Comparative Law Review

2024 – Vol. 15 n. 3

ISSN:2038 - 8993

COMPARATIVE LAW REVIEW
The Comparative Law Review is a biannual journal published by the
I. A. C. L. under the auspices and the hosting of the University of Perugia Department of Law.

Office address and contact details:
Department of Law - University of Perugia
Via Pascoli, 33 - 06123 Perugia (PG) - Telephone 075.5852437
Email: complawreview@gmail.com

Comparative Law Review is registered at the Courthouse of Monza (Italy) - Nr. 1988 - May, 10th 2010.

COMPARATIVE LAW REVIEW

VOL. 15/3 - 2024

CERTIFICATIONS AND PROTECTION OF PERSONAL DATA: AN IN-DEPTH ANALYSIS OF A POWERFUL COMPLIANCE TOOL

*Paolo Guarda – Razmik Vardanian**

TABLE OF CONTENTS:

The aim of this article is to provide an analysis of the general framework for data protection and privacy certification, also from a comparative perspective. The paper begins by considering data protection certification as an effective tool for demonstrating compliance with the General Data Protection Regulation. In particular, the essay explores the requirements for the development, approval, and attribution of certification according to the GDPR. Moreover, this contribution briefly explores the main features of the certification schemes currently approved in the EU. In the second part, the article delves into the regulatory frameworks of the UK, Canada, US and PRC legal systems concerning certification in data protection and online privacy. The comparison with these experiences highlights the impact of integration with the EU and examines the nuances of each country's approach. The paper underscores the differences and similarities in their certification processes. The conclusion recaps the key remarks of the paper, emphasising the effects and advantage of data protection and privacy certifications.

Keywords: data protection – certification – accountability – GDPR – co-regulation

I. ACCOUNTABILITY AND CERTIFICATIONS

There is one concept among others that represents the true novelty of the European discipline on personal data protection as provided by Regulation (EU) 2016/679 (General Data Protection Regulation; hereinafter: GDPR)[1]: the so-called "accountability" that has assumed a pivotal role within the European approach. The evaluation of the context and the choice of solutions aimed at mitigating risks are completely up to those who carry out, and are in charge of, the data processing (i.e. the data controllers). Art. 5, par. 2, therefore, states: "*The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')*". Art. 24 relating to the responsibilities of the data controller is even more explicit in paragraph 1: "*Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary*". The importance of such recording activities - indispensable to fulfil the obligations of art. 24 - is also emphasised elsewhere in the

* Paolo Guarda (Faculty of Law - University of Trento) authored paragraphs 1 and 4; Razmik Vardanian (Law Graduate - Faculty of Law – University of Trento) authored paragraphs 2 and 3.

[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.

GDPR, and is linked to newly introduced requirements, such as the register of processing activities (art. 30), the Data Protection Impact Assessment (art. 35), etc.

Accountability finds its first operational expression in the so-called "data protection by design" approach. Art. 25, par. 1, thus requires to incorporate the principles and rules regarding the protection starting from the design phase of the processing, also and above all at the level of IT solutions. This provision is recapped and explained in Recital no. 78: the data controller is required to adopt internal policies and measures that address the principles of data protection by design and by default (e.g. minimisation of data use, pseudonymisation, greater transparency on processing, etc.). Data protection by design is connected to so-called "data protection by default", which aims at fostering the adoption of adequate technical and organisational measures to guarantee that only the personal data needed for each specific purpose of the processing are processed (art. 25, par. 2, GDPR)[2].

The attention that is paid to the data controllers and their ability to carry out a proper risk analysis taking into account a series of parameters that the Regulation itself indicates thus becomes the founding aspect of the proactive European approach. The output of this activity must correspond to the adoption of adequate measures aimed at reducing and, if possible, eliminating the risk linked to the processing of personal data.

This is the context for understanding the new (powerful) tool provided by arts. 42 and 43 GDPR: certification. Despite not yet being properly emphasised by commentators or popularised at the level of practice, certifications have the potential to become the fundamental support to the data controller for managing the security of the processing, both in the risk assessment phase and in its mitigation; it also represents a very useful and valuable documentary instrument[3].

Certifications represent a voluntary (contractual) instrument, accessible following a specific transparent procedure. Member States, supervisory authorities, the European Data Protection Board and the Commission encourage the establishment of data protection certification mechanisms as well as data protection seals and marks with the aim of demonstrating compliance with European data protection legislation. The data controller or data processor who submits the processing to the certification mechanism shall provide the certification body or competent supervisory authority with all the information and access to the processing activities necessary to carry out the certification procedure (art. 42, para. 6).

It appears evident that certifications represent important steps in the unification of the rules on the protection of personal data: they do not meet the limits of legal rules as they are not affected by individual national traditions and are identical for all Member States[4].

---

[2] See G. Bincoletto, D*ata protection by design in the e-health care sector. Theoretical and applied perspectives*, Luxembourg Legal Studies, Baden-Baden, Nomos Verlagsgesellschaft mbH & Co. KG, 2021; L. A. Bygrave, *Article 25. Data protection by design and by default*, in C. Kuner, L. A. Bygrave, C. Docksey, L. Drechsler (eds.), *The EU General Data Protection Regulation: a Commentary*, Oxford, Oxford University Press, 2020, 571-581.

[3] See G. M. Riccio, *Commento art. 42-43 GDPR*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, (eds.), *Codice della privacy e data protection*, Bologna, Giuffré, 2021, 602-615; R. Leenes, *Article 42. Certification and Art. 43. Certification bodies*, in C. Kuner, L. A. Bygrave, C. Docksey, L. Drechsler (eds.), *The EU General Data Protection Regulation: a Commentary*, Oxford, Oxford University Press, 2020, 732-754; S. Sileoni, *I codici di condotta e le funzioni di certificatore*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (eds.), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2016, 946-977.

[4] G. M. Riccio, *Commento art. 42-43 GDPR*, cit., 607.

Furthermore, in general terms, and considering market dynamics, the certifications should ensure greater reliability for consumers (i.e. users/data subjects). Associated with the use of icons, they could generate trust and transparency in data processing[5]. These are reasons why institutions at all levels should place great emphasis on creating an appropriate culture regarding these tools and their limits.

Precisely to stimulate reflection on this still unexplored but important topic, this paper aims at delving deeper into this relevant tool also from a comparative perspective by taking into account mechanisms provided in other relevant legal frameworks. The focus concerns the regulation on personal data protection, that will be our point of reference for dealing with this topic. Other aspects and possible legal issues, relevant from a general perspective, will be mentioned and taken up when needed, but not analysed in detail as they do not fall within the main scope of this paper. Following this introduction, in the second paragraph ample space will be dedicated to the rules and requirements needed for the establishment, creation, approval and assignment of certification schemes, identifying their scope of application on the basis of articles 42 and 43 GDPR. The third paragraph will be dedicated to the analysis of the certification tool in a comparative perspective. The European discipline, directly explored in paragraph 2, will be deployed as the point of reference. But the paragraph specifically aims to go beyond the EU borders to verify how certification schemes work in different legal frameworks, with a focus on the United Kingdom - especially after Brexit – Canada, the United States and the People's Republic of China. In the final remarks we will summarise the juridical-conceptual approaches to the issue.

II. Certification mechanisms in the General Data Protection Regulation

2.1 Purpose of the data protection certifications and entities involved

The GDPR certification mechanism constitutes a voluntary compliance tool that data controllers and processors may adopt for managing the security issues inherent in any data processing, allowing data subjects to quickly assess the level of data protection of relevant products and services[6]. However, the process of certification detailed by the GDPR is complex and involves multiple actors: the EU Commission, the Member State, the national supervisory authorities (SAs), the European Data Protection Board (EDPB), the national accreditation bodies in Reg. (EC) 765/2008, the Certification Bodies (CBs) and the scheme owners. The following describes only the main features of the seals and the certification process provided under articles 42 and 43 GDPR[7].

The scope of the certification is broad, encompassing all data processing activities carried out by a data controller or processor. However, it excludes additional parties, such as Data Protection Officers (DPOs) or individuals acting under the authority of the controller or

[5] See S. Grabner-Kraeuter, *The role of consumers' trust in online-shopping*, in *Journal of Business Ethics,* 2002, vol. 39, 43-60.

[6] See L. Bolognini, *Art. 42 – Certificazione*, L. Bolognini, E. Pelino, I. M. Alagna (eds.), *Codice della disciplina privacy*, Giuffré, Milano, 2019, 297.

