the reliability of the certification mechanisms.

[510] See p. 80
[511] See p. 129f

Type of possible actions	Options
Adoption of binding act	Adoption by the Commission of binding acts in line with Art. 43(8) and Art. 43(9) GDPR to lay down technical standards on conformity assessment to ensure the adoption of common benchmarks in certification processes.[512]
Policy/Guidance	Particularisation of the requirements of the conformity assessment technical standards in the context of data protection certifications by the EDPB, including a list of minimum documents necessary for the assessment.
Other	Open a dialogue with trained auditors. The NABs, in collaboration with the DPAs or the EDPB, could establish mandatory training seminars for auditors of certification bodies that apply for accreditation.
	Encourage the development of codes of ethics for certification auditors and quality manuals.

Table 10-9: Common benchmarks for certification procedures

10.3.3.4. Quality of accreditation

It is recommended that initiatives are undertaken to ensure that the accreditation provided under the different models is of equivalent quality. While for the NABs there are already established procedures provided for in the Accreditation Regulation ('peer assessment'), these procedures are not guaranteed in the case of the other models of Art. 43 GDPR.

Type of possible actions	Options
Adoption of binding act	Adoption of a delegated act by the Commission in line with Art. 43(8) GDPR requiring the adoption of accreditation procedures based on specific standards on accreditation.[513]
Policy/Guidance	Guidelines by the EDPB to address issues of peer assessment, the applicability of the ISO/IEC 17065 standard in the Accreditation Model of Art. 43(2) GDPR and the requirements of Regulation 765/2008 to supervisory authorities when acting as accreditors.
Other	Establishment of task force and knowledge database among

[512] See Annex 5 (separate document)
[513] See discussion in Chapter 7 p. 129f

	National Accreditation Bodies and supervisory authorities.
	Encourage the development of codes of ethics of accreditation auditors and quality manuals.

Table 10-10: Measures to ensure quality of accreditation

10.3.3.5. International cooperation for enforcement of certifications for data transfers

The analysis on the commitments of data importers accompanying the data protection certifications showed especially in cases of third countries with no sufficient mechanisms provided for in the national legislation enforceability is not always guaranteed. A framework agreement for cooperation between EU data protection authorities and enforcement authorities in third countries should be developed. International enforcement cooperation could be fostered in already existing networks or structures such as the International Conference of Data Protection and Privacy Commissioners. In addition, enforcement should be sought in the framework of cross-border accreditation via established channels such as the International Accreditation Forum.

10.3.4. Theme 4: Accessibility

10.3.4.1. Access to the ISO/IEC 17065:2012 standard and other relevant conformity assessment standards

Type of possible actions	Options
Policy/Guidance	Develop an open access repository of technical standards on conformity assessment which are used for the GDPR certification mechanisms.

Table 10-11: Open access policy for conformity assessment standards

10.3.4.2. Adaptation of certification pricing policies to risk of processing and size of organisation

To facilitate accessing certification, the size of the applicant of organisation should be considered alongside with other elements. The Commission, MS, DPAs and EDPB, are recommended to encourage the certification bodies to adopt pricing policies and evaluation assessments based on the nature of data, risks and scale of processing, and among other factors the qualification of the applicant as SME or start-up.

10.3.4.3. Encourage summaries of granted certifications in layman's terms

The, often complex, language of certifications is not accessible to everyone. To enable data subjects to assess the level of data protection of the processing of a controller or a processor, the Commission, the DPAs or the EDPB could encourage a summary of the scope of certifications in layman's terms (for example in a form of F.A.Q).

Bibliography

Article 29 Data Protection Working Party "Working Document establishing a Model Checklist application for Approval of Binding Corporate Rules" 2005, WP 108

Article 29 Data Protection Working Party "Working Document Setting-up a framework for the structure of Binding Corporate Rules", 2008, WP 154

Article 29 Data Protection Working Party "Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules", 2008, WP153

Article 29 Data Protection Working Party, 'Opinion 02/2015 on CSIG code of conduct on cloud computing', WP232, adopted on 22 September 2015

Article 29 Data Protection Working Party, 'Opinion 8/2007 on individuals with regard to the processing of personal data in Jersey' WP141, adopted on 9 October 2007

Article 29 Data Protection Working Party, 'Opinion 01/2012 on the data protection reform proposals' WP 191, adopted on 23 March 2012

Article 29 Data Protection Working Party, 'Opinion 11/2011 on the level of protection of personal data in New Zealand' WP182, adopted on 4 April 2011

Article 29 Data Protection Working Party, 'Opinion 4/2002 on the level of protection of personal data in Argentina' WP63, adopted on 3 October 2002

