Recommendations on European data protection certification

Kamara, Irene; Burnik, Jelena

Publication date:
2017

Recommendations on European Data Protection Certification

VERSION 1.0
NOVEMBER 2017

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use isdp@enisa.europa.eu.
For media enquires about this paper, please use press@enisa.europa.eu.

ISBN 978-92-9204-238-7, DOI 10.2824/787306

Table of Contents

Executive Summary

The General Data Protection Regulation (EU) 679/2016 ('GDPR')[1] will be, as of 25 May 2018, the main data protection legal framework in the EU directly applicable in all Member States, repealing the Data Protection Directive 95/46/EC. The Regulation provides for a harmonization of the legal data protection regime throughout the EU, re-enforces several principles and obligations of the Directive, it repeals and adds new provisions, including ones on data protection certification, seals and marks. Data protection certifications, seals and marks have the potential to play a significant role in enabling data controllers to achieve and demonstrate compliance of their processing operations with GDPR provisions. An additional function of certification, in the context of the GDPR, is to enhance transparency, since certifications, seals, and marks allow data subjects to "*quickly assess the level of data protection of relevant products and services*". The objective of this report is to identify and analyse challenges and opportunities of data protection certification mechanisms, including seals and marks, as introduced by the GDPR, focusing also on existing initiatives and voluntary schemes.

Certification, as a conformity assessment activity against specified requirements, is performed and attested by a third party. These requirements are derived from technical standards or legislation, as in the case of certification under GDPR, where the secondary EU legislation provides the normative framework as a basis for the assessment requirements. The outcome of a successful certification (process) is a certificate (thus a document), and/or a seal, that attests that the applicant organisation meets the requirements (substantive and procedural) specified in the certification scheme, and provided in technical standards or legislation. In the near future, it is also possible that such requirements, originating from GDPR provisions, are also provided in technical standards.

Certification can be mandatory, when a relevant obligation for certification is established in legislation or voluntary when such obligation is not legally imposed, as in the case of GDPR certifications, which rely on the decision of a data controller or a processor to submit oneself to the certification procedure. Certification, under GDPR, is well linked to the newly introduced principle of accountability and appears to be limited to substantive requirements related only to GDPR provisions, must concern specific processing operations and can only be pursued only by data controllers or data processors, as they perform the personal data processing.

Currently, several privacy and data protection related certifications exist that are targeted at products and services, processes, and management systems and are based on either the existing legislation or technical standards. Certifications based on the management standards, such as the ISO/IEC 27001 may target a single business process, a particular service or the whole business process of an organization. There are also certifications such as EuroPrise, which focus on the processing operations performed within a service or by a product. The CNIL privacy seals offer a variety of scopes, which range from governance, products (digital safe boxes), procedures (audit procedures covering the processing of personal data) to courses (data protection training courses). Certifications targeting governance aspects and management systems are different from certifications targeting processing (processing as such or processing as part of a service

[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), L 119/1 4.5.2016

or a product). Certifications on management and governance issues are more “process-oriented” than “goal-oriented”.

The data protection mechanisms of GDPR Articles 42 and 43 can be considered as goal-oriented certifications; the focus should not be only on whether measures are in place, but also to what extent such measures are sufficient in ensuring compliance. However, the GDPR provisions on certification also introduce a number of challenges that relate to the interpretation of provisions and the terminology, the disposal of different accreditation models, the consistency of benchmarks and approval procedures by competent authorities and connected questions of mutual recognition and harmonization at national and European level.

Following the analysis, the main recommendations of the report are listed below.

- National certification bodies and supervisory authorities (DPAs), under the guidance and support of the European Commission and the European Data Protection Board (EDPB), should pursue a common approach on inception and deployment of GDPR data protection certification mechanisms.

- The European Data Protection Board (EDPB), in close cooperation with national certification bodies and supervisory authorities (DPAs), should promote an EU scalable approach with approved and widely accepted criteria.

- National certification bodies and supervisory authorities (DPAs), with the support of the European Data Protection Board (EDPB) and the European Commission, should provide guidance and promote best practises to ensure consistency and harmonization in the deployment of GDPR data protection certification mechanisms.

- The European Commission and the European Data Protection Board (EDPB) should stimulate the establishment of safeguards that will ensure trustworthiness and transparency of the certification process.

- The European Commission and the European Data Protection Board (EDPB), in close cooperation with national certification bodies and supervisory authorities (DPAs), should stimulate the exchange of best practises and lessons learnt from certification practices in other well established domains (e.g. cybersecurity).

1. Introduction

The General Data Protection Regulation (EU) 679/2016 ('GDPR')[2] will be, as of 25 May 2018, the main data protection legal framework in EU directly applicable in all Member States, repealing the Data Protection Directive 95/46/EC. The Regulation provides for a harmonization of the legal data protection regime throughout the EU, re-enforces several principles and obligations of the Directive it repeals and introduces new provisions such as the data protection by design and data protection by default. In order to enhance transparency of the processing operations of the data controllers and the processors, the Regulation introduces also specific provisions on certification, seals and marks.

According to Article 42 of GDPR, "The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors". In the Recitals of the Regulation, it is stated, "*In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services*".[3]

Against this background, in accordance with its 2017 Programming Document[4], ENISA initiated a project in the area of data protection certification mechanisms, seals or marks with the aim of imprinting the current landscape and providing guidance for further work in the field. This project was executed in parallel to the Agency's activities in the area of cybersecurity certification in order to be afterwards able to draw useful conclusions, experiences and best practises from both domains. This report is the result of this work and is expected to consist the basis of the comparative analysis described earlier that can be carried out in the next years.

1.1 Objectives of the report

The objective of this report is to identify and analyse challenges and opportunities of data protection certification mechanisms, including seals and marks, as introduced by the GDPR, focusing also on existing initiatives and voluntary schemes. More specifically the report aims at:

- Elaborating on the main aspects of certification, seals and marks in personal data protection.
- Identifying existing certifications in the greater area of privacy and/or data protection.
- Identifying the main challenges and opportunities, both at organizational and technological level, of data protection certification regime under GDPR with a look towards a common EU data protection certification framework.
- Making proposals for future steps, both at technological and organisational level, towards data protection certification that would be a contributor to greater compliance with data protection rules in the EU.

[2] 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), L 119/1 4.5.2016

[3] Recital 100 GDPR

[4] ENISA (2016) ENISA Programming Document 2017-2019 : Available at https://www.enisa.europa.eu/publications/corporate/enisa-programming-document-2017-2019/view

1.2 Methodology

The report was supported by an expert group, comprising of: Jelena Burnik (Data Protection Authority of Slovenia) and Irene Kamara (Tilburg University and Vrije Universiteit Brussel)[5]. The research was based on a literature review, legal analysis, and analysis of certifications. Several standards were reviewed, together with selected existing certification schemes in the broader area of privacy, data protection and conformity assessment. Significant studies in the field of Privacy seals and certification formed a useful basis for the analysis of certifications, but also for the identification of issues and challenges of certifications deployed before the GDPR came into play. The GDPR, especially Articles 42 and 43 of the GDPR, were analysed to provide insights on the newly introduced data protection certification mechanisms.

1.3 Structure of the report

Section 2 of the report introduces basic certification concepts and makes correlations with the data protection and privacy terminology as used in the GDPR. It aims at familiarising data protection experts with the terminology of certification and clarifying concepts that are relevant to the GDPR certification, established in Articles 42 and 43 of the GDPR. Section 3 introduces the key elements of Articles 42 and 43 of the GDPR. Section 4 presents an overview of the research and analysis conducted on the existing certification schemes relevant to data protection. This part aims to provide insights on how the market of data protection certification works, before the GDPR applies, and offer lessons for the data protection certification mechanisms of Art. 42 and 43 of the GDPR. Section 5 focuses on the open questions and challenges for the establishment and successful take-up of the certifications, but also for the role of certifications as a transparency and accountability instrument under the GDPR. Lastly, section 6 concludes the report with recommendations, drawn based on the lessons learned from the analysis of existing certification schemes and the analysis of the GDPR provisions. These recommendations are meant to provide high-level guidance to supervisory authorities, certification bodies, and controllers/processors that intend to be involved in certification in the field of data protection.

[5] Disclaimer: Any views expressed in this report by the members of the expert group only reflect their own views and analysis and do not necessarily reflect or in any way prejudice the views of organizations they are affiliated with.

2. Basic concepts in certification

The General Data Protection Regulation introduces provisions on certification to enhance transparency of the processing operations of the data controllers and the processors. The legislature also envisaged a role of certification in assisting controllers and processors to demonstrate compliance with the Regulation[6]. The following section outlines the main aspects in existing certification practice[7], as applicable to the newly established data protection certification regime under the GDPR.

2.1 Normative basis

Certification is a conformity assessment activity.[8] Certification entails "*the provision of assessment and impartial third-party attestation that fulfilment of specified requirements has been demonstrated*"[9]. The requirements are usually derived from technical standards or legislation. The latter is the case of certification in the field of data protection, where the secondary EU legislation safeguarding the right to protection of personal data provides the normative framework as a basis for the assessment requirements. It is also possible that requirements are embedded in a technical standard, which is inspired by the GDPR provisions. The GDPR provisions need to be further elaborated to be fit-for-purpose for certification. As the ISO/IEC 17067:2013 standard provides "*where it is necessary to elaborate upon the requirements to remove ambiguity, the explanations should be formulated by competent people and should be made available to all interested parties*".