[7] See F. Pezza, *Art. 42 – Certificazioni and Art. 43 – Organismi di certificazione*, in E. Belisario, G. M. Riccio, G. Scozza (eds.), *GDPR e Normativa Privacy*, Wolters Kluwer, Milano, 2020, 475-476.

processor, as stated in art. 29 GDPR[8]. Regarding the material scope, art. 42 states that any processing of personal data related to a product, process, or service may be certified. In particular, according to the EDPB, three basic elements should be taken into account when evaluating the processing operations: the personal data processed, the technical infrastructure or the systems used for the processing and the organisational processes and procedures related to the data processing[9]. Such guidance provides ample flexibility in identifying the scope of certifications. Specifically, the object ('target of evaluation') of a certification can be either generic (the certification scheme can be deployed for any data processing), or specific (the certification scheme is aimed at a particular category of data or at certain legal requirements).

The object of certification is also evidently reflected in the development of certification criteria. These are the technical and organisational requirements and controls with which entities seeking certification must comply in order to obtain the certification mark.

2.2 Approval of certification criteria and accreditation of Certification Bodies

According to art. 42 GDPR, the scheme owner has to obtain the approval of the certification criteria from the competent SA or the EDPB in order to make the scheme operational[10]. The Regulation does not provide additional specific methods for identifying and drafting criteria for a scheme, but the EDPB has emphasised in its guidelines that the certification criteria should reflect GDPR requirements and principles. More specifically, its document refers to the rules governing the principles of processing (arts. 5-11), risk analysis of processing (arts. 33-35), security obligations (art. 32) and the concepts of data protection by design and by default (art. 25)[11]. The development of certification criteria should therefore focus on the verifiability, relevance, and suitability of these elements, taking into account their practical application and, above all, the scope of the certification[12]. The national SA must consider all of these characteristics when approving certification criteria in accordance with art. 42, par. 5[13].

As mentioned above, the certification criteria can also be approved by the EDPB, resulting in a common certification, the European Data Protection Seal. The evaluation of the

---

[8] By reserving the certification only to data controllers and data processors (as well as sub-processors), it is reasonable to assume that data subjects - in the Digital Single Market - will increasingly choose services offered by certified data controllers. Moreover, when dealing with data processors, data controllers will look exclusively for certified ones, as they are more trustworthy thanks to the compliance system adopted. See D. Poletti, M. C. Causarano, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in E. Tosi (eds.), *Privacy digitale: riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffré, Milano, 2019, 395-397.

[9] See EDPB, *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*, 2019, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_it.

[10] According to the Irish Data Protection Commission, the scheme owner is the "*person or organisation responsible for developing and maintaining a specific certification scheme. A scheme owner can be a certification body, a governmental authority, a trade association, a group of certification bodies or others*". See DPA, *Guidance Note: GDPR Certification*, 2020, 7, available at: https://www.dataprotection.ie/sites/default/files/uploads/2020-09/GDPR%20Certification%20Guidance_0.pdf.

[11] See EDPB, *Guidelines 1/2018*, cit., 17; L. Bolognini, *Art. 42 – Certificazione*, cit., 296.

[12] On this point, the Guidelines list a number of general characteristics that need to be taken into account in the development and subsequent approval of the criteria. See EDPB, *Guidelines* 1/2018, cit., 22-24.

[13] See *ibid.*, 24 ff.

Board is based on the criteria's scope and the ability to serve as a common standard applicable among Member States, while taking into account the different data protection requirements that exist in each of them[14]. Awarding a recognisable mark in different Member States is likely to increase individuals' trust in certified processing, given the prior verification activities by independent experts and the approval of the criteria by the EDPB. As a result, the certified organisation may gain a competitive advantage[15].

Upon completion of the certification criteria approval process, certifications can be issued by accredited CBs under art. 43 GDPR or by national SA. However, it is not advisable for the latter authority to be involved, as its main responsibility is to monitor compliance with certification and GDPR requirements[16]. Conversely, CBs must be accredited by a national accreditation body or the competent SA (or by a combination of these two) in order to carry out their tasks. The process of accreditation certifies that the CB meets the independence, impartiality, and competence requirements, not only concerning the protection of personal data in general but also regarding the operation of certification criteria as outlined in art. 43 GDPR[17]. Additionally, CBs must adhere to a set of technical and operational requirements, such as establishing suitable procedures to manage the certification process and compliance with the technical standard ISO/IEC 17065:2012[18]. This standard outlines the requirements for bodies certifying products, processes, and services, and CBs must respect its requirement as further supplemented by additional criteria devised by SAs[19]. The accreditation is valid for five years but can, in any case, be suspended or withdrawn by the national accreditation body or the competent SA in case of violations of accreditation requirements or GDPR obligations.

After completing the accreditation process, a controller or processor can apply one or more processing operations (related to the target of evaluation) to the certification mechanism for a maximum of three years. This period can be renewed under the same conditions, provided that the relevant criteria are still met. However, in the event of a breach of the GDPR provisions or certification criteria, certification may be withdrawn by the CB or SA[20].

[14] See F. Pezza, *Art. 42 – Certificazioni*, cit., 479.
[15] See L. Bolognini, *Art. 42 – Certificazione*, cit., 297.
[16] This is because of the risk of the excessive mixing of roles at the head of the national SA. As even pointed out by the EDPB, where an SA chooses to conduct certification, it shall exercise its functions in a transparent manner, paying special attention to the separation of investigative and enforcement powers in order to avoid any potential conflict of interest. See EDPB, *Guidelines 1/2018*, cit., 7.
[17] See R. Leenes, *Article 43. Certification bodies*, cit., 747-751.
[18] Art. 43, par. 1.
[19] See EDPB, *Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation*, 2019, 9, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_en; F. Pezza, *Art. 43 – Organismi di certificazione*, cit., 489; R. Giannetti, *La certificazione ai sensi del GDPR: standard per l'affidabilità del mercato data-driven*, in L. Bolognini (eds.), *Privacy e libero mercato digitale: convergenza tra regolazioni e tutele individuali nell'economia data-driven*, Giuffré, Milano, 2021, 218-220.
[20] Art. 42, par. 7.

2.3 Certification schemes approved under the GDPR

Currently, there are several GDPR certification mechanisms in place, and other schemes are undergoing the criteria approval procedure by the respective SA.

The GDPR-Certified Assurance Report-Based Processing Activities Certification Criteria (CARPA) constitutes the first certification mechanism approved under art. 42 GDPR[21]. The scheme is unique, as it was developed by the Luxembourg SA to create an accredited compliance model for data controllers and processors[22]. The approval of the scheme has sparked criticism, as the Regulation does not explicitly provide for SAs to develop a certification mechanism[23]. However, the EDPB took a different view, recognising that SAs may develop their own schemes, if they guarantee to act impartially[24].

Approved following Opinion 25/2022 of the EDPB[25], the EuroPriSe© certification represents the direct evolution of an existing certification project in the German state of Schleswig-Holstein, already in place since Directive 95/46/EC[26]. This certification is primarily used by data processors to attest - in accordance with art. 28 GDPR - their compliance with the Regulation, with the aim of increasing trust among data controllers and data subjects[27]. Under this scheme, the certification criteria assess the processing activities from both a legal and technical perspective, verifying the satisfaction of formal obligations and the adequacy of the technical and organisational protection measures implemented to respond effectively to the accountability principle. Additionally, particular importance is given to relationships with data controllers and the management of data subjects' requests[28].

The EDPB has approved EuroPrivacy, the first European Data Protection Seal valid in all EU Member States with Opinion 28/2022. As previously stated, the European seal holds great value for the EU as it satisfies the varying needs of all Member States through

---

[21] The certification was approved following EDPB Opinion 1/2022. See EDPB, *Opinion 1/2022 on the draft decision of the Luxembourg Supervisory Authority regarding the GDPR – CARPA certification criteria*, 2022, available at: https://edpb.europa.eu/our-work-tools/ourdocuments/opinion-board-art-64/opinion-12022-draft-decision-luxembourg_en.

[22] With a desire to meet this need, the certification is made to be flexible and scalable, not focusing on a specific field or treatment, but being applicable in various areas. See CNPD, *Le schéma de certification "GDPR CARPA"*, 2023, available at: https://cnpd.public.lu/fr/professionnels/outils-conformite/certification/gdpr-carpa.html.