Article 29 Data Protection Working Party, 'Opinion 5/2003 on the level of protection of personal data in Guernsey' WP79, adopted on 13 June 2003

Article 29 Data Protection Working Party, 'Opinion 6/2009 on the level of protection of personal data in Israel'' WP165, adopted on 1 December 2009

Article 29 Data Protection Working Party, 'Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay' WP177, adopted on 12 October 2010

Article 29 Data Protection Working Party, 'Opinion 7/2009 on the level of protection of personal data in the Principality of Andorra' WP166, adopted on 1 December 2009

Article 29 Data Protection Working Party, Consultation version of Guidance on accreditation of certification bodies, WP261, adopted on 6 February 2018

Bundesamt für Sicherheit in der Informationstechnik "The PP/ST Guide" August 2010 Version 2

Barron Mark R, 'Creating Consumer Confidence or Confusion? The Role of Product Certification in the Market Today' (2007) 11(2) Marquette Intellectual Properties Law Review 427

Bartley Tim, 'Certification as a Mode of Social Regulation' [2011] Handbook on the Politics of Regulation 441

Bartley Tim, 'Transnational Governance and the Re-centered State: Sustainability or Legality?' (2014) 8 Regulation & Governance 93
Bartley Tim, 'Certifying Forests and Factories: States, Social Movements, and the Rise of Private Regulation in the Apparel and Forest Products Fields' (2003) 31 Politics & Society 433

Bast Jürgen, "Is There a Hierarchy of Legislative, Delegated and Implementing Acts?" In Carl Fredrik Bergström and Dominique Ritleng, Rulemaking by the European Commission: The New System for Delegation of Powers, Oxford Scholarship Online, 2016

Boiral Olivier, 'ISO Certificates as Organizational Degrees? Beyond the Rational Myths of the Certification Process' (2012) 33(5-6) Organization Studies 635

British Standards Institution, 'Certification to ISO/IEC 27001 Information Security Management' (Bsigroup, 2018)

British Standards Institution, 'Personal Information Management' (Bsigroup, 2018)

Bundesamt für Sicherheit in der Informationstechnik, 'Referenzierung des Trusted Cloud Data Protection Profile V 1.0 auf C5' (2017)

Busch Lawrence, Standards: Recipes for Reality (MIT Press, 2012)

Cafaggi Fabrizio et. al. 'Transnational Private Regulation' (OECD 2013)

Casadesús Marti et al., 'Benefits of ISO 9000 implementation in Spanish industry' (2001). 13(6) European Business Review 327

CEN and CENELEC, 'Guide 15 Tasks and responsibilities of the New Approach Consultants'

CEN/TC 52, 'Business Plan. Safety of Toys' (2017)

Civic Consulting, 'A Pan-European Trustmark for E-Commerce: Possibilities and Opportunities' (2008)

Cloud Security Alliance, 'Cloud Controls Matrix Working Group' (CSA, 2017)

Cloud Security Alliance, 'Cloud Security Alliance Issues New Code of Conduct for GDPR Compliance' (CSA, 2017)

Cochoy Franck et al., 'Comment l'écrit Travaille l'organisation : Le Cas Des Normes ISO 9000' (1998) 39–4 Revue Française de Sociologie

Cochoy Franck, 'De l'"AFNOR" à "NF", Ou La Progressive Marchandisation de La Normalisation Industrielle' (2000) 18(102) Réseaux 63

Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC OJ L 181, 4.7.2001

Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council, OJ L 344, 17.12.2016

Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, OJ L 235/7, 9.9.2015

Commission Regulation (EC) No 1235/2008 of 8 December 2008 laying down detailed rules for implementation of Council Regulation (EC) No 834/2007 as regards the arrangements for imports of organic products from third countries, OJ L 334, 12.12.2008

Commission Staff Working Document on Knowledge-Enhancing Aspects of Consumer Empowerment 2012-2014, 'Consumer attention and understanding of labels and logos', (2012) (SWD, Final, 19.7.2012 4.1)

Conroy Michael E., Branded! How the Certification Revolution Is Transforming Global Corporations (New society publish 2007)

Consumer Research Associates Ltd., Certification and Marks in Europe, A Study commissioned by EFTA, European Free Trade Association, January 2008

Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, as amended by Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 OJ L 331 1 7.12.1998

Council Regulation (EC) No 834/2007 of 28 June 2007 on organic production and labelling of organic products and repealing Regulation (EEC) No 2092/91, OJ L 189, 20.7.2007

De Hert Paul, Papakonstantinou Vagelis, Kamara Irene, 'The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection' (2016) 32(1) Computer Law and Security Review 16