2.2 Third-party assessment Vs self-assessment

As its definition makes clear, certification is a third-party conformity assessment activity. The assessment is performed by a party, other than the organisation that seeks certification (first party) and other than the entity (if any) requiring the organisation to be certified (second party). In terms of data protection, the first party assessment would be a data controller or a processor self-assessing its compliance with the GDPR. This model would resemble a data protection impact assessment, in terms of the actors involved in the process and the nature of a self-assessment exercise. A second party assessment would take place when a data controller assesses whether a data processor, with which it collaborates, complies with the General Data Protection Regulation. In that case, a data controller would be the second party in the assessment process. Certification however requires assessment by a third independent party, which usually is a certification body. In the case of the GDPR, as explained in section 3, the third party may be either an accredited certification body or a Data Protection Authority. It is important to stress that while third-party assessment leads to certification, self-assessment does not lead to certification. The self-assessor may issue a self-declaration of conformity, but such a declaration has nothing to do with Art. 42 and 43 GDPR.

[6] As set out in GDPR Recital 100 and GDPR Article. 42 paragraph 1
[7] For example in the context of well established procedures of certification against international ISO/IEC conformity assessment standards and other.
[8] The ISO/IEC 17000 standard defines conformity assessment as: "demonstration that specified requirements (relating to a product, process, system, person or body are fulfilled"
[9] ISO/IEC 17067:2013

2.3 Certification scheme

A certification scheme is a document that includes the rules, procedures, and management for carrying out certification for a specific product, process, or service.[10] The owner of a certification scheme may be a certification body, a public (supervisory) authority (for instance a data protection authority), or a private actor (which nevertheless is not itself active in the sector targeted by its certification scheme).

2.4 Certification requirements, procedural aspects and criteria

Following the non-harmonised terminology in the field of certification, several terms are used to signify identical concepts. According to the terminology proposed by ISO and IEC, a certification requirement is a requirement "that is fulfilled by the client as a condition of establishing or maintaining certification". The term includes both the *substantive* requirements (otherwise called 'product/process/person' requirements) and *procedural* requirements. The substantive requirements are derived from the normative basis. Data subjects' rights (Arts. 15-22 GDPR), data security (Art. 32 GDPR), data protection by design (Art. 25 (1) GDPR) and data protection by default (Art. 25(2) GDPR) offer, for instance, a normative basis that may be further specified in substantive certification requirements. At the same time, procedural requirements are also part of a certification scheme and necessary to be fulfilled by the party seeking certification.[11] Such procedural requirements would for example specify under which conditions a data controller may use the acquired certificate, what are surveillance periods, the compensation structure, etc. Some of the procedural aspects are already clarified by the GDPR – for example the length of certification validity of 3 years (Art. 42(7)). Some existing certification schemes might use the term 'criteria' to signify the substantive (product/process/person) requirements.[12] The GDPR seems to refer to the substantive requirements as the "criteria" and to procedural requirements as "requirements".

2.5 Certificates, seals and marks

The outcome of a successful certification (process) is a certificate (thus a document), and/or a seal, that attests that the applicant organisation meets the requirements (substantive and procedural) specified in the certification scheme, and provided in technical standards or legislation. As the following sections of the report indicate, there is no uniform approach in practice on the outcome of a successful certification process. In some cases, there is sector-specific legislation that defines the terms and clarifies their legal significance. In the context of electronic identification and trust services for electronic transactions, the Regulation 920/2014 defines 'electronic seal' as "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"[13] and a 'certificate for electronic seal' as a "an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person"[14]. Certification schemes may provide that a successful assessment leads to a certificate or a seal or both.

In addition, there might also be a mark available for use by the organisation that was granted with certification. Such a mark or logo is a sign of a successful certification process. The terms 'mark', 'trademark' or 'trustmark' are sometimes used interchangeably in practice, but 'trademark' also bears

[10] This generic definition based on the ISO/IEC 17067:2013. The issue of the subject matter of the data protection certification mechanisms as provided in the GDPR is further discussed in section 5.
[11] The ISO/IEC 17065:2012 standard provides examples of such requirements. One example is the payment of fee from the applicant organisation to the certification body.
[12] An example is the EuroPrise certification.
[13] Art. 3(25) Regulation 910/2014
[14] Art. 3(29) Regulation 910/2014

legal significance, as it implies a *registered* trademark in line with national or regional legislation.[15] The role of the mark is to identify the issuer and the aspects covered by the mark in a clear way.[16]

2.6 Accreditation

According to the Regulation 765/2008 (: Accreditation Regulation) accreditation is "*an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity*." In other words, accreditation aims to ensure that the certification body, or any other conformity assessment body, has the necessary competence to carry out its tasks. The assessment in the framework of accreditation is not limited to independence, capacity, resources, and other requirements, but extends to the subject matter, such as for instance competence in information security or data protection matters. Each Member State has, in principle, one National Accreditation Body (NAB) which grants accreditation certificates to conformity assessment bodies. Even though in general a certification body may operate without being accredited, this is not the case for the data protection certification mechanisms of the GDPR, as Art. 43 explicitly requires accreditation of the certification body.

2.7 Mandatory Vs voluntary certification

Certification may be mandatory, when a relevant obligation for certification is established in legislation. Examples of mandatory certification exist in the EU legislation, but are scarce.[17] The most common mandatory mark is the CE marking, which however, is not considered certification, but *self-declaration of conformity*. Any entity is free to declare its compliance with the harmonised legislation imposing the obligation to bear a CE marking, in principle, without an assessment from a third independent body. In the field of EU data protection, both under the Data Protection Directive 95/46/EC and the GDPR, data protection certification is voluntary. The voluntary nature of certification relates to the *decision* of a data controller or a processor to submit oneself to the certification procedure.[18] Furthermore, a controller or processor may choose other or additional means to demonstrate compliance with its legal obligations stemming from the GDPR.

2.8 Privacy-seals Vs data protection certifications

One last clarification should be made regarding the distinction between privacy-related certifications and seals on the one hand, and data-protection certifications and seals on the other. Such a distinction follows the distinction of the right to protection of personal data and the right to respect private and family life,

[15] For instance, in line with Art. 27(1) of the Directive (EU) 2015/2436, a certification mark means a "*trade mark which is described as such when the mark is applied for and is capable of distinguishing goods or services which are certified by the proprietor of the mark in respect of material, mode of manufacture of goods or performance of services, quality, accuracy or other characteristics, from goods and services which are not so certified*".

[16] ISO/IEC 17030:2013

[17] Directive 2004/49/EC establishes safety certification granted by a public authority as a mandatory requirement for a railway undertaking to be granted access to a railway infrastructure. (Art. 10)

[18] Kamara I. De Hert P. (2017)

home and communications.[19] This study is primarily concerned with the GDPR certification, which is data protection certification.[20]

[19] Read further De Hert P. and S. Gutwirth (2008), Gonzalez-Fuster G. (2014)

[20] Despite the focus of the study being data protection certification, the research for the following sections was not limited to strictly data protection related certifications, which are still limited in number due to the newly introduced provisions in the EU data protection legislation (Art. 42 and 43 GDPR).

3. Main elements of GDPR Articles 42 and 43

The GDPR introduced certification as a means for a data controller or a data processor to demonstrate compliance of a processing operation with the Regulation. An additional function of certification in the context of the GDPR is to enhance transparency, since certifications, seals, and marks allow data subjects to "quickly assess the level of data protection of relevant products and services".[21]

3.1 Certification as an accountability-based mechanism

Certification is well linked to the newly introduced principle of accountability. As already highlighted by the Article 29 Data Protection Working Party in 2010, data protection needed additional mechanisms that translate legal requirements into real data protection measures.[22] Certification and seals are treated as accountability-based mechanisms, due to their potential effect to facilitate scalability, compliance, transparency, and to some extent legal certainty.

Art. 5(2) GDPR requires the data controller to both comply with the principles relating to the processing of personal data and demonstrate its compliance. Demonstration of compliance in practice may require multiple actions, such as proper documentation and record keeping (in line with art. 30 GDPR). Certification can play a role in that respect; a controller that has had its processing operations successfully evaluated by a certification body, may use the certification and its supporting documentation as an element to demonstrate compliance to the supervisory authority. The fact that data protection certification in the GDPR is an accountability-based mechanism is supported by its voluntary nature.[23]

3.2 Certification of compliance with GDPR provisions

As the GDPR provides in Art. 42 (4), a certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation, meaning that compliance with the GDPR is not possible to be certified. What can be certified, is compliance with (or else: conformity to) certification criteria that are derived from the GDPR. Compliance with such criteria entails that a controller or processor at a certain period in time has taken measures to ensure that it fulfils certain obligations, for instance to secure personal data in a given processing operation.

In general, where the EU legislature, intends to assign a different effect to certification or self-declaration of conformity, this is explicitly provided in the legislation. For instance, conformity with harmonised standards that are developed on the basis of the New Approach Directives, offer a presumption of conformity with the legislation and this is explicitly provided for in the relevant law. Similarly, the CE marking offers specific effects in relation to the safety of the products. This is not the case in the GDPR, which does not assign such legal effects to certifications.

3.3 Key actors: Certification bodies and Supervisory authorities

The data protection mechanisms as proposed in Art. 42 and 43 GDPR involve mainly the following actors:

- The data controller or data processor that aims to apply for certification ('applicant')
- The certification body
- The supervisory authority (data protection authority)

[21] Recital 100 GDPR.
[22] WP29 (2010), Opinion 3/2010 on the principle of accountability, WP173.
[23] Art. 42 (3) GDPR.