[23] The Regulation does not explicitly allow SAs to create their own certification mechanism. According to art. 42, par. 5, SAs are solely responsible for approving the certification criteria and are not authorised to create their own. Acknowledging such a possibility could create a conflict of interest between the authority's role as a supervisory body and its role as an investigative authority responsible for preventing unlawful processing. See E. Lachaud, *What GDPR tells about certification*, in *Computer Law & Security Review*, 2020, vol. 38, 3-4, available at: https://doi.org/10.1016/j.clsr.2020.105457.

[24] See EDPB, *Guidelines 1/2018*, cit. 8.

[25] See EDPB, *Opinion 25/2022 regarding the European Privacy Seal (EuroPriSe) certification criteria for the certification of processing operations by processors*, 2022, available at: https://edpb.europa.eu/our-worktools/our-documents/opinion-board-art-64/opinion-252022-regarding-european-privacy-seal_en.

[26] See G. Hornung, S. Bauer, *Privacy Through Certification?: The New Certification Scheme of the General Data Protection Regulation*, in P. Rott (eds.), *Certification - Trust, Accountability, Liability*, 2019, 109-132, available at: https://link.springer.com/book/10.1007/978-3-030-02499-4.

[27] See LDI-NRW, *LDI NRW genehmigt erste deutsche Kriterien für Datenschutz-Zertifizierung*, 2022, available at: https://www.ldi.nrw.de/ldi-nrw-genehmigt-erste-deutsche-kriterien-fuer-datenschutz-zertifizierung.

[28] See EuroPriSe Gmbh, *EuroPriSe Criteria for the certification of processing operations by processors*, 2022, available at: https://www.euprivacyseal.com/wp-content/uploads/2022/12/Kriterien_Verarbeitungsvor gangevon-AV_EN_v3_0.pdf.

its objective criteria[29]. Identifying objective criteria for assessing compliance can ensure a consistent application of the GDPR[30]. Indeed, being primarily aimed at commercial actors, in addition to general requirements on data protection principles, the scheme also includes specific criteria that make the certification adaptable to certain processing or business sectors, for example through the use of emerging technologies such as Artificial Intelligence, Internet of Things, and blockchain; it is also designed to be scalable to the needs of small and medium-sized enterprises[31].

In conclusion, there are currently two additional certifications, although unofficial under art. 42 GDPR. The first is the ISDP©10003 certification, which, despite being judged by the Tilburg University study commissioned by the EU Commission as compliant with GDPR requirements, has not yet been approved by the relevant Data Protection Authority[32]. The scheme sets out generic criteria for assessing GDPR compliance related to every case of processing. However, it can be adapted to complex and specific contexts, potentially integrating additional requirements[33]. The second certification, developed by scheme owner Brand Compliance, is awaiting approval from the Dutch Supervisory Authority and is addressed in EDPB Opinion 15/2023. However, relevant doubts have been raised regarding the formulation of certification criteria and the subjective scope of this scheme. It is unclear if it can be applied to *sub*-processors, and its ability to serve as a useful control element for assessing the correctness of measures implemented by the data controller or processor has been questioned. This is due to unclearly phrased and excessively generic terms which may lead to confusion in the auditing process, and the absence of specific criteria regarding the identification of all data processing activities that would fall within the scope of the certification[34].

III. A COMPARATIVE PERSPECTIVE: OTHER EXPERIENCES OUTSIDE THE EUROPEAN ECONOMIC AREA

Because the global economy relies on the exchange of data across borders, it is important to consider perspectives on certification schemes different from the one proposed in the

[29] See EDPB, *Opinion 28/2022 on the Europrivacy criteria of certification regarding their approval by the Board as European Data Protection Seal pursuant to Article 42.5*, 2022, 4, available at: https://edpb.europa.eu/system/files/2023-03/edpb_opinion_202228_europrivacy_eu_data_protection_seal_it.pdf.

[30] See ECCP, *Europrivacy GDPR Core Criteria*, 2020, 1-3, available at: https://community.europrivacy.com/europrivacy-gdpr-core-criteria/.

[31] See EU Commission, *Europrivacy: the first certification mechanism to ensure compliance with GDPR*, 2022, available at: https://digital-strategy.ec.europa.eu/en/news/europrivacy-first-certificationmechanism-ensure-compliance-gdpr.

[32] See EU Commission, Directorate-general for justice and consumers, G. Bodea, K. Stuurman, M. Brewczyńska, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: final report*, 2019, available at: https://data.europa.eu/doi/10.2838/115106.

[33] See Inveo, *ISDP©10003, Schema internazionale per la valutazione della conformità al Regolamento Europeo 2016/679*, 2020, 6 (par. 1.2), available at: https://www.in-veo.com/privacy-tools-new/schema-dicertificazione-isdp-c-10003-dw/37-schema-di-certificazione-isdp-10003-2020-rev-01-ita-new-release.

[34] See EDPB, *Opinion 15/2023 on the draft decision of the Dutch Supervisory Authority regarding the Brand Compliance certification criteria*, available at: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-152023-draft-decision-dutch-supervisory_en, 2023.

GDPR. The comparative approach aims to identify the state of the art of data protection certification also outside EU countries, in order to understand the differences - both in law and in practice - compared to the GDPR, and possibly to borrow its advantages. Therefore, the present analysis considers tools also based on a notion of privacy[35] and self-regulation or co-regulation tools with broader scope, when compared to art. 42 and 43 GDPR. The legal systems chosen for this analysis are: the United Kingdom, for its peculiarities linked to the recent exit from the EU; Canada for the sensitivity that has always characterised this legislation regarding the protection of personal data; the United States, as an example of a different approach to privacy issues compared to the European one; the People's Republic of China, for similarities between its national data protection law and GDPR.

Lastly, it is worth mentioning that certifications based on international ISO standards, such as ISO/IEC 27701, are of considerable importance worldwide. Although not legally recognised by specific regulations, these certifications enable private and public organisations to build trust in their solutions, e.g. by developing an effective privacy information management system, i.e. a management model to mitigate key privacy risks[36]. The uniqueness of these tools lies in the fact that they are usually built according to principles and concepts that originate in the US and must then be applied, and therefore interpreted, in the European legal framework when adopted by EU controllers and processors. A clear example may be the recent ISO 31700:2023 on privacy by design for consumer goods and services[37].

3.1 United Kingdom: UK GDPR and the first certification schemes approved

The United Kingdom was still part of the European Union when the GDPR was enacted[38]. Furthermore, the domestic legislation related to the safeguarding of personal data had originally been developed under the influence of Directive 95/46/EC, producing

[35] Right to privacy and right to data protection are two different fundamental rights. While the right to privacy is a broader concept encompassing various aspects of private life and family life, as addressed by art. 8 of the European Convention on Human Rights, the right to data protection (or informational privacy) is a more specific right focusing on the control and protection of personal data against possible unlawful data processing that could affect rights and fundamental freedoms of data subjects. See R. Gellert, S. Gurwirth, *The legal construction of privacy and data protection*, in *Computer Law & Security Review*, 2013, vol. 29, 522-530; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, 2016, 43-56; S. D. Warren, L. D. Brandeis, *The right to privacy*, in *Harvard Law Review*, vol. 5, n. 4, 1890, 193-220.

[36] See E. Lachaud, *ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification*, in *European Data Protection Law Review*, vol. 2, 2020, available at: https://www.researchgate.net/profile/Eric-Lachaud/publication/339988867_ISOIEC_27701_Threats_and_Opportunities_for_GDPR_Certification/links/617ab3b93c987366c3f6c026/ISO-IEC-27701-Threats-and-Opportunities-for-GDPR-Certification.pdf.

[37] See M. B. Pisoni, F. Tugnoli, *The new ISO 31700:2023 and the standardisation of Privacy by Design*, in *Privacy and Data Protection by ICTLC Italy*, 2023, available at: https://www.ictlc.com/the-new-iso-317002023-and-the-standardization-of-privacy-by-design/?lang=en.

[38] Even though the United Kingdom is no longer a Member State of the EU, in 2019 it signed the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, which provides - according to the art. 71, par. 1, - that: "*Union law on the protection of personal data shall apply in the United Kingdom in respect of the processing of personal data of data subjects outside the United Kingdom, provided that the personal data: (a) were processed under Union law in the United Kingdom before the end of the transition period; or (b) are processed in the United Kingdom after the end of the transition period on the basis of this Agreement*".

significant similarities between European and British regulations concerning data protection. Today, after Brexit, formally enacted on 1 January 2021, despite amendments made by the UK GDPR to the Data Protection Act (DPA), the rules on the protection of personal data, including the main principles and obligations, remain substantially identical to those of the EU[39].