Directive 2000/70/EC of the European Parliament and of the Council of 16 November 2000 OJ L 313 22 13.12.2000

Directive 2001/104/EC of the European Parliament and of the Council of 7 December 2001 OJ L 6 50 10.1.2002

Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007 OJ L 247 21 21.9.2007

Directive of the European Parliament and the Council on the safety of toys (2009) OJ 2 170/01

Dumortier Jos, 'Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation)' (2016) available: https://ssrn.com/abstract=2855484 accessed 12 March 2018

ENISA, 'Recommendations on European data protection certification' (November 2017)

ENISA, 'Security certification practice in the EU - Information Security Management Systems - A case study' (2013)

ETSI, 'All Active Work Items for CYBER For Current Status: From 'Creation of WI by WG/TB' Up to 'End of pre-processing' ' (Work Programme, 2018)

European Commission "Vademecum on European Standardisation in support of Union Legislation and Policies, Part I, Role of the Commission's Standardisation requests to the European Standardisation Organisations", Commission Staff Working Document, SWD 205 final (2015)

European Commission "Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council" OJ L39/5 (2010)

European Commission "Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under the Directive 95/46/EC following the Judgement by the Court of Justice in Case C-362/14 (Schrems)", COM(2015) 566 final

European Commission, 'Commission Notice. The 'Blue Guide' on the implementation of EU products rules 2016' (26.7.2016), OJ C 272/01

European Commission, Communication from the Commission to the European Parliament and the Council "Exchanging and Protecting Personal Data in a Globalised World" COM (2017)

European Commission, 'Report From The Commission To The European Parliament, The Council And The European Economic And Social Committee on the implementation of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93', (COM/2013/077 final)

European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Unleashing the Potential of Cloud Computing in Europe", COM (2012) 529 final (27 September 2012), 8

European Commission, CERTIF 2013-02– Requirement to seek accreditation in the Member State of establishment - IMP N006

European Commission, Communication from the Commission to the European Parliament and the Council "Exchanging and Protecting Personal Data in a Globalised World" COM (2017) 7 final, 13

European Committee for Standardization, 'CEN/TC 224 - Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment' (CEN, 2018)

European Committee for Standardization, 'Internal Regulations Part 3' [2017] 1(1) Principles and rules for the structure and drafting of CEN and CENELEC documents

European Committee for Standardization, 'The 'New Approach'' (CEN, 2016)

European Data Protection Board, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 (public consultation version, adopted 25th May 2018)

Fumy Walter, 'Cybersecurity and Data Protection standards in support of European policy' (presentation given at Cybersecurity Act - Establishing the link between Standardization and Certification', Brussels, 13 February 2018)

Gaultier, Thomas. "Cross-Border Mediation: A New Solution for International Commercial Settlement?." INT'L L. PRACTICUM 26 (2013): 38-42.

IAF, IAF Mandatory Document for Harmonisation of Sanctions to be applied to Conformity Assessment Bodies, Issue 1, Version 2, 2010

International Accreditation Forum, Memorandum of Understanding, Issue 6, 26 February (2016)

International Organization for Standardisation, 'ISO/IEC JTC 1/SC 27' (2017)

InVeo, 'ISDP 10003:2015 Data Protection Certification'

ISO/IEC 15408 Information technology -Security techniques -Evaluation criteria for IT security

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

Japanese Industrial Standards JIS Q 15001:2006 - Personal Information Protection Management System - Requirements

Kamara Irene, "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'", in European Journal of Law and Technology, Vol 8, No 1, 2017

Kamara Irene, De Hert Paul, 'Art. 42 & 43 GDPR' in Döhmann Spiecker, Vagelis Papakonstantinou, Gerrit Hornung, Paul De Hert (eds), Commentary on the European General Data Protection Regulation (NOMOS 2019, forthcoming)

Kamara Irene, De Hert Paul, 'Data protection certification in the EU: Possibilities, Actors and Building Blocks in a reformed landscape' in Rowena Rodrigues and Vagelis Papakonstantinou (eds), Privacy and Data Protection Seals (T.M.C. Asser Press 2018)

Kawakami Mark T. et al. 'Certification: a sustainable solution? Insights from Dutch companies on the benefits and limitations of CSR certification in international supply chains' Utrecht, MVO Nederland, (2014)

Keeney Ralph and Gregory Robin, 'Selecting attributes to measure the achievement of objectives' (2005) 53(1) Operations Research 1

Kuner Christopher, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' [2017] 18(881) German Law Journal

Lachaud Eric, 'Could the CE Marking Be Relevant to Enforce Privacy by Design in the Internet of Things?' in Serge Gutwirth, Ronald Leenes, and Paul De Hert (eds) Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection (Springer Netherlands 2016)