- The European Data Protection Board (EDPB)

The certification bodies and the supervisory authorities are key actors in the certification process. Certification may be conducted by either a certification body that fulfils the conditions of art. 43 GDPR, or by a supervisory authority. The GDPR does not determine when the process is conducted by a certification body and when by a supervisory authority. This legal gap appears to be intentional: Member States and national supervisory authorities may organise certification at a national level according to their preferred model. However, we should note the inherent risk to the possibility of cross-border recognition of the certifications that lies with the adoption of diverse models across Member States, as discussed later in section 5.

After the evaluation phase, in the case that the applicant fulfils the necessary requirements, certification is granted by the certification body or the supervisory authority. Certification is issued for three years, and may be renewed. It is important to mention that even when the certification body issues the certification, the supervisory authority has several powers, such as to withdraw the certification or order the certification body to withdraw the certification.[24]

The supervisory authorities also have the power to approve *criteria* for certification. Not every certification in the field of data protection is automatically a data protection certification mechanism as provided in the GDPR. The national supervisory authority needs to formally *approve* the certification criteria. Such approval may constitute an administrative act, with legal effects.[25]

The European Data Protection Board (EDPB) takes the role of the national supervisory authorities, as outlined above, in the case of a European Data Protection Seal. The European Data Protection Seal is a common EU-wide certification, the criteria of which, are approved not by one or more national data protection authorities, but by the European Data Protection Board.

3.4 Scope of certification under GDPR

As highlighted, not every certification in the field of data protection is automatically a data protection certification mechanism as provided in the GDPR. In fact, the GDPR appears to be quite limiting when providing the scope of processing activities where data controllers and processors can use certification as an element to show compliance. The scope is mainly limited by the following conditions:

1. Purpose of certification

According to Article 42 of GDPR, "The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors". The purpose of a data protection certification mechanism under GDPR is thus demonstrating compliance with the Regulation of processing operations by controllers and processors, which clarifies that the substantive requirements a client must fulfil must be related to the provisions of the GDPR, for example to demonstrate compliance with the provision on data security (Art. 32). If a certification mechanism involves a scope that is not in the scope of the GDPR, for example a data protection education course,

[24] Art. 42(7) GDPR.

[25] Data Protection Authorities are independent authorities of public (administrative) law. It follows therefore, that the decision of the Data Protection Authority approving or rejecting criteria for certification may be challenged before national administrative courts.

such a mechanism cannot be used to demonstrate compliance with the GDPR. Such a certification mechanism would therefore not be in the scope of Art. 42 and 43 GDPR data protection certification mechanisms. Nevertheless, such certification may exist in the free market and potentially contribute to raising the levels of data protection awareness.

2. Processing operation

The object of certification must be a processing operation. The GDPR regulates the processing of personal data, which may be conducted in the context of a product or system or a service. However, the wording of Art. 42(1) requires that a certification mechanism under GDPR must concern an activity of data processing. Such an activity may be (also an integral) part of a product, a system, or service, but the certification must be granted in relation to the processing activit(ies), and not to the product, system or service as such (e. g. certification of data deletion process in product X).

3. Controllers or processors

The reference to "by controllers or processors" limits the scope of applicants that can opt for certification under the GDPR to controllers and processors. Producers or manufacturers of products, systems and services, if they do not process any personal data, as controllers or processors, are not in the scope of the GDPR certification mechanisms.[26]

Nevertheless, there might be certifications in the market, aimed at manufacturers (e.g. OS providers and mobile device manufacturers), in relation to data protection-friendly configuration of products or systems, which will undoubtedly contribute to raise the level of data protection. However, they will be outside of the scope of the GDPR data protection certification mechanisms of Art. 42 and 43 GDPR

3.5 Accreditation of certification bodies

A substantial part of the GDPR provisions on certification refers to accreditation. The legislature emphasises the importance of having reliable, competent, and independent bodies carrying out the certification by devoting Art. 43 GDPR to certification bodies. Art. 43 GDPR requires the certification bodies that provide data protection certifications to be accredited. The GDPR allows the Member States to select the accreditation model they will follow, from a selection of three options:

a. accreditation by a Data Protection Authority (or the European Data Protection Board, in the case of the European Data Protection Seal)[27],
b. accreditation by the National Accreditation Body on the basis of the Accreditation Regulation and the ISO/IEC 17065:2012 standard and additional requirements in the field of data protection provided by the Data Protection Authority, or
c. both authorities, namely the National Accreditation Body and the competent Data Protection Authority, collaborating in this task.

[26] The provision of Art 42(7) GDPR reiterates the position: "Certification shall be issued to a controller or processor for a maximum period (..)"
[27] Art. 70 (1) (o) GDPR.

4. Existing data protection-related certification schemes

In this section, the existing certification landscape in the EU and outside the EU is reviewed, with the aim of drawing experience already available in the market. Previous research has identified and analysed several certifications, which have in a broad sense a focus on privacy, data protection and data security.[28] The findings suggested that only a small number of EU schemes can be said to relate to the Data Protection Directive 95/46/EC or the GDPR. Transparency of the certification process, criteria, and assessment methodology has also been identified as a problematic area.[29]

4.1 Parameters of analysis

To further build on that foundation, the present study focuses on a limited number of existing certifications that have been identified as the most relevant for discussion in relation to the GDPR provisions, due to i) their focus on privacy and data protection, ii) requirements based on the EU data protection legislation or relevant international standards, iii) organisational structure and iv) maturity in the market. Selected existing certification schemes are presented, analysed according to a number of key parameters, mainly corresponding to open issues, challenges and opportunities of certification under the GDPR.

The analysis does not aim to be exhaustive, but to provide a grasp of the current landscape and offer insights for the GDPR certification. The parameters are summarized below:

- **Subject matter and scope of certification** is concerned with how existing schemes define their scope and identify what can be certified according to their requirements – whether it is only the data processing activities that can be certified or the entire products, services or systems. The aim of certification is also of interest in this regard.
- **Normative basis**. This parameter refers to the normative basis of the analysed certifications. Subsequently, it is important to identify how the criteria are formulated and to what extent the certifications offer assurance of compliance with the GDPR or assure that a controller or a processor "has measures in place to comply with legislation/standard.
- **Certification process** of the analysed certifications is examined, including the roles of involved stakeholders, the role of the certification body in terms of its independence, the stages of the certification process, how information is exchanged, the measures that need to be implemented by the applicant, how the certificate is granted and under which conditions. The GDPR does not instruct specifically on the process of certification, hence the aim of analysis is to identify the stages of the certification processes.
- **Duration of the certification process**, post-certification surveillance of issued certifications, validity period of certification are described, where available, in search of current practices that could inform future decisions regarding these topics, that are not generally specifically provided for by the GDPR (except for the length of validity of the certificate).
- **Accreditation of the certification bodies**. The GDPR requires that only certification bodies that are accredited may grant certifications, and provides for several options of accreditation, either by the

[28] Rodrigues R. et. al, 2013 , ENISA, 2013
[29] Rodrigues R. et. al, 2013

DPA or the national Accreditation body.[30] Hence it is important to look at the existing certification landscape from this aspect.[31]

Bellow the results of the analysis are presented in relation to the above identified criteria. The analysed certifications are the following:

- ePrivacyseal EU
- EuroPrise
- CNIL Labels
- ICO Privacy Seal (under development)
- Certification based ON ISO/IEC 27001
- Certification based on ISO/IEC 27018
- PrivacyMark system
- Privacy by Design by Ryerson University and Deloitte Canada

4.2 Subject matter and scope of certifications

The analysis of the scope and subject matter of the existing certifications revealed variations in the existing practices. Several certifications target products and services, others processes, and others management systems. Certifications based on the management standards, such as the ISO/IEC 27001 may target a single business process (e.g. in human resources), a particular service or the whole business process of an organization. Similarly, the Privacy Mark System (from Japan) focuses on the assessment of a Personal Information Protection Management System (PMS). The aim of the assessment is to determine whether the applicant organization manages adequately risks on handling personal information. There are also certifications such as EuroPrise, which focus on the processing operations performed within a service or by a product. Within the scope of the EuroPrise certification are IT products such as hardware and software, IT based services and automated processing of data.

The CNIL privacy seals offer a variety of scopes, which range from governance, products (digital safe boxes), procedures (audit procedures covering the processing of personal data) to courses (data protection training courses). Regarding services that are provided by more than one service providers, CNIL provides a "joint privacy seal".[32] The certifications based on the ISO/IEC 27018 standard target processes that relate to the processing of Personally Identifiable Information (PII) for providers of public cloud services.

Certifications targeting governance aspects and the management systems are different from certifications targeting processing (processing as such or processing as part of a service or a product). Certifications on management and governance issues are more "process-oriented" than "goal-oriented". The auditor in the ISO/IEC 27001 certification will ask the applicant whether for instance a Data Retention Policy is in place. On the other hand, a "goal-oriented" certification is not focusing primarily on the measures taken, but whether the measures are sufficient to fulfil certain pre-determined goals. The "goal-oriented" certification therefore focuses more on qualitative elements. To return to the previous example, the

[30] See section on '**Error! Reference source not found.**'

[31] In the Annex of the Report there is an additional parameter is considered on Resources needed to obtain certification, in terms of fees as well as organisational resources. The GDPR points to the usefulness of certification schemes for smaller organizations and companies, hence it will be considered whether a lightweight version of the scheme already exists among the analysed certifications. The number of issued certificates, where available, is included in the overview.

[32] https://www.cnil.fr/fr/node/682

auditor would not only examine whether there is a Data Retention Policy in place, but also whether the Policy addresses issues that need to be covered by such a policy in the specific organization etc. Such different approaches have an impact on the effort and the resources the applicant needs to invest, but also the level of assurance they offer. The data protection mechanisms of Art. 42 and 43 can be characterised as goal-oriented certifications, as the focus should not be only on whether measures are in place, but also to what extent such measures are sufficient.