The revision process undertaken by the UK GDPR also involved the rules regarding certification mechanisms[40]. All references to European institutions, such as the EDPB, national SAs or the European Commission were removed, and the Information Commissioner Officer (ICO) and the United Kingdom Accreditation Service (UKAS) were given full authority to approve certification criteria, and to define procedures for establishing certification criteria and for evaluating methodology[41]. For example, in its guidance, the ICO specifies the material scope of certification under the UK GDPR: these must concern a specific processing operation or a set of treatments that constitute a product, process, or service offered by the organisation seeking certification[42]. The purpose, even under the UK GDPR, is to demonstrate compliance with accountability obligations and the conformity of a specific processing operation with the regulations protecting personal data. Encouraging and rewarding compliance of certified entities, these mechanisms are assigned significant evidential value, useful for demonstrating compliance with the DPA regulations to the ICO, as well as to third parties[43]. Due to their evidential value, certifications allow the certified entity to demonstrate the adoption of all appropriate and reasonable measures to ensure the protection and security of processed personal data, as well as the rights and freedoms of the data subjects. Therefore, in the event of breaches, it is reasonable to expect that certification would be considered a mitigating factor in potential sanctions. However, certification might not always carry such weight. In cases of serious violations resulting from non-compliance with the DPA

[39] The Data Protection Act 2018 (c.12) is the national implementation GDPR. Since Brexit, the UK has committed itself to maintaining a data protection regulation equivalent to the EU's. This happened with Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, which revised the 2018 DPA to the new changes brought about by Brexit and for which it was named "UK GDPR". Indeed, the EU Commission, through Adequacy Decision No. 1772/2021, has determined that the UK legal framework provides the same guarantees as the European one to the individuals involved, allowing for cross-border transfer of data between the UK and the EU. See EU Commission, *Commission Implementing Regulation (EU) 2021/1772*, 2021, available at: https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex%3a32021d1772; P. de Hert, V. Papakonstantinou, *The rich UK contribution to the field of EU data protection: Let's not go for "third country" status after Brexit*, in *Computer Law & Security Review*, 2017, vol. 33(3), 355-356, available at: https://doi.org/10.1016/j.clsr.2017.03.008.

[40] See Data Protection Act 2018, §17 e Schedule 5 — *Accreditation of certification providers: reviews and appeals.*

[41] UKAS (United Kingdom Accreditation Service) is the national accreditation body of the United Kingdom established by the government to assess the competence of organisations that provide certification, testing, inspection, and calibration services.

[42] Similar to the GDPR, certification can focus on one, part of, or multiple personal data processing activities that constitute a unified product, process, or service. See ICO, *What can a UK GDPR scheme be about?*, available at: https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-schemes-detailed-guidance/how-do-we-develop-a-certification-scheme/#2.

[43] See Impact News Service, *New certification schemes will "raise the bar" of data protection in children's privacy, age assurance and asset disposal*, in *LexisNexis*, 2021, available at: https://advance.lexis.com/api/document?collection=news&id=urn:contentitem:63f7-2yd1-jdg9-y46w-00000-00&context=1516831.

regulations and certification criteria, adherence to a scheme may be assessed by the ICO as an aggravating factor because of the seriousness of the violation[44].

The process for creating a certification scheme is very similar to setting up under the GDPR. The development of related criteria is accompanied by their approval by the ICO, and the accreditation of a certification body by UKAS[45]. The certification criteria must thoroughly focus on evaluating specific processing operations performed and how data is handled in light of the DPA. The scope of certification can then be either broad, covering all aspects of the UK GDPR, or specific to a particular sector or a specific type of processing[46]. Additionally, the interoperability of criteria with other technical standards is important, as is the scalability of certification concerning the varying sizes of organisations seeking certification. Unlike the EU GDPR, certifications in the United Kingdom must address an additional requirement: an identified need or requirement within the realm of personal data protection. According to the ICO, certifications, in general, should have a clear purpose and cover a wide range of diverse processing activities, in order to meet the data protection needs demanded by the market or consumers (data subjects)[47].

Currently, the ICO has approved four certification mechanisms[48]:

1. Age Check Certification Scheme (ACCS): the scheme owner Age Check Certification Scheme has developed two certification mechanisms. The first (ACCS) is aimed at verifying processes that estimate and verify a person's age (to impose age limits on access to certified products or services)[49]. The primary objective of the

[44] See ICO, *Will the ICO consider certification as a mitigating factor in an investigation?*, available at: https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-schemes-detailed-guidance/how-do-we-apply-for-gdpr-certification/#how5.

[45] The accreditation of CBs is based on compliance with the technical standards outlined in ISO/IEC 17065 and additional accreditation requirements established by the ICO, similar to practices in the EU. Naturally, for accreditation, the CB must ensure its impartiality, independence from third parties, and especially from organisations requesting certification. Additionally, the CB must demonstrate compliance with the UK GDPR and the specific competence of its personnel regarding personal data protection. Once accredited to issue a certification mechanism, the CB will be responsible for continuously monitoring the certified entities' compliance and taking action to suspend or revoke certification if these entities no longer meet the certification criteria.

[46] From this perspective, the ICO emphasises that, rather than solely focusing on governance provisions and data management, it is crucial to carefully analyse the technical specifications and measures adopted by data controllers and processors seeking certification.

[47] Specifically, in the application for approval of certification criteria, the scheme owner must: provide that the certification meets specific needs within the personal data protection sector; demonstrate the added value of their certification compared to existing schemes; identify relevant economic, social, technological, legal, or other sectors that may be influenced by the certification and its development and implementation; demonstrate that the certification criteria are based on legislative or governmental priorities identified by the ICO or arising from the market and stakeholders involved in data processing. See ICO, *How do we develop a certification scheme?*, available at: https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-schemes-detailed-guidance/how-do-we-develop-a-certification-scheme/#10.

[48] See ICO, *Certification schemes register*, available at: https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-schemes-register/(last access 15th January 2024). In addition to the certifications mentioned, the 1st February 2024 the ICO have approved a new certification: the Legal Services Operational Privacy Certification Scheme. See ICO, Certification scheme register: Legal Services Operational Privacy Certification Scheme (LOCS), 2024, available at: https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-scheme-register/legal-services-operational-privacy-certification-scheme-locs/.

[49] See ICO, *Certification schemes register: Age Check Certification Scheme (ACCS)*, 2021, available at: *https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-scheme-register/age-check-certification-scheme-accs/*.

scheme is to verify an organisation's compliance with obligations related to age verification and data processing of minors, thus addressing public needs concerning the protection of children's privacy[50]. The ACCS certification provides a set of technical criteria focused on evaluating the effectiveness and accuracy of age verification processes for customers, as well as the appropriate design of those systems[51]. Specifically, the certification mark will be awarded based on controls which include, for example: age verification tools based on video identification; identity document verification; social proofing systems, which confirm age through validation requests to verified third-party contacts (e.g. parents).

2. Age Appropriate Design Certification Scheme (AADCS): this second certification developed by ACCS aims to provide a set of criteria for the appropriate design of age verification services, in accordance with the principles of data protection by design and by default and the principles of the British Children's Code[52]. The AADCS scheme is more general compared to ACCS, because it can be applied to any processing activity related to services provided by 'information society services' accessible to minors in the United Kingdom[53]. The scheme includes a series of technical, organisational, and documentary requirements that organisations processing personal data of minors must meet to demonstrate

[50] The certification criteria of ACCS 2-2021 concern several services which are based on data processing performed by data controllers or data processors, such as: "*a) Proof-of-Age ID Providers that verify age attributes and issue a reusable physical ID card, token or app that an unknown third party (such as a retailer) can rely on with or without a pre-arranged contractual relationship with the Proof-of-Age ID Provider; b) Age Check Providers that verify age attributes on request by a third party on a transaction-by-transaction basis under a pre-arranged contractual relationship with the Age Check Provider; c) Age Check Exchange Providers or Brokers that provide an online gateway for Age Check Providers and Relying Parties to access user asserted, permissioned and verified attributes; d) Relying Parties (online or offline) that rely on results of an age check (either remotely or during a face-to-face encounter) to establish the age-related eligibility of an individual for the purposes of a transaction (such as sellers or providers of age restricted goods and services)*". See Age Check Certification Scheme Ltd, *ACCS 2:2021 Technical Requirements for Data Protection and Privacy*, 2021, 5-8, available at: https://ico.org.uk/media/for-organisations/documents/2620426/accs-2-2021-technical-requirements-aadc.pdf.