Lachaud Eric, 'The General Data Protection Regulation Contributes to the Rise of Certification as Regulatory Instrument' (2017) Computer Law & Security Review

Macenaite Milda and Kosta Eleni, 'Consent for processing children's personal data in the EU: Following the US footsteps?' (2017) 26(2) Information & Communications Technology Law 146

Meidinger Errol, 'Forest Certification and Democracy' (2010) 16 Legal Studies Research Paper

Mitrakas Andreas, 'The emerging EU framework on cybersecurity certification.' Datenschutz und Datensicherheit-DuD 42, no. 7 (2018): 411-414

OECD 'Guidelines for Consumer Protection in the Context of Electronic Commerce' (OECD, 1999)

OECD, 'Innovation Vouchers' (OECD Innovation Policy Platform, 2010)

Otto Paul and Antón Annie, 'Managing Legal Texts in Requirements Engineering' in Kalle Lyytinen, Pericles Loucopoulos, John Mylopoulos, and Bill Robinson (eds), Design Requirements— Engineering: A Ten-Year Perspectives (Springer Berlin Heidelberg 2009), 374-393

Pettiti Priscilla, 'Il marchio collettivo. Commento alla nuova legge sui marchi' (1994) 9-10 Rivista del Diritto Commerciale e del Dirritto generale delle Obbligazioni 621

Ramli Nor Azam, 'Protection profile, a key concept in the common criteria' SANS Institute InfoSec Reading Room (2003) GSEC Practical Assignment Version 1.4b
Regulation (EC) N Directive 2001/104/EC of the European Parliament Council of 29 September 2003 OJ L 284 1 31.10.2003

Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, OJ L 218/30.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, OJ L 119, 4.5.2016

Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014

Regulation 1025/2012 of the European Parliament and the Council on European standardisation of 25 October 2012 OJ L 316/12

Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (2016) OJ 2 119/01

Rodrigues Rowena et al. 'EU Privacy seals project. Comparison with other EU certification schemes. Final Report Study Deliverable 2.4' (2014)

Rodrigues Rowena, Barnard-Wills David, De Hert Paul, 'The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR' (2016) 30(3) International Review of Law, Computers & Technology 248

Rodrigues Rowena, Barnard-Wills David, Wright David, De Hert Paul, Papakonstantinou Vagelis,'EU Privacy seals project. Inventory and analysis of privacy certification schemes' (Publications Office of the European Union 2013)

Rotenberg Mark and Jacobs Daniel, 'Updating the Law of Information Privacy: The New framework of The European Union' (2012) 36 Harvard Journal of Law & Public Policy 607, 641

Rubino-Sammartano, Mauro. *International arbitration law and practice*. Juris Publishing, Inc., 2014.

Shara Monteleone and Puccio Laura, 'From Safe Harbour to Privacy Shield Advances and shortcomings of the new EU-US data transfer rules' (2017) EPRS

Tarí Juan José et al., 'Benefits of the ISO 9001 and ISO 14001 Standards: A Literature Review' (2012) 5 Journal of Industrial Engineering and Management 297

TrustArc, 'Extend your privacy commitment with the APEC Cross Border Privacy Certification' (TrustArc, 2018)

United Nations (2016) UNCITRAL Model Law on International Commercial Arbitration 1985 with amendments as adopted in 2006." United Nations Publication

Ustaran Eduardo et al. European Data Protection: Law and Practice. IAPP Publication (2017)

Van der Zeijden Paul et al., 'Keurmerken, erkenningsregelingen en certificaten; klare wijn of rookgordijn? Zoetermeer: EIM Onderzoek voor Bedrijf en Beleid" (2002)

Verbruggen Paul, Havinga Tetty, 'The Rise of Transnational Private Meta-Regulators' (2014) 20(10) TBGI Project Subseries

Voigt Paul and von dem Bussche Axel, The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer, 2017

Wiengarten Frank et al., 'A Supply Chain View on Certification Standards: Does Supply Chain Certification Improve Performance Outcomes?, ISO 9001, ISO 14001, and New Management Standards' (Springer 2018)

World Fair Trade Organization and Fairtrade Labelling Organizations International, 'Charter of Fair Trade Principles' (January 2009)

Annex 1: Glossary

[separate document]

Annex 2: Overview of existing certifications in data protection

[separate document]

Annex 3: Factsheets per analysed certification

[separate document]

Annex 4: Accreditation survey

[separate document]

Annex 5: Stakeholder survey

[separate document]

Annex 6: Workshop Reports

[separate document]