4.3 Normative basis and compliance with the legislation

The analysed certifications are based on either the legislation or the technical standards. The ePrivacyseal derives its criteria from what it refers to as "applicable EU Data Protection Directives" and the GDPR. Additionally, there is a set of criteria related to Online Behavioural Advertising. The criteria refer to grounds for processing, data protection principles, and subjects' rights. EuroPrise certification is based on the Directive 95/46/EC (and the GDPR) and the ePrivacy Directive.[33] The PrivacyMark is based on a Japanese standard, the requirements of which relate to personal information protection policy, specification of personal information, relevant legislation, implementation and operation, documentation, complaints mechanisms, inspections, and preventive actions.

The Privacy by Design certification is neither based on legislation nor a technical standard, but the Framework of 7 Foundational Principles for Privacy by Design.[34]

On the topic of the assurance in relation to compliance with the legislation, there can be three main approaches that are listed below.

4.3.1 Certifications that are independent from legislation

Such are the certifications based on the ISO/IEC standards or other normative documents, such as the Privacy by Design Principles framework. The Privacy by Design certification provided by Ryerson University and Deloitte Canada does not signify compliance with the Ontario privacy laws. The ISO/IEC 27018 standard for instance states that it "establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment"[35] These certifications also do not use legislation as the normative source, but instead use other technical standards. They may take into account existing legislation, in the sense for instance that the requirements in the standard may not contradict the legal obligations. However, no direct references to the law are made.

4.3.2 Certifications that use the legislation as a source for their substantive criteria

The ePrivacyseal EU claims that it attests a product's "compliance with the list of ePrivacyseal EU criteria, which reflects the requirements imposed by EU data protection legislation."[36] In that sense, such certifications do not directly promise to offer compliance with the data protection legislation. They use

[33] Directive 2002/58/EC, amended in 2009.
[34] By Ann Cavoukian https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf
[35] 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", section 1 ("Scope")
[36] ePrivacyseal EU website: https://www.eprivacy.eu/en/privacy-seals/eprivacyseal/

however the legislation as their normative framework. The criteria for each certification reviewed are provided as part of Annex A.

4.3.3 Certifications that provide assurance of compliance with the legislation

An example is the CNIL case. The aim of the CNIL privacy seals is to provide a recognition from the French Data Protection Authority to the applicant that its product, course, procedure "corresponds to the requirements of the Data Protection Authority" ("confidence indicator").[37] Another example in this stream is EuroPrise.[38]

It should be noted that attestation provided by a data protection authority, should not be misinterpreted as assurance of compliance with the legislation, provided by the authority, in its supervisory role. In view of avoiding such implications, the CNIL provides a clarification that the CNIL Privacy Seals do not aim to exempt its holders from administrative fines.[39] A different approach was proposed by ICO. ICO announced in 2015 its plans to introduce a national privacy seal. The aim was to deliver a stamp that an organization "demonstrates good practice and high data protection compliance standards." What was interesting about the announced ICO privacy seals, is that the seal would not only demonstrate compliance with the requirements of the UK Data Protection Act, but would also show that the certified organization surpasses the legal requirements and went "above and beyond the call of duty".[40]

4.4 Certification process

The certification processes of the analysed certifications follow similar, but not identical approaches. The models usually include:

1. a stage of application and first assessment of the application,
2. evaluation by expert auditors/assessors which leads to an evaluation report,
3. the decision (by person(s) other than the auditor(s)),
4. granting of certification and
5. possibility for re-certification

The exact models and expertise of the certification procedures provide useful examples and good practices. EuroPrise collaborates with legal and technical experts, which are admitted as experts by EuroPrise.[41] The EuroPrise experts evaluate the product or service and report their findings in an evaluation report. The Certification Authority (EuroPrise) checks the evaluation report with respect to completeness, plausibility, and comparability with other certifications. It then drafts an internal certification report, awards the seal, and publishes a short report. The CNIL employs a Labelling Committee, at the evaluation stage, which performs the legal analysis, develops recommendations and plans for corrective actions. The decision is made by the Data Protection Authority in its plenary meeting. The granting of the CNIL Privacy Seal is published on the website of CNIL and the Official Journal (Legifrance). The ePrivacyseal includes a workshop in a preparatory stage before the actual evaluation.

---

[37] https://www.cnil.fr/fr/node/682

[38] EuroPrise website for instance provides: "We certify the privacy compliance of IT products and IT-based services with European data protection regulations" https://www.european-privacy-seal.eu/EPS-en/About-EuroPriSe

[39] CNIL provides: "The privacy seal informs the public that the procedure or product proposed corresponds to the requirements of the Data Protection Authority. In this, it plays the role of a confidence indicator. It does not aim to exempt its holders from administrative formalities." https://www.cnil.fr/fr/questions-reponses-sur-les-labels-cnil

[40] See ICO blog 28 January 2015 https://iconewsblog.org.uk/2015/01/28/what-you-need-to-know-about-ico-privacy-seals/

[41] See website of EuroPrise: https://www.european-privacy-seal.eu/EPS-en/Expert-admission

During the workshop, legal and technical experts examine the product or service based on the relevant technical, organizational, and legal requirements.

The Privacy by Design certification has its evaluation and decision phases performed by different organisations. Deloitte is responsible for scrutinizing the product or service and issuing a report, while the Privacy by Design Centre of Excellence of the Ryerson University issues a decision on granting the certification. This is a best practice as it provides guarantees for independence of the actors involved in each stage. The well-established Privacymark system collaborates with over one thousand assessors, assessment and training bodies. The assessment of conformity with the standard has two stages, namely the assessment of the documentation and on-site assessment.

The duration of the certification process is usually not specified. This shortcoming may be attributed to the diversity of the applications, the size of the organisations, ranging from large industry with complex systems to SMEs, and varying risk in the operations and systems of the applicants.

With regard to the possibilities of an applicant to challenge the decision of the certification body or authority to grant the certification, there should be a distinction between internal dispute resolution mechanisms and judicial review. EuroPrise for instance has a dispute resolution mechanism in place.[42] CNIL on the other hand, does not have such processes in place. However, this does not mean that a rejection decision by CNIL cannot be challenged. The decisions of supervisory authorities are subject to administrative law judicial review but for specific grounds, foreseen in national administrative law. The decision of CNIL to reject an application for certification may therefore be appealed to the Conseil d'Etat within two months from the publication of the decision.[43] This situation is different than the certifications issued by private organisations. Such organisations might have a dispute resolution mechanism, as mentioned above, but their decisions can be subject to judicial review by civil law courts (in civil law juridictions), instead of administrative courts. The legal grounds may potentially be derived from contract law, due process issues, and competition law issues.

4.5 Post-certification stage and monitoring of granted certifications

With regard to the post-certification stage, the analysed certifications follow different practices. In most of the cases, there is a follow-up after granting the certification. CNIL reserves the right to perform checks at any time and by any means that the certified product or procedure complies with the conditions of certification. If such conditions are no longer met, CNIL may withdraw the granted privacy seal (and certification). A different model is followed by the Ryerson Privacy by Design certification. The certification is valid for three years, but each organization needs to renew on an annual basis the certification. The renewal requires an attestation from the organization that there has not been any change affecting the granted certification and the payment of a renewal fee. Certifications based on ISO/IEC standards may include a post-certification surveillance stage, when following the ISO/IEC conformity assessment standards. According to the ISO/IEC 17065 standard, surveillance[44] is necessary for continuing use of a certification mark which is authorized for placement on a certified product, process or service.

4.6 Accreditation

The analysed certifications do not follow common approaches. The ICO seal, which is under development, follows an approach close to the GDPR accreditation model: the certification body that will be granting the

[42] https://www.european-privacy-seal.eu/EPS-en/Dispute-Resolution
[43] https://www.cnil.fr/en/all-you-should-know-about-privacy-seals
[44] "Surveillance" is defined as "systematic iteration of conformity assessment activities as a basis for maintaining the validity of the statement of conformity" ISO/IEC 17000 standard.

ICO Privacy Seal has to be accredited by the National Accreditation Body (UKAS[45]) and meet additional criteria established by the Data Protection Authority. CNIL, grants the seals and has not outsourced this activity. CNIL is not accredited. The PrivacyMark system, EuroPrise and ePrivacy are not using accredited certification bodies by the National Accreditation Bodies. Instead, they have a system of training or accepting trained experts and auditors. The certifications based on the ISO/IEC standards on the other hand are often granted by accredited National Certification Bodies.

[45]See website of the UK National Accreditation Body www.ukas.com

5. Data Protection Certification: Challenges and open questions

The following section focuses on several challenges that data protection certification under GDPR is likely to face. Some challenges stem from the GDPR provisions itself, which are only to some extent in harmony with existing (more mature) frameworks in certification and accreditation in other fields, close to the field of data protection (cybersecurity, eIDAS Regulation, etc.), while others are a consequence of (national and international) diversity of the privacy and data protection certifications, that already exist in the market.

5.1 Terminology

The meaning of some terms used in GDPR is unclear, among them the term "criteria". In the certification context in other sectors the term "requirement" is regularly used to signify the specific levels of service or contents that have to be fulfilled by an applicant, whereas the term "criteria" is not defined unitedly. In some certifications, as highlighted in Chapter 2, the term *criteria* is used to signify substantive requirements. The same goes for certification mechanisms/seals/mark, which the GDPR uses collectively, without differentiating among the legal concepts.