[51] In addition to ensuring the proper implementation of technical and organisational measures necessary to guarantee the lawfulness of processing, there is also a need to verify age verification procedures. See *ibid.*, 20-66; See E. Koulierakis, *Certification as guidance for data protection by design*, in *International Review of Law, Computers & Technology*, 2023 7-8, available at: https://doi.org/10.1080/13600869.2023.2269498.

[52] The Children's Code, in effect since 2 September 2021, is a specific regulation applicable to all digital services aimed at individuals under 18 years of age or that, even if targeted at the general user base, are likely to be used by minors. See ICO, *Introduction to the Children's code*, available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/.

[53] With regard to this definition, it is to be considered that certification is applicable to both data controllers and joint data controllers, as well as data processors.

compliance with the Children's Code: for example, not resorting to geolocation systems[54] and data-profiling[55].

3. ICT Asset Recovery Standard 8.0: the scheme owner ADISA has developed a certification mechanism to ensure that personal data are processed correctly at the time of disposal of resources and computer equipment[56]. The certification regulates the disposal process by identifying procedures and operational methods based on risk from processing activities during sanitization of the storage media from personal data[57]. Because informed by a risk-based approach, the measures to be implemented and the controls for the assessment of conformity differ based on the category of the processed data[58].

4. UK GDPR Compliance Certification Scheme for the Provision of Training and Qualifications Services: developed by APM Group, it aims to build up the compliance with the UK GDPR of the organisations operating in the field of human resources training[59]. The scope is addressed to companies (private and public), acting as data controllers, in all activities related to their provision of training services and qualifications to candidates over 16 years of age. The scheme applies to the entire data lifecycle and all personal data processed, including those belonging to third parties, when providing these services. The only processing activities

[54] Those processes, however, are allowed if necessary and in the best interests of the child (such as safeguarding health, safety, and physical and moral integrity). See Age Check Certification Scheme Ltd, *ACCS 3:2021 Technical Requirements for Age Appropriate Design for Information Society Services*, 2021, 36, available at: https://ico.org.uk/media/for-organisations/documents/2620427/accs-3-2021-technical-requirements-aadc.pdf; ICO, *Certification scheme register: Age Appropriate Design Certification Scheme (AADCS)*, 2021, available at: https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-scheme-register/age-appropriate-design-certification-scheme-aadcs/.

[55] The criteria are clear in stipulating that, by default, profiling and automated processing of a child's data should not be carried out except in specific exceptions. However, in any situation where profiling is permitted, the data controller must take all necessary measures to protect the child from any harmful effects.

[56] The various processing activities included in the scope of application encompass customer involvement, logistics services, storage, resource management, and the recycling or resale of ICT equipment. See ADISA Certification Ltd, *ICT Asset Recovery Standard 8.0 Part 1: Introduction and Explanatory Notes*, 2022, 3, available at: https://ico.org.uk/media/for-organisations/documents/4021012/adisa-asset-recovery-standard-8_0-v3_1-part-1-introduction-and-explanation-notes.pdf; ICO, *Certification scheme register: ADISA ICT Asset Recovery Certification 8.0*, 2021, available at: https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-scheme-register/adisa-ict-asset-recovery-certification-80/.

[57] The treatment involving 'data sanitization' refers to the process of permanently and irreversibly destroying data on a storage device. This can occur at the end of the device's life cycle, at the conclusion of a device rental, or during the maintenance of non-functioning data storage devices for the purpose of recovering the device itself. However, the device is not intended to be returned to the data controller (e.g., refurbished products resold to the public). See ADISA Certification Ltd, *ICT Asset Recovery Standard 8.0 Part 1: Introduction and Explanatory Notes*, *cit.*, 4.

[58] See *ibid.,* 10 and *ff.* A unique aspect of the certification scheme is the provision for a new risk assessment document distinct from the Data Protection Impact Assessment (DPIA). To ensure that the data controller can manage their risk without being solely driven by cost, the Data Impact Assurance Levels (DIAL) is introduced. This evaluates the risk of the sanitization treatment based on five variables: 1. Threats; 2. Risk propensity; 3. Data category; 4. Data volume; 5. Impact of a data breach.

[59] See The APM Group Ltd, *UK GDPR Compliance Certification Scheme for the Provision of Training and Qualifications Services Criteria*, 2022, available at: https://ico.org.uk/media/for-organisations/documents/4023361/uk-gdpr-compliance-certification-scheme-for-the-provision-of-training-and-qualifications-services-v-6_2.pdf; ICO, *Certification scheme register: Provision of Training and Qualifications Services*, available at: https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-scheme-register/provision-of-training-and-qualifications-services/.

excluded from the scheme, since they are not considered relevant for the purposes of training and qualification, are those related to minors under 16 years of age, and personal data concerning criminal convictions and offences. The scope of evaluation of the criteria is particularly broad, as they are aimed at verifying compliance with the general requirements and principles of the UK GDPR[60], the provision of free consent from the data subject, the methods of managing the requests for exercising the rights of the data subjects, the formulation of a clear information notice to the latter and other operational requirements (including data breach notifications, the register of processing activities, procedures for cooperating with authorities, etc.)[61].

3.2 Canada: Privacy by Design Certification Shield

Following the full implementation of GDPR, the Brussels Effect has had significant influence on Canada's data protection regime[62]. In recent years, there have been several attempts to reform the Personal Information Protection and Electronic Documents Act (PIPEDA)[63], contributing to a more comprehensive and cohesive shift in perspective regarding data protection as a recognized right within the legal framework. Of particular note is Bill C-27: Digital Charter Implementation Act 2022, because it aims to introduce a new legislative text that would repeal much of PIPEDA, namely the Consumer Privacy Protection Act[64]. With the bill, new obligations for personal data processing will be introduced, granting new rights to data subjects - such as the right to data disposal and the private right to sue for damages in a Federal Court for loss or injury suffered as a result of a violation by an organisation. Also, a new body, the Personal Information and Data Protection Tribunal, will be established to adjudicate disputes regarding violations of the

[60] As, for example, the appointment of the DPO, company staff training, audit checks, compliance with DPbDD, conducting DPIAs and adherence to principles of lawfulness, fairness and transparency; purpose limitation; data retention limitation; data minimization; accuracy; integrity and confidentiality.

[61] See The APM Group Ltd, *UK GDPR Compliance Certification Scheme for the Provision of Training and Qualifications Services Criteria*, *cit.*, 12-36.

[62] See A. Bradford, *The Brussels Effect: How the European Union Rules the World*, New York, Oxford Academic, 2020, 25–66, available at: https://doi.org/10.1093/oso/9780190088583.001.0001.

[63] The PIPEDA represents the primary Canadian legislation concerning the protection of personal data in the private sector. This law focuses on safeguarding any personal information related to an identified individual. Unlike the European GDPR, the PIPEDA does not consider data pertaining to an indirectly identifiable subject as personal data. The PIPEDA establishes the requirements and principles that data processing must adhere to in order to be considered lawful. Furthermore, it grants rights to affected individuals similar to those outlined in the GDPR, ensuring control over their personal data and the ability to request access, rectification, erasure, and restriction of processing, when applicable. See M. Bhasin, *Challenge of Guarding Online Privacy: Role of Privacy Seals And Government Regulations*, in *South Asian Journal of Marketing & Management Research*, 3 (2), 2016, 69, available at: https://www.researchgate.net/publication/309407924_challenge_of_guarding_online_privacy_role_of_privacy_seals_and_government_regulations.

[64] Currently the bill has not yet been approved. See Government of Canada, *Consumer Privacy Protection Act*, 2023, available at: https://ised-isde.canada .ca/site/innovation-better-canada/en/consumer-privacy-protection-act; G. Bincoletto, *Il diritto alla protezione dei dati: una prospettiva comparata*, in P. Guarda, G. Bincoletto, *Diritto comparato della privacy e della protezione dei dati personali*, cit., 124.

legislation protecting personal data, as a second instance beyond the decisions of the Office of the Privacy Commissioner of Canada.