It is important to note, that although certification has not been formally recognized by legislation in the data protection field before GDPR, certification as a process is already operational in other areas and sectors – such as security, safety, etc. It is thus important not to reinvent the vocabulary for certification in data protection that would differ from other areas in general terms, to avoid confusion on the part of actors already providing certification or actors taking part in standard setting community that might be also involved in data protection certification and standard setting. The same argument is applicable to procedures normally known and respected in certification landscape, to which data protection certification would preferably align.

5.2 Subject matter of certification: processing operations

One significant issue relates to the aim and scope of the data protection certifications in line with Art. 42 and 43 GDPR. Approved certifications are mentioned in several provisions such as the data security (Art. 32) and data protection by design and by default (Art. 25). The ISO/IEC conformity assessment standards commonly refer to certification of products, services, process and persons.[46] There are schemes available on the market, already offering certification in such cases,[47] especially in relation to products and systems that are intertwined with data processing operations, such as different software used for data processing or hardware and appliances that are essentially used for data processing activities. However, the wording of GDPR, as shown in the Annex, is limiting in this regard as it only recognizes certification of processing operations and not products or services as such. Additionally, it aims at controllers or processors who might use the products or services designed for their data processing, and not the manufacturers or produces of these products and services. Any data processing operation needs to be put in context to be able to assess the data controllers' or processor's compliance with data protection rules (e. g. an online booking system used in healthcare, processing sensitive data has different implications for the user than if the same booking system was used in marketing, not processing sensitive data). Nonetheless, certification of products and services, which enable compliant data processing operations of data controllers and processors, may contribute to raising awareness and offering transparency on the activities of the controller/processor, or the qualities of a product.

[46] ISO/IEC 17065:2012, ISO/IEC 17021-1:2015, ISO/IEC 17024:2012
[47] See Annex of the Report

5.3 Diversity in accreditation models

The GDPR leaves room for manoeuvre for the Member States to decide the accreditation model. The challenges are linked to the resources the DPAs possess in relation to accreditation following ISO/IEC 17065:2012, if the Data Protection Authorities are to be accrediting by themselves, as well as the resources and knowledge of accreditation bodies in additional data protection criteria. In practice cooperation between the two authorities seems a viable solution, however procedures of cooperation need to be specified and the additional data protection criteria harmonized across EU Member States.

5.4 Approval of criteria for certification by Data Protection Authorities and/or EDPB

The GDPR provides that the DPAs and/or the EDPB have the authority to approve criteria for certification. However, the GDPR does not provide further guidance on benchmarks for the approval of the criteria by the data protection authorities. Consistency is of utmost importance to ensure same level of quality of the different data protection certifications.

It is important to arrive at common interpretations regarding approval of certification criteria that are based on conformity against widely recognized international standards, such as the ISO standards. It is important to clearly set the roles of EDPB and national DPAs in this regard and also to recognize the importance of such international standards and their integration in the certification under GDPR. The role of the Commission in regulating with implementing acts should also be taken into account. It needs to be clarified who should seek approval of criteria.

5.5 EU level vs. national certifications: risks of proliferation of national certifications

As recognized by the GDPR and in other fields of certification, such as security,[48] harmonization of approaches to certification across the EU is a goal to be pursued, due to challenges, posed by proliferation of nationally focused certifications[49]. Complex issues of mutual recognition arise in case of different national approaches, in addition to transparency issues and, especially from the consumer side, lack of recognition and trust in a potentially large number of seals offering different kinds and levels of protection of their personal data, in the context of the single market. The GDPR specifically instructs the Member States, Data protection authorities, the EDPB and the Commission to encourage, *in particular at Union level,* the establishment of data protection certification mechanisms and of data protection seals and marks. However, keeping the focus on harmonized approaches that could be valid throughout the EU Member States will most likely be challenging; currently many certifications exist in Member States[50], as shown in section 2, most of them not being harmonized neither in terms of procedures nor requirements. The emergence or recognition of certifications at the EU level will therefore need strong initiative from the EDPB and/or the European Commission.

On the downside of single EU wide certification approaches, endorsed or developed by authorities, market initiatives in development of very specialized certifications for specific, or even niche processing

---

[48] Wurster S, et al. *Consolidated report on security standards, certification and accreditation – best practice and lessons learnt: Deliverable 2.2 for the CRISP project*. CRISP project, 2015

[49] As recognized also in the Discussion paper of Centre for Information Policy Leadership, on the role of certification mechanisms under GDPR, highlighting the value propositions of the industry, data controllers and processors, available at: https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2017/04/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf

[50] In Germany alone more than 40 certifications in the data protection field exist; and updated list from February 2017 is available at: https://stiftungdatenschutz.org/fileadmin/Redaktion/PDF/Zertifizierungsuebersicht/SDS-Zertifizierungsuebersicht_02_2017.pdf.

operations, may hamper the development of specific certifications targeting niche sectors. Mutual recognition of such certifications across the EU should be an impetus in such cases.

Under the GDPR, the DPAs and the EDPB both have the task to approve certification criteria, submitted to them by providers of data protection certification mechanisms, which may result in conflicting decisions. That may be in the case of cross border providers of certifications, which might have gained approval of their criteria in one Member State, but have been confronted with a negative decision by the EDPB or another Member State. To ensure legal certainty these procedures will have to be streamlined and mutual recognition issues considered also in the relation DPAs – EDPB.

Since many different forms of certifications under the GDPR may coexist, namely national, EU wide, offered by public and private bodies, there is a risk of confusion on the market, and hence low trust in the seals.[51] The GDPR provides in Art. 42(8) that the EDPB shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means. It is not clear however whether this only refers to the certification mechanisms approved by the EDPB (with EU wide notion) or also to the national approved certification mechanisms. Since under GDPR DPAs will have to be informed about each issued or withdrawn certification, it would be beneficial, in terms of transparency, trust, and mutual recognition issues, that the above register maintained by the EDPB would include all approved certification mechanisms, either national or EU recognized.

5.6 Cross-border recognition of national certifications

The existence and prioritization of an open EU single market and the fact that many services (especially on the internet) are cross border in nature, raises many important challenges of mutual recognition of the certifications under the GDPR. For certification to be an efficient tool in aiding compliance with data protection rules, it needs, among other conditions, to be recognized as beneficial by data controllers and processors. The benefits may include showing accountability and demonstrating compliance, as well as the effect of certification on graduation of sanctions and corporate liability [52].

a. Cross-border recognition of national certifications

Mutual recognition of certifications issued by authorities or certification bodies in different Member States and possibly also by the EDPB is one of the crucial questions of added value of a certification to a data controller or processor operating cross border. The challenges for mutual recognition of certifications are linked to the:

- Lack of harmonization of procedures and requirements in existing data protection certification landscape which is likely to continue, as the GDPR allows many different forms of certification formats to (co)exist. This might be beneficial in terms of considering specific interests of sectors at the level of Member States, however for cross border service providers lack of harmonization of requirements and procedures is a direct obstacle in the motivation to invest in acquiring different certifications in different Member States that are not mutually recognized.
- Additionally, there will be challenges for DPAs, being faced with certifications data controllers and processors have acquired in other Member States.

[51] This can to some extent be observed from the US experience with seals where it is hard for an individual to assess which certifications indeed have value in good protection of privacy (Rodrigues R. 2013)
[52] Tomšič A, Burnik J, et al. *Consolidated report on enhancing confidence and acceptability of new certification measures. Deliverable D7.1 for the CRISP project.* CRISP project, 2017. 19 p.

DPAs also have the authority to approve certification criteria. However, their procedures of approval are likely to differ, which also means the results of their approval might differ in different Member States, from, for example, a certification body, operating cross border, seeking approval of its certification criteria.

b. Recognition of certifications from outside the EU and certifications against international standards

Many data protection certification schemes currently exist outside the EU, and it is to be expected that the issuers will either seek formal approval of their certification criteria from EU DPAs or that data controllers from outside the EU that are conducting business in the EU will be looking for assurances based on their certification acquired outside the EU. In such cases the same arguments of mutual recognition and harmonization of such possible recognitions can be applied as above. It would be beneficial if decisions of EU bodies regarding such foreign certifications were aligned and that they have the resources to be able to arrive at such non-conflicting decisions (procedural guidelines, ways of informing each other, of cooperating in procedures of recognitions and possible approvals).

5.7 Function creep of DPAs when acting as certification body/body approving criteria, and supervisory authority

The GDPR allows different models of certification processes to (co)exist across Member States, also in terms of the body issuing certification. Although there are many benefits of certification relevant for the DPAs acting in their capacity as supervisory authorities (such as endorsement of compliance by soft approaches, facilitation of inspection supervisions in cases where certification documentation is a trustworthy demonstration of data controllers' accountability and compliance), there are also challenges to be avoided in case the DPAs opt for such a dual role. If the supervisory body both assesses conformity of the applicant against requirements based on the GDPR and issues certification, while at the same being entrusted with the power of supervision over the same processing operations of the data controller or processor, challenges related to a conflict of interest arise. Even more so, if certification is provided for a fee and the DPA is the beneficiary of the revenues from certification. If such a dual role is assumed by the DPA, measures need to be put in place to mitigate risks of potential function creep. As all available models come with specific challenges and advantages, depending also on the specificities of each Member State, there cannot be, at least for now, a most or least preferable model.

6. Recommendations

The last part of this report outlines recommendations for development of the European data protection certification under GDPR that would contribute to compliance and fulfil the aims of transparency and accountability. The recommendations are relevant for the European Commision, the European Data Protection Board (EDPB) and the supervisory authorities who are in position to develop common and harmonized understanding of GDPR data protection certification mechanisms and provide further guidelines and clarifications where open questions and challenges arise, as well as to the organizations who are interested in issuing certifications or seeking certifications.

6.1 Common approach on GDPR data protection certification mechanisms

Due to the issues related to (non-existent) certification terminology in the text of the GDPR, but also issues that might arise from the adoption of diverse accreditation models and certification processes, it is crucial that the national supervisory authorities adopt a common approach. Such common approach and understanding should be extended to all relevant issues of scope, aim, and criteria of the data protection certification mechanisms under GDPR. This novel endeavour of certification stemming from secondary data protection legislation should learn from examples in other fields, where such certifications are already operational, but also successful existing certifications. Such an exercise based on existing knowledge can function as a useful basis for the development of certifications in the field, to the extent permitted by the conditions and requirements of the GDPR.

A common approach should also be adopted in relation to the criteria that are being approved by DPAs and EDPB, most importantly regarding their level of detail and whether they are assessed directly against GDPR or against a more developed list of broader criteria, developed on the basis of GDPR[53]. It is important to deploy an aligned approach on whether the criteria only relate to the substantive requirements based on GDPR or also to procedural requirements of a certification mechanism (or scheme), such as the surveillance periods, the condition for granting the seal, etc.

The data subjects need to know whether a certification mechanism is approved in line with Art. 42 and 43 GPDR. For the certifications which are out of the scope of the GDPR certification provisions, any added value to the contribution of raising awareness on data protection overall should be highlighted.

There should be procedures in place to aid data controllers and DPAs in cases that certifications issued in one EU Member State are used in another Member State. Mechanisms to help could relate to provision of information and documentation, but also mutual recognition. An example is a common register of all issued/withdrawn certification mechanisms, and if possible certifications as well, in all EU Member States and development of guidelines as to the procedures that should be followed in mutual recognition procedures.

National certification bodies and supervisory authorities (DPAs), under the guidance and support of the European Commission and the European Data Protection Board (EDPB), should pursue a common approach on inception and deployment of GDPR data protection certification mechanisms.

[53] Such broad criteria and more specific requirements, developed on the basis of GDPR, are specified in a CEN Workshop Agreement no. 17147:2017 , stemming form the foundations of EU co-funded project CRISP. Available: https://www.nen.nl/NEN-Shop/Norm/CWA-171472017-en.htm

6.2 Guidance regarding open questions to ensure consistency

As the report highlights, there are several open questions, where guidance would be beneficial. Further guidance is also in the interest of harmonization and with the look to future developments in the area of privacy and data protection. The following topics would benefit from further guidance:

1) The procedures for mutual recognition of national certifications by the Data Protection Authorities
2) Compatibility of certifications based on international standards (such as ISO/IEC) and non-EU certifications with GDPR
3) With regard to the Register with issued certifications to be kept by the EDBP:
   a) Does it refer only to EDPB approved certification mechanisms, or to nationally approve as well?
   b) Is it open to public?
   c) Does it refer to certification mechanisms alone or to all issued certifications?
4) Accreditation models and procedures to avoid conflict of interests and ensure consistency with Regulation 765/2008.
5) In relation to the criteria for certification, approved by DPAs and EDPB, guidance is necessary on:
   a) What are the procedures for approval and how consistency can be ensured?
   b) Are the criteria approved directly against GDPR provisions or against a list of broader criteria specifying the GDPR provisions that may be developed by the authorities?
6) Common guidelines should be developed on the procedures that the DPA, as well as the EDBP, are to follow in approval of certification criteria in order to achieve harmonization and avoid mutual recognition issues.
7) Post-certification surveillance measures.
8) Transparency thresholds and complaints mechanisms.

National certification bodies and supervisory authorities (DPAs), with the support of the European Data Protection Board (EDPB) and the European Commission, should provide guidance and promote best practises to ensure consistency and harmonization in the deployment of GDPR data protection certification mechanisms.

6.3 Safeguards to avoid function creep

The GDPR allows for different models of engagement of Data Protection Authorities in the processes of accreditation and certification. In order to avoid function creep. It is recommended that a Data Protection Authority does not function as the sole accreditation and certification body.

Additionally, in the case that a Data Protection Authority performs all the stages of certification, without the involvement of a certification body, safeguards for mitigation of the risk of conflict of interest with its supervisory capacity, should be put in place. Such measures may include separation of the staff conducting certification from the staff conducting supervisory activities, resolution of the issue of monetary compensation to the supervisory authority.

The European Commission and the European Data Protection Board (EDPB) should stimulate the establishment of safeguards that will ensure trustworthiness of the certification process.

6.4 Approval of high-quality and transparent certifications with sufficient guarantees

As diverse certifications already exist on the market it is to be expected that this trend is likely to continue. In this regard promotion of quality schemes is recommended in order not allow for the market to be flooded with untrustworthy certifications. Simplicity, openness and transparency[54] are among the most important signs of quality of a certification mechanism that should include:

- Transparent procedures and transparency regarding scheme fees
- Publicly accessible summary reports on certifications, and
- Publicity of criteria, requirements and methods for evaluation.
- On spot audits in combination to documentation reviews
- Regular post-certification surveillance and updates of certifications, when necessary
- Transparent complaints mechanism
- Auditors' competences.

The European Commission and the European Data Protection Board (EDPB) should stimulate the establishment of safeguards that will ensure transparency of the certification process.

6.5 Promotion of an EU approach

As recognized in other fields of certification, such as security,[55] harmonization of approaches to certification across the EU is a goal to be pursued, due to challenges, posed by proliferation of nationally focused certifications in relation to market recognition, trust, economic factors and (legal) uncertainty. The EDPD has the mandate to approve EU wide criteria, that lead to the European Data Protection Seal.

6.6 Scaling for SMEs

As provided by the GDPR, development of certification mechanisms should be encouraged, keeping in mind specific needs of small, medium and micro enterprises (SMEs). There are many enterprises falling in that category. At the same time, SMEs may be processing large quantities of personal data, which may pose significant risks to individuals (for instance in the market of m-Health apps). As certification may be a lengthy and costly process SMEs are unlikely to be motivated to undertake certification due to their resource limitations. However, SMEs with low risk processing operations may benefit from using the published approved criteria to assess their level of conformity. Such self-assessment would not lead to certification or issuance of a seal, since it does not fulfil the conditions of Art. 42 and 43 GDPR.

---

[54] Golyardi S, Hortensius D, Lau YY, Burnik J et al. *Final Consolidated Exploitation Plan: Deliverable 7.4 for the CRISP project.* CRISP project, 2017. 12-15 p. p.

[55] Wurster S, Pohlmann T, Kamara I, De Hert P, Hirrschman N, Murphy P et al. *Consolidated report on security standards, certification and accreditation – best practice and lessons learnt: Deliverable 2.2 for the CRISP project.* CRISP project, 2015. 539 p.

Nevertheless, it may still have an added value for the SMEs themselves and their demonstration of compliance (with self-made documentation) to the supervisory authorities.

The European Data Protection Board (EDPB), in close cooperation with national certification bodies and supervisory authorities (DPAs), should promote an EU scalable approach with approved and widely accepted criteria.

6.7 Exchange best practices and lessons learnt with certification practises in other domains

Data protection certification mechanisms, seals or marks under GDPR have specificities that do not allow for a direct analogy with existing successful certification practises and approaches in other domains, such as ICT security. GDPR provisions require that a certification mechanism must concern an activity of data processing. Such activity may be (also an integral) part of a product, a system, or service, but the certification must be granted in relation to the processing activit(ies), and not to the product, system or service as such, which is not the case in the aforementioned example of ICT security certification. Nevertheless, the experience accumulated and the best practises already implemented in other domains could support European Commission, EDPB and national certification and supervisory authorities on further laying out and implementing certification mechanisms under GDPR. Such experience[56] can pertain identification and analysis of relevant market needs and trends to better match demand and supply, mutual recognition procedures, identification of standardisation gaps and coordination of standardisation activities at EU level.

The European Commission and the European Data Protection Board (EDPB), in close cooperation with national certification bodies and supervisory authorities (DPAs), should stimulate the exchange of best practises and lessons learnt from certification practices in other well established domains (e.g. cybersecurity).

[56] See for example relevant ENISA's work in this field: https://www.enisa.europa.eu/topics/standards/certification

7. Bibliography

- Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, WP 173, 13.07.2010
- Cavoukian, A, *Privacy by design: The 7 foundational principles. Implementation and mapping of fair information practices*. Information and Privacy Commissioner of Ontario, Canada, 2009
- CEN Workshop Agreement* on "Guidelines for the evaluation of installed security systems, based on the STEFi dimensions" (CWA 17147:2017).
- Centre for Information Policy Leadership. Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms, April 2017. Available at: https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2017/04/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf (last accessed 30. 10. 2017)
- De Hert, P., Papakonstantinou, E., & Kamara, I. (2016). The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection. Computer Law & Security Review, 32(1), 16-30
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) L 201 , 31.07.2002
- Directive 2004/49/EC of the European Parliament and of the Council of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railway undertakings and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification (Railway Safety Directive) L 164/44 30.4.2004
- Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, L 337/11 18.12.2009
- European Commission, Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM(2016) 410 final, 5 July 2016
- European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, 10.01.2017
- ENISA "Security certification practice in the EU", October 2013.
- Fuster Gonzalez G. *The emergence of personal data protection as a fundamental right of the EU*. Springer Science & Business, 2014
- Golyardi S, Hortensius D, Lau YY, Burnik J et al. Final Consolidated Exploitation Plan: Deliverable 7.4 for the CRISP project. CRISP project, 2017.
- Gutwirth S, Hert P. *Regulating profiling in a democratic constitutional state. Profiling the European citizen*. 2008:271-302.