In the PIPEDA, as in the rest of current Canadian legislation, there is no reference to certifications or codes of conduct related to data protection. However, in an effort to establish Canada as a global player in digital policy, a project was initiated to create a Canadian mark for consumer data protection that would be recognized internationally[65]. This certification was intended to be developed by the private sector in cooperation with the government, consumer-interest groups and the Canadian Standards Association (CSA) International[66]. This mark would be managed by a neutral third party tasked with raising consumer awareness, promoting the adoption of the certification program, monitoring compliance and adherence, and providing a dispute resolution system[67]. In this context, Canada's thrust as a global player in the evolution of the data protection field is witnessed by Ann Cavoukian's elaboration of the privacy by design principle, which seeks to pre-empt data protection issues already at the design stage of information systems[68].

In 2015, the Privacy by Design Certification Shield program emerged from this vision, launched by the Privacy and Big Data Institute at Ryerson University in collaboration with Deloitte Canada.

The purpose of the certification scheme is to assist companies and organisations in proactively incorporating privacy into their processes by translating the seven principles of privacy by design into empirically measurable criteria. The scope of the certification involves privacy in the design, operation, and management of a specific information system, business process, or network project. From this perspective, compared to other legal systems, the Privacy by Design Certification Shield is very similar to data protection certifications provided under the EU GDPR and UK GDPR, as both encompass data processing related to products, processes, or services[69]. One relevant aspect of this certification scheme is its potential for international application: the privacy by design

---

65 This initiative stems from the observations made by the Canadian E-Business Opportunities Roundtable in the report *Fast Forward: Accelerating Canada's Leadership in the Internet Economy*. In particular, the Roundtable pointed out the importance of developing privacy and consumer protection issues to establish e-business leadership. See R. Simpson, *Making Canada a Global Centre of Excellence for Electronic Commerce*, in *Horizons*, vol. 3(1), 2000, 17-18, available at: https://publications.gc.ca/collections/Collection/CP12-1-3-1E.pdf.

66 In fact, the Canadian standardisation body has developed the Model Code for the Protection of Personal Information, which forms one of the pillars of Canada's approach to data privacy legislation. It is available at: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-7.html. See J. M. Spaeth, M. J. Plotkin, S. C. Sheets, *Privacy, Eh! The Impact of Canada's Personal Information Protection and Electronic Documents Act on Transnational Business*, in *Vanderbilt Journal of Entertainment and Technology Law*, vol. 4, 2002, 30, available at: https://scholarship.law.vanderbilt.edu/jetlaw/vol4/iss1/3.

67 See A. Cavoukian, M. Chibba, *Privacy Seals in the USA, Europe, Japan, Canada, India and Australia*, in R. Rodrigues, V. Papakonstantinou (eds.), *Privacy and Data Protection Seals*, 76.

68 Concept developed by Ann Cavoukian, former Privacy Commissioner of Ontario, and based on seven principles aimed at regulating data protection: proactive not reactive, preventive not remedial; privacy as the default setting; privacy embedded into design; full functionality - positive-sum, not zero-sum; end-to-end security - full lifecycle protection; visibility and transparency - keep it open; respect for user privacy - keep it user-centric. See A. Cavoukian, *Privacy by design, The 7 Foundational Principles*, Canada, 2011, available at: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf; G. Bincoletto, *La privacy by design: un'analisi comparata nell'era digitale*, Roma, 2019, 79-81.

69 See EU Commission, Directorate-general for justice and consumers, G. Bodea, K. Stuurman, M. Brewczyńska, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: annexes*, 2019, 65, available at: https://data.europa.eu/doi/10.2838/297807.

certification criteria identified by Deloitte aim to be aligned with the GDPR but also with other major international regulations and standards on the protection of personal data and information - including Convention no. 108 of the Council of Europe and ISO/IEC 27001 and ISO/IEC 27701 certification[70].

The certification process is directly managed by the Privacy and Big Data Institute and Deloitte[71], which will enter into an agreement with the requesting party seeking certification, which will regulate the terms of using the certification mark and outline the responsibilities for its usage. They will also conduct all necessary audit and assessment checks required for the certification[72]. In the event of a positive outcome, the organisation will be granted the Certification Shield mark. This certification is valid for a maximum of three years and is subject to annual renewal checks to ensure the certified subject's continuous compliance with the certification criteria. Additionally, these renewal checks oversee the updating of measures implemented for the protection of personal data concerning new technologies[73].

At the conclusion of the certification process, the certified subject will be capable of conducting personal data processing that is largely compliant with Canadian regulations. This capability enables the organisation to minimise the risks associated with potential non-compliance and, consequently, reduces the likelihood of facing administrative or

[70] It is reasonable to assume that if an organisation that is not part of the EU sought to obtain the Privacy by Design Certification Shield, it could achieve a significant level of compliance compared to other alternative privacy certifications in relation to the GDPR. However, it is important to emphasise that possessing such certification does not automatically guarantee full compliance with the GDPR, as these are two different regulatory contexts. The certification primarily focuses on the privacy by design principle and may not necessarily cover all specific aspects and requirements of the GDPR.

[71] Therefore, there are no third-party CBs involved with the mentioned organisations. See A. Cavoukian, Ryerson University, *Commit to Privacy, Publicly – Privacy by Design Certification Program*, 6, available at: https://www.torontomu.ca/content/dam/pbdce/certification/PbD-Brochure.pdf; Ryerson University, *Privacy by Design Assessment and Certification*, available at: https://www.torontomu.ca/content/dam/pbdce/certification/Privacy- by-Design-Overview_PbDCE.pdf.

[72] In particular, Deloitte will examine the products, services, and processes to be certified by conducting interviews, analysing documentation, and reviewing operational procedures. Subsequently, Deloitte will publish a report on which the Privacy by Design Centre of Excellence will conduct its verification assessments to determine whether or not to grant the certification. See A. A. Foujdar, *Implementing Privacy by Design through Privacy Impact Assessments*, Turku, 2019, 28-31, available at: https://urn.fi/urn:nbn:fi-fe2019061019771. For a delve into the content of the certification criteria see Deloitte, *Privacy by Design Certification Program: Assessment Control Framework - Privacy by Design: Privacy Assessment Methodology*, 2016, available at: https://www.torontomu.ca/content/dam/pbdce/certification/Privacy-by-Design-Certification-Program-Assessment-Methodology_PbDCE.pdf.

[73] The renewal, in fact, requires a statement from the organisation confirming that there have been no changes affecting their certification. See ENISA, Recommendations on European Data Protection Certification, 2017, 42-43, available at: https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification; A. Cavoukian, M. Chibba, *Privacy Seals in the USA, Europe, Japan, Canada, India and Australia*, cit., 77-78. In addition to this annual check, the Privacy by Design Centre of Excellence provides a reporting mechanism to the public through its website. Through this mechanism, individuals can report any violations or discrepancies observed in the certified entity in compliance with the certification policy. In cases where violations or discrepancies are found, the Centre reserves the right to suspend or revoke the certification. See EU Commission, Directorate-general for justice and consumers, G. Bodea, K. Stuurman, M. Brewczyńska, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: annexes*, cit., 68-69.

criminal sanctions, as well as compensation claims for data breaches[74]. Moreover, similar to certifications in the European framework, the Privacy by Design Certification Shield provides a distinctive mark compared to other competitors. This increases the trust of third parties and consumers in the certified products and processes, thereby providing a significant competitive advantage.

3.3 United States: an overview in the healthcare and online industry scenarios

The US system has been selected due to its position as a global leader in the development of new technologies, as well as its primary role as an economic and trade partner with the EU. Nonetheless, the implementation of self-regulatory tools has been made problematic and susceptible to interference due to the lack of a unified legislative text on data protection or a regulatory recognition of certification to ensure their enforcement. In that context, the development of certifying mechanisms aimed at protecting personal data has been achieved through the various implementing decisions concluded with the European Commission for the cross-border transfer of personal data. However, this was done solely with the aim of creating a legal framework that is suited to the EU.

Differently from the UK and to a lesser extent from Canada, the United States does not have a uniform level of personal data protection[75]. Since the enactment of the Privacy Act - which governs informational privacy[76] in processing carried out by federal agencies - no other federal law comprehensively addresses the protection of personal information. Instead, a series of federal laws and regulations govern the collection and disclosure of personal information, each of which is addressed differently by the US law based on

---

[74] See B. Sookman, *Privacy by Design certification framework launched by Ryerson and Deloitte*, 2015, available at: *https://www.barrysookman.com/2015/05/25/privacy-by-design-certification-framework-launched-by-ryerson-and-deloitte/*.

[75] See A. C. Raul, T. D. Manoranjan, V. Mohan, *United States*, in A. C. RAUL (eds.), *The Privacy, Data Protection and Cybersecurity Law Review*, 2014, 268-270, available at: *https://www.sidley.com/-/media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurity-la__/files/united-states/fileattachment/united-states.pdf*.

[76] The term "informational privacy" began to develop in US jurisprudence as a declination of the right to privacy and, specifically, as "*individual interest in avoiding disclosure of personal matters*" (Nasa v. Nelson, 131 S. Ct. 746 (2011)). A clearer definition is provided by scholars, who define "informational privacy" as freedom from epistemic interference that is archived where there is a restriction on personal information about someone that is unknown. Such information can include data that are directly related to a person, such as personal lifestyle, finances, medical history, and academic achievement. See H. T. Tavani, *Informational Privacy: Concepts, Theories, and Controversies*, in K. E. Himma, H. T. Tavani (eds.), *The Handbook of Information and Computer Ethics*, 2008, 139-141, available at: https://doi.org/10.1002/9780470281819.ch6; L. Floridi, *The Ontological Interpretation of Informational Privacy*, in *Ethics and Information Technology*, vol. 7(4), 185– 200, 2005, available at: https://link.springer.com/article/10.1007/s10676-006-0001-7. It is clear from this that the concept of personal information is narrower than that of personal data, which - according to art. 4, no. 1 GDPR - corresponds to "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly[...]*".

specific sectors[77]. Furthermore, the US regulatory landscape is complex, in light of various initiatives by specific States to adopt privacy laws at the domestic level[78].

In response to this critical situation, both public and private institutions have attempted to adopt a soft-law approach - based on self-regulatory or co-regulatory tools developed by trade associations - to modernise information privacy and align protection similarly to provisions in other legal contexts[79]. Nevertheless, within this framework, the standardisation did not focus on safeguarding personal data, because the initial goal was to establish regulations for consumer privacy on the internet and enhance cybersecurity for information.

Since the early 2000s, initiatives have emerged to regulate online business practices, including certifications aimed at verifying compliance with consumer privacy in the United States. Some of these certifications have an international scope, relying on global principles of personal data protection, such as the 1980 OECD Privacy Guidelines[80], surpassing sector-specific legislation on informational privacy[81].

The privacy certification mechanisms in the United States have, therefore, gained progressive significance due to their potential to standardise the management of informational privacy. Moreover, these certifications are intended to contribute to building consumer trust in web platforms through an attestation provided by a third-party institution that is impartial and possesses high professional expertise. Based on these characteristics, this entity is expected to transfer trust from third parties and consumers to

[77] Federal laws regulating the protection of personal information encompass, for example, consumer credit reports, electronic communications, federal agency records, educational records, banking information, healthcare information, protection of minors' personal information, and safeguarding financial information. See M. Bhasin, *Challenge Of Guarding Online Privacy: Role of Privacy Seals And Government Regulations*, cit., 66-67. For a more comprehensive list see P. Guarda, G. Bincoletto, *Diritto comparato della privacy e della protezione dei dati personali*, cit., 32-34.

[78] Currently, thirteen states have enacted national laws regarding consumer data privacy protection: California, Virginia, Colorado, Connecticut, Utah, Florida, Texas, Oregon - which are currently effective - and Iowa, Indiana, Tennessee, Montana, Delaware, New Hampshire, New Jersey, Kentucky, Nebraska, Rhode Island.. See generally S. P. Shatz, P. J. Lysobey, *Update on the California Consumer Privacy Act and Other States' Actions*, in *The Business Lawyer*, vol. 77(2), 2022, 539-547, available at: https://www.mcglinchey.com/wp-content/uploads/2022/04/011-ABA-TBL-77-2-Shatz_Lysobey.pdf; F.P. Pittman, *US Data Privacy Guide*, in *White&Case Newsletter*, available at: https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide (last access 22nd October 2024).

[79] The Fair Information Practice Principles are of considerable importance. They were developed by the Department of Health, Education, and Welfare Advisory Committee and have been implemented in various measures by different US agencies and departments. See Privacy Council*, Fair Information Practice Principles (FIPPs),* available at: https://www.fpc.gov/resources/fipps/.

[80] See OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 1980.

[81] The advantage of privacy certifications, as a means of self-regulation through industry associations, would have been to adapt more rapidly and effectively to technological innovations compared to state or federal legislation. See FTC, *Protecting consumer privacy in an era of rapid change. Recommendations for businesses and policymakers*, 2012, 2-14, available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

certified online operators[82]. By creating such a trust mechanism among consumers, the certifying entity and the certified bodies, organisations that do not respect user data privacy - and thus could not obtain certification - would be ousted from the market. This would benefit entities capable of demonstrating their privacy compliance through a distinctive mark[83].

The privacy certifications are intended to address three points - based on which they can also be classified - namely, whether they contribute to ensuring consumer privacy, whether they assure the security of their information, or whether they safeguard the integrity of online transactions. Each certification is supposed to pursue one or more of these 'functions', depending on the structure of the certification criteria, ultimately leading to the reinforcement of consumer trust in online services[84].

In this framework a significant role in certifying and managing privacy and security is played by HITRUST and TRUSTe, within their respective domains, namely healthcare (HITRUST) and consumer privacy (TRUSTe)[85].

The HITRUST (Health Information Trust Alliance) certification is a comprehensive approach designed specifically for the healthcare industry to manage and safeguard Protected Health Information (PHI) effectively. This is the dominant certification framework in the US health industry. HITRUST provides a framework and a common security standard that integrates various regulations and standards, such as the HIPAA Act[86], HITECH Act[87] and ISO/IEC 27001, to assess and manage risks related to health information[88]. Like European GDPR certification, the HITRUST approach is based on

---

[82] See S. Listokin, *Does Industry Self-Regulation of Consumer Data Privacy Work?*, in *UIC John Marshall Journal of Information Technology & Privacy Law*, vol. 32(1), 2015, 17-19, available at: https://repository.law.uic.edu/jitpl/vol32/iss1/2/.

[83] Indeed, certification could offer a solution to the information asymmetry found in the market between businesses and consumers. It could allow consumers to distinguish, at first glance, products and services from companies that respect personal data from those that do not take it into account. See FTC, *Protecting consumer privacy in an era of rapid change. Recommendations for businesses and policymakers*, cit., 60-71.

[84] See K. Kyongseok, K. Jooyoung, *Third-party Privacy Certification as an Online Advertising Strategy: An Investigation of the Factors Affecting the Relationship between Third-party Certification and Initial Trust*, in *Journal of Interactive Marketing*, 2011, 25(3), 145–158, available at: https://doi.org/10.1016/j.intmar.2010.09.003.

[85] See M. Bhasin, *Challenge Of Guarding Online Privacy: Role Of Privacy Seals And Government Regulations*, cit., 63-65.

[86] The Health Insurance Portability and Accountability Act, enacted in 1996, aims to safeguard individuals' Protected Health Information (PHI), which is personal information related to medical history, health diagnoses and insurance data that can be used to identify patients. HIPAA establishes privacy and security standards for healthcare data, ensuring its confidentiality and integrity. The law also grants individuals control over their health information and regulates the use and disclosure of PHI by healthcare providers, health plans, and other entities. HIPAA compliance is essential in maintaining the privacy and security of patient information, with significant penalties for non-compliance.

[87] The Health Information Technology for Economic and Clinical Health Act, enacted in 2009, incentivises the widespread adoption of electronic health records (EHRs) among healthcare providers in the US. It aims to improve healthcare quality, efficiency, and patient outcomes. The legislation enforces HIPAA regulations, imposing penalties for non-compliance to enhance data privacy and security. For more details see L. Determann, *Healthy Data Protection*, in *Michigan Technology Law Review*, vol. 26, 2020, 241-244, available at: https://repository.law.umich.edu/mtlr/vol26/iss2/3.

[88] On the basis of these international standards and regulations, HITRUST incorporates almost 2,000 controls on protecting personal information that are continually updated. For example, its certification criteria are aligned with the California Consumer Privacy Act - as one of the most advanced regulations in the United States relative to the protection of personal data - and the GDPR also. For a list of all the authoritative sources which are covered by certification see HITRUST, *Introduction to the HITRUST CSF*, 9-

risk management, providing adequate transparency, scalability, consistency, accuracy, integrity, and efficiency on compliance assessment[89]. This seal aims at standardising and, consequently, facilitating the adoption of management systems for PHI and their integrity and security, as well as internal policies and regulations for the management and mitigation of risk concerning potential non-compliance or cyber threats[90]. Consequently, the depth of cybersecurity controls and data protection measures can be tailored to align with the risk profile of a specific organisation. This profile may vary based on the relationships that healthcare entities may have with different clients, stakeholders, and third-party end users[91]. However, this characteristic represents a significant difference from the GDPR. While the European regulation is rooted in a risk-based approach, it is more oriented towards a right-based methodology, varying the possible compliance requirements for data controllers but still maintaining a core set of obligations and rights that must always be respected[92].

As previously mentioned, the HITRUST Seal is based on federal and state regulations that oversee the management and safeguarding of PHI. This represents a key benefit of the certification, as it guarantees that healthcare companies applying the framework comply with the security and privacy laws of the United States.

One potential limitation of the HITRUST Seal is a concentrated emphasis on healthcare compliance. Its certification criteria take partial account of technical and organisational measures aimed at ensuring effective cybersecurity management and preventing breach risks[93]. However, this shortcoming can be remedied with other standards that focus primarily on information security management systems, thanks to the interoperability of HITRUST. Integrating the requirements of the latter with other certification schemes

10, available at: https://hitrustalliance.net/product-tool/hitrust-csf/; A. A. Garba, A. M. Bade, *An Investigation on Recent Cyber Security Frameworks as Guidelines for Organizations Adoption*, in *International Journal of Innovative Science and Research Technology*, vol. 6(2), 2021, 106, available at: https://ijisrt.com/assets/upload/files/IJISRT21FEB114.pdf.

[89] See HITRUST, *Why HITRUST Certifications are Broadly Accepted and Considered the Gold Standard*, 2, available at: https://hitrustalliance.net/content/uploads/Why-the-HITRUST-Certification-is-So-Broadly-Accepted.pdf. From an operational point of view, to evaluate organisations, HITRUST uses external auditors who test and validate security controls, possessing vast experience in IT compliance and auditing. The assessors must adhere to strict requirements to ensure the adequacy and efficiency of controls in order to award the HITRUST mark. See HITRUST, *Introduction to the HITRUST CSF*, cit., 8.

[90] See A. U. Patel, C. L. Williams, S. N. Hart, C. A. Garcia, T. J. S. Durant, T. C. Cornish, D. S. McClintock, *Cybersecurity and Information Assurance for the Clinical Laboratory*, in *The Journal of Applied Laboratory Medicine*, vol. 8(1), 2023, 145–161, available at: https://doi.org/10.1093/jalm/jfac119, where the authors highlight possible risks for healthcare facilities and identify procedures for their mitigation, in relation to US regulations as well as current standards.

[91] See M. F. Abo El Rob, *A narrative review of advantageous cybersecurity frameworks and regulations in the United States healthcare system*, in *Issues in Information System*, vol. 24(2), 2023, 9, available at: https://doi.org/10.48009/4_iis_2023_126.

[92] See WP29, *Opinion 1/1998 - Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)*, 1998, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp11_en.pdf; cf. R. Gellert, *Understanding the notion of risk in the General Data Protection Regulation*, in *Computer Law & Security Review*, 2018, vol. 34(2), 279-288; ID., *Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative*, in *International Data Privacy Law*, 2015, vol. 5(1), 3-19.

[93] See M. F. Abo El Rob, *A narrative review of advantageous cybersecurity frameworks and regulations in the United States healthcare system*, cit., 16.

could prove beneficial for adopting proactive measures in data protection compliance[94]. These could mitigate a wide array of risks in the processing of PHI, providing effective security of data and ensuring that data subjects and other stakeholders place greater trust in the certified subject. From this perspective, obtaining HITRUST certification could help as a competitive advantage by expanding current partnerships and earning new business for healthcare industries[95].

The TRUSTe certification scheme, developed by TrustArc Inc., is a personal data management model used for online platforms. The certification primarily concerns transparency and cybersecurity, mandating that companies implement commercially reasonable protections for data security. TRUSTe bases its criteria on both US and international standards[96] which take into account the protection of personal information[97] and privacy of consumers on the web[98].

Regarding the certification process for TRUSTe, the organisation that owns the online platform seeking certification must agree to the principles of the scheme and adhere to the supervision and monitoring procedures of the certification program. These principles are particularly significant. Organisations are required to include a privacy policy on their website that clearly outlines the personal information collected, also seeking user consent for the processing of this information. Additionally, the site must have adequate security measures in place to safeguard user information. TRUSTe conducts a verification of these principles and required security standards. Upon completion of the inspection procedures, TRUSTe may certify that the applicant is compliant with the program's requirements[99].

After assigning the mark, TRUSTe does not directly monitor compliance with certification requirements. Instead, it employs an indirect control mechanism that permits third parties to report potential certification violations. Upon receiving such reports, a sort of inspection process can be activated, during which the certification may be temporarily suspended or withdrawn[100]. However, it is unclear how TrustArc effectively manages non-

[94] *Ibidem*.

[95] See HITRUST, *Why HITRUST Certifications are Broadly Accepted and Considered the Gold Standard*, cit., 4.

[96] In particular, this relies in part on the FTC Fair Information Practice Principles, the NAI (Network Advertising Initiative) principles, and the DAA (Digital Advertising Alliance) principles. These frameworks help guide businesses towards responsible data practices in various aspects of consumer data protection and privacy in advertising and digital realms.

[97] Personal data is not considered, but rather personal information. The difference lies in the fact that for the protection of informational privacy, it is necessary that the information/data be directly linked to an identified individual, whereas data that allow potential identification of the subject to whom they belong are not protected.

[98] The criteria can be classified into various categories, including: limitation of processing; use of personal information; choice; collection and use of third-party personal information; user profile visibility; access; promotional communications and newsletters; material changes; data security; data quality and integrity; data retention; third-party data sources; service providers; training; user complaints and feedback; data breaches; accountability; and cooperation with TrustArc. See TrustArc, *TRUSTe APEC Privacy Certification Standards*, 2016, available at: https://download.trustarc.com/dload.php/?f=LH7RIJRS-627.

[99] See M. Bhasin, *Challenge of Guarding Online Privacy: Role of Privacy Seals and Government Regulations*, cit., 63-65; EU Commission, Directorate-general for justice and consumers, G. Bodea, K. Stuurman, M. Brewczyńska, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: annexes*, cit., 83-88.

[100] See EU Commission, Directorate-general for justice and consumers, G. Bodea, K. Stuurman, M. Brewczyńska, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: annexes*, cit., 85-86.

compliance. This lack of transparency in the functioning of the monitoring system represents a serious flaw in the certification scheme. There have been reported instances where several certified subjects, despite violating the required privacy principles for obtaining the mark, were still certified. Furthermore, it appears that the revocation of the seal is not frequently exercised, often keeping any identified violations confidential. Additionally, in 2014, TrustArc underwent an FTC investigation for allegedly failing to adhere to its own programs regarding annual recertification for maintaining certification marks in over 1,000 cases between 2006 and 2013, allowing previously certified platforms to retain the seal without any oversight[101].

The weak enforcement capability of TrustArc as a certifying body, along with the significant potential for abuse of certification by third parties, highlights the inherent weaknesses in privacy certifications like TRUSTe in the United States. This is due to the fact that certification bodies lack real power to address potential abuses of their own schemes. In such circumstances, certification could ultimately lead to a negative impact on the privacy and security of information, as data handling practices would be at a higher risk of data breaches[102].

One cause of the inefficiency of privacy certifications could indeed be the absence of general norms on personal data protection or legislative frameworks that enable federal authorities and agencies to oversee the proper implementation of certification schemes. Adopting a federal legislative text on personal data protection might, therefore, be a solution, making the right to informational privacy of users more enforceable. However, this possibility faces opposition from many[103], proving difficult to achieve[104]. Consequently, it might be more suitable to adopt an approach focused on co-regulation. Three possible co-regulatory models have been identified within legal theory[105]. Nevertheless, it is evident that cooperation between companies, private organisations, and

[101] See FTC, *TRUSTe Settles FTC Charges it Deceived Consumers Through Its Privacy Seal Program*, 2014, available at: https://www.ftc.gov/news-events/news/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its-privacy-