- ISO/IEC 17000:2004 Preview Conformity assessment - Vocabulary and general principles
- ISO/IEC 17067:2013 Preview Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes
- 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
- Kamara I., De Hert P. *Data protection certification in the EU: Possibilities, Actors and Building Blocks in a reformed landscape*, in Rodrigues R. and Papakonstantinou V. (eds) Privacy and Data Protection Seals, 2017 (forthcoming)
- 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), L 119/1 4.5.2016
- 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 L 257/73 28.8.2014
- Rodrigues Rowena, Barnard-Wills D., Wright David, De Hert Paul, Papakonstantinou Evangelos,. *EU Privacy seals project. Inventory and analysis of privacy certification schemes, Final Report Study Deliverable 1.4,* Publications Office of the European Union
- Tomšič A, Burnik J, et al. Consolidated report on enhancing confidence and acceptability of new certification measures. Deliverable D7.1 for the CRISP project. CRISP project, 2017.
- Wurster S, et al. *Consolidated report on security standards, certification and accreditation – best practice and lessons learnt: Deliverable 2.2 for the CRISP project*. CRISP project, 2015.

Annex A: Analysis of existing certifications overview

A.1 ePrivacyseal

ePrivacyseal	
Scope & Subject matter	The ePrivacyseal certifies products or services, that are in line with the pre-determined criteria catalogue of the ePrivacyseal scheme.[57]
Requirements & Normative basis	ePrivacyseal states that it derives the criteria from the 'European data privacy law', which they refer to as the 'applicable EU Data Protection Directives' and the EU General Data Protection Regulation. In addition, there is a set of criteria related to the 'Online Behavioral Advertising' framework. In terms of topics, the criteria cover a broad range of topics, such as the principles of processing, grounds for lawful processing, and data subjects' rights.
Certification process	The certification process of the ePrivacySeal EU involves five stages: • Definition of targets • Workshop • Optimisation • Final Evaluation • Certification Stages 1-3 are preparatory for the evaluation process ('final evaluation' stage). In the context of the workshop, technical and legal experts examine the product or service on the basis of relevant technical, organisational and legal requirements. The final evaluation stage entails testing from the auditors according to the ePrivacy criteria catalogue and recommendations for improvements. The final phase of the process is the application for seal and the licensing of the ePrivacyseal. ePrivacy provides that consulting and audit services are provided by the ePrivacy GmbH, the assignment of the privacy seal occurs through another company, the ePrivacyseal GmbH.
Accreditation of certification body	The ePrivacy GmbH does not provide that it is itself an accredited certification body by the National Accreditation Body of Germany, where the enterprise is established.
Duration of process	Not specified
Post-certification surveillance	Not specified
Validity period of certification	Two years, re-certification is possible
Resources	Information regarding the costs of the services are available in the Terms and Conditions of the ePrivacy.[58]
Issued certifications	ePrivacyseal EU has been awarded to 27 companies (until September 2017)[59].

[57] The criteria catalogue is available online. https://www.eprivacy.eu/fileadmin/Redakteur/PDF/Kriterienkataloge/ePrivacyseal_criteria_catalog_EU_july_2016.pdf

[58] General Terms and Conditions of Business, version of December 2016 https://www.eprivacy.eu/fileadmin/Redakteur/PDF/2016.12_ePrivacy_General_T_C_EN.pdf

[59] https://www.eprivacy.eu/en/customers/awarded-seals/#seal5

A.2 EuroPrise

EuroPrise	
Scope & Subject matter	The subjects of the scheme are IT products such as hardware (e.g., a hardware firewall) and software (e.g., a database application in a hospital) and IT-based services and automated processing of data (e.g., commissioned data processing, websites). Evaluation of such a service includes auditing of live performance of data processing. Evaluated is either the complete product (e.g., a piece of software) or a part of a product. EuroPrise also certifies websites and "commissioned data processing".[60] The aim of certification is increasing market transparency for privacy relevant products and an enlargement of the market for Privacy Enhancing Technologies and increase of trust in IT by certifying privacy compliance with European data protection regulations (Europrise 2017).
Requirements & Normative basis	One list of criteria based on the Directive 95/46/EC and the ePrivacy Directive, and a list of criteria based on the GDPR and the ePrivacy Directive are available on the website of EuroPrise. The criteria are formulated as questions. According to EuroPrise: " *Not each and every question will be applicable to each and every product or service. The certification authority shall ensure that in any certification procedure the relevant criteria are applied and that all related questions are answered in a plausible manner, the appropriate granularity, and at a uniform and comparable level."*[61] However, there is no information available on the assessment methodology on the applicability of such criteria.
Certification process	(1) EuroPrise experts evaluate the product or service in line with the evaluation criteria specified for intended usage, legal framework and technical environment of the product. They report their findings in an evaluation report. The evaluation criteria include: overview of fundamental issues, legitimacy of data processing, technical-organizational measures, data subject's rights. (2) Certification body checks the evaluation results The certification body checks the evaluation report with respect to completeness, plausibility and comparability with other certifications. A certification report is published. Additionally, a short public report summarizing the evaluation findings is published. (3) Award of European Privacy Seal The certification body compiles an internal certification report, awards of the seal and publishes of the short public report. The certification is granted by the EuroPrise Gmbh, the only entity issuing certificates and performing certification assessment.
Accreditation of certification body	No information available
Duration of process	Not specified
Post-certification surveillance	Not specified
Validity period of certification	Two years, re-certification is possible

[60] https://www.european-privacy-seal.eu/EPS-en/certifications-offered
[61] The criteria catalogue is available online. https://www.european-privacy-seal.eu/EPS-en/Criteria

Resources	Costs for the evaluation by the experts and fees for certification by the certification bodies. The evaluation costs are negotiated between applicant and expert. The costs for certification are set by certification body.
Issued certifications	From 2008 until September 2017: 68 Certifications (including re-certifications)

A.3 CNIL Labels

CNIL Labels	
Scope & Subject matter	The subject of certification may be any natural person or legal entity, whose procedure or product corresponds to one of the standards published by the CNIL in the Official Journal.
Requirements & Normative basis	Requirements are currently set in 4 standards: 1. Audit procedures covering the processing of personal data: The processing audit privacy seal delivered by the CNIL *does not directly apply to processing carried out*. It applies to the audit procedure which is used to check that these processes are compliant with the French data protection act. The procedure describes the various stages and processes according to which such an audit must be prepared, implemented and finalised. It also includes requirements regarding the organisation performing the audit, and the auditors themselves. It can be issued for processing audit procedures carried out by service providers (consulting firms, lawyers, etc.,) or by organisations (in this case, we speak of an internal audit). CNIL's privacy seal is delivered to legal and technical audits. 2. Data protection training courses: CNIL's privacy seal can be delivered for internal training courses to an organisation, either for training courses in the classroom or via e-learning, providing they meet the requirements of the standard. 3. Digital safe boxes: they differ from a storage space in that the data that is stored there (documents and some meta data) is only accessible to the holder of the safe box, and to any persons whom he/she may have mandated. Service-providers who carry out a digital safe box (operators) or propose one to users (suppliers) may apply for the privacy seal. The request may therefore be made jointly by the operator and its customer (the supplier). 4. Personal Data governance procedures are all measures, rules and best practices for managing an organisation's personal data. CNIL examines the compliance of the request for certification of the organisation with 25 requirements, all cumulative, in the standard relative to three topics: internal organisation of the management of personal data; the procedure for checking compliance of processing with the Act; the management of complaints and incidents (CNIL 2017). 5. A certificate is recognition by the CNIL that a product or a procedure is compliant with the provisions of the French Data Protection Act. It does not aim to exempt its holders from administrative formalities (CNIL 2017)
Certification process	The procedure consists of the following stages: 1. Application: the applicant sends its request on a form, available at the CNIL website. It must provide all elements for demonstrating that its procedure or product is compliant with the requirements of the standard. 2. Admissibility assessment: CNIL has 2 months to analyse the admissibility of an application. Failing this, it is deemed to be admissible. 3. Examination by the Privacy Seals unit of CNIL where exchanges may take place between the privacy seal division and the applicant to clarify some points in the application.

	4. Compliance assessment by the Labelling Committee: When examination by Privy Seals Unit is complete, it is presented to the certification committee, which performs Legal analysis, develops recommendations and plan of corrective actions. 5. Presentation and granting of the privacy seal: The decision to deliver a privacy seal is made by the Data Protection Authority meeting in its plenary configuration. 6. Notification and publication. The decision is sent to the applicant, accompanied by personalised logos in the name of the holder of the privacy seal, as well as the regulations for using the brand, and it is published on the CNIL's website, then on Légifrance (CNIL 2017)[62]
Accreditation of certification body	Not applicable (The seals are awarded only by the CNIL, there are no certification bodies involved)
Duration of process	Examination of the application for certification takes place in two stages: the admissibility of the application and the examination. The CNIL has 2 months to analyse the admissibility of an application. The period of examination varies. The privacy seal must be delivered within 6 months from reception of the last elements necessary to satisfying the requirements of the standard.
Post-certification surveillance	The CNIL may check at any time and by any means that the certified product or procedure complies with the conditions defined in the standard. CNIL can withdraw a privacy seal. On its Internet site, the CNIL keeps an up-to-date list of products and procedures that are certified, with the identity of their holders.
Validity period of certification	3 years, re-certification/renewal is possible
Resources	No fee is paid to CNIL for award of a seal. However, the applicant may need to devote organization resources to comply with standards and adapt its practices.
Issued certifications	CNIL has issued 91 certifications (including re-certifications) until September 2017[63]

[62] See for instance: https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000032460877&fastReqId=1830757081&fastPos=1

[63] https://www.cnil.fr/fr/labels

A.4 ICO Privacy Seal

ICO Privacy Seal (under development) *	
Scope & Subject matter	In 2015, the UK Information Commissioner announced its intention to introduce a national privacy seal, as a stamp of approval 'which demonstrates good privacy practice and high data protection compliance standards'.[64] The aim of the seal is not only to demonstrate compliance of the certified organisation with the requirements of the UK Data Protection Act, but to show that it surpasses the legal requirements 'when it comes to looking after people's information'. The ICO Privacy Seal will show that the certified organisation went 'above and beyond the call of duty'. The scheme operators (other than the ICO) will focus on different sectors, processes, products or areas of compliance.[65]
Requirements & Normative basis	Requirements from the UK Data Protection Act
Certification process	Organisations wishing to apply for an ICO privacy seal will then be able to make an application to a relevant scheme operator. Organisations will be awarded an ICO privacy seal 'if they can show that they meet the operator's assessment criteria and in doing so demonstrate that they meet the highest data protection standards'. Despite not directly involved in the process of awarding the ICO privacy seal, the data protection authority will retain powers over the overall operation of the seal, such as the power to withdraw the endorsement to a scheme operator.
Accreditation of certification body	National Accreditation Body of the UK (UKAS)[66] and will need to meet additional criteria established by the ICO.
Duration of process	Not specified
Post-certification surveillance	Not specified, only the intention of the ICO to retain powers over the overall operation of the seal.
Validity period of certification	Not specified
Resources	Not specified
Issued certifications	Not applicable (certification under development)

[64] https://ico.org.uk/for-organisations/resources-and-support/privacy-seals/
[65] https://iconewsblog.wordpress.com/2015/01/28/what-you-need-to-know-about-ico-privacy-seals/
[66] https://www.ukas.com/

A.5 Certification based on ISO/IEC 27001

Certification based on ISO/IEC 27001	
Scope & Subject matter	The object of certification can be a single business process (e.g. HR), a particular service or the whole business process of an organisation. Certified organisation is able to identify and mitigate information security risks to desired levels, improve trust into its services and manage information security processes.
Requirements & Normative basis	ISO/IEC 27001 defines the mandatory requirements for an Information Security Management System (ISMS).
Certification process	The certification process includes: 1. A two-stage initial audit, defined by the ISO/IEC 17021 and ISO/IEC 27006 standards, where: 2. Stage 1 is dedicated to the review of the documented ISMS against the standard, and 3. Stage 2 to the review of the implementation of the ISMS within the business and evidence of adherence. 4. Surveillance audits in the first and second years that are carried out in order to verify that the organisation remain compliant to the standard, 5. A recertification audit in the third year prior to expiration of certification. The certification can later be renewed for subsequent three-year periods (ENISA 2013). 6. The certificate can be revoked or suspended if the annual audit finds reasons for it. The certification body suspends certification in cases when, for example, the client's certified management system has persistently or seriously failed to meet certification requirements, including requirements for the effectiveness of the management system, the certified client does not allow surveillance or recertification audits to be conducted at the required frequencies, or the certified client has voluntarily requested a suspension (ENISA 2013).
Accreditation of certification body	ISO directs its clients to accredited certification bodies, which have acquired independent confirmation of competence by an Accreditation Body. Accredited certification bodies must be able to offer certification in conformity with ISO/IEC 17021-1 standard, which contains principles and requirements for the competence, consistency and impartiality of bodies providing audit and certification of all types of management systems and ISO/IEC 27006 standard which provides requirements for bodies providing audit and certification of information security management systems (criteria document for accreditation, peer assessment or other audit processes) (ISO 2017).
Duration of process	The length of the certification procedure as a whole depends on the scope of certification. According to a previous study the time period that was required for the surveyed companies in order to prepare for

	the certification varied between 3 and 18 months, the majority of the companies required about 6 to 12 months in order to complete the preparation. The certification process itself did not exceed a week.[67]
Post-certification surveillance	Depends on the certification body that provides the certification
Validity period of certification	3 years
Resources	Not specified
Issued certifications	A total of 27536 certificates were issued worldwide in 2015, taking into account only those awarded by accredited certification bodies (ISO 2015)

[67] ENISA 2013, p.19

A.6 Certification based on ISO/IEC 27018

Certification based on ISO/IEC 27018	
Scope & Subject matter	ISO/IEC 27018:2014 Code of Conduct establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. It specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services.
Requirements & Normative basis	Controls relate to Information security policies, organisations of information security, human resource security, asset management, access control, cryptography, physical and environmental security, operations security, communications security, system acquisition – development & maintenance, supplier relationships, information security incident management, continuity managements, compliance with legal and contractual requirements. In Annex A new controls are included, classified on the basis of the privacy principles of the ISO/IEC 29100.
Certification process	See ISO/IEC 27001 table
Accreditation of certification body	See ISO/IEC 27001 table
Duration of process	See ISO/IEC 27001 table
Post-certification surveillance	See ISO/IEC 27001 table
Validity period of certification	See ISO/IEC 27001 table
Resources	See ISO/IEC 27001 table
Issued certifications	See ISO/IEC 27001 table

A.7 PrivacyMark System

PrivacyMark System	
Scope & Subject matter	The PrivacyMark system is operated by JIPDEC, a non-for profit organisation in Japan aiming to develop and propose mechanisms and framework infrastructures to ensure safety and security, and the use of IT and digital information.[68]
Requirements & Normative basis	The PrivacyMark System is based on the JISQ15001 technical standard on Protection of Personal Information in Management Systems.[69] The requirements of the JISQ15001:2006 relate to: a. general requirements, b. personal information protection policy c. plan (specification of personal information, laws and guidelines stipulated by state, roles, responsibilities, etc.) d. implementation and operation (principles on acquisition, use and provision of personal information, appropriate controls, rights of persons) e. documentation f. complaints mechanism g. inspections h. corrective and preventive actions.[70]
Certification process	The assessment of the conformity of the applicant with the requirements of the standard has two main components: an assessment of the documentation and an on-site assessment. The aim of the overall assessment is to decide on whether the Personal Information Protection Management System (PMS) of the applicant adequately manages risks on handling personal information. The PrivacyMark System collaborates with in total 1.246 assessors, 305 of which are lead assessors. There are eighteen assessment bodies and three training bodies.
Accreditation of certification body	Not specified
Duration of process	Not specified
Post-certification surveillance	Not specified
Validity period of certification	Two years, recertification is possible
Resources	The fee structure of the PrivacyMark System accounts for the business scale of the applicant (small, medium, large) and whether the application it is a first application or renewal of the PrivacyMark.
Issued certifications	By 2017, 21.307 certifications have been granted the PrivacyMark, including recertifications

[68] https://english.jipdec.or.jp/greeting.html
[69] JISQ15001: 2006 is a Japanese Industrial Standard
[70] https://privacymark.org/reference/pdf/ThePrivacyMarkSystem.pdf

A.8 Privacy By Design Certification by Ryerson University & Deloitte Canada

Privacy By Design Certification by Ryerson University & Deloitte Canada	
Scope & Subject matter	Its stated aim is to "advance the operationalization of Privacy by Design" and to help companies and organizations who are working to embed Privacy by Design into their everyday processes.[71] The certification assesses: IT systems, "accountable business practices" and networked infrastructure.
Requirements & Normative basis	The criteria are based on the 7 foundational principles of Privacy By Design (The criteria are based on the 7 Foundational Principles of Privacy by Design: 1. Proactive not Reactive; Preventative not Remedial 2. Privacy as the Default Setting 3. Privacy Embedded into Design 4. Full Functionality – Positive-Sum, not Zero-Sum 5. End-to-End Security – Full Lifecycle Protection 6. Visibility and Transparency – Keep it Open 7. Respect for User Privacy – Keep it User-Centric The list of criteria and the relevant control activities are available online.[72] Privacy by Design Certification does not signify compliance with Ontario privacy laws.[73]
Certification process	The process starts with the application of the interested organisation. The "Privacy and Big Data Institute" reviews the application and forwards the information to Deloitte Canada to begin the assessment. The applicant makes a separate agreement with Deloitte Canada. Deloitte Deloitte "scrutinize the product(s), services(s) and/or offering(s) being certified, conduct interviews, and examine operational processes. Deloitte will then issue a report based on the assessment methodology and scorecard technique developed exclusively for Privacy by Design Certification which examines the organization's adherence to Privacy by Design".[74] Following Deloitte's report, the Privacy by Design Centre of Excellence issues a decision on granting the certification. The organisation that is granted the Privacy by Design Certification, may use the relevant seal, called "Certification Shield".

[71] http://www.ryerson.ca/pbdce/certification/
[72] http://www.ryerson.ca/content/dam/pbdce/certification/Privacy-by-Design-Certification-Program-Assessment-Methodology-20161011.pdf
[73] http://www.ryerson.ca/pbdce/certification/
[74] http://www.ryerson.ca/pbdce/certification/process/

Accreditation of certification body	Not specified
Duration of process	Not specified
Post-certification surveillance	Annual. Certifications must be renewed annually to be kept current. The renewal requires an attestation from the organisation that there has been no change affecting their certification. In addition, a renewal fee is charged.
Validity period of certification	Three years
Resources	Not specified
Issued certifications	7 certifications from 2015 until September 2017.[75]

[75] http://www.ryerson.ca/pbdce/certification/certifications-granted/

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

TP-07-17-037-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-238-7
DOI: 10.2824/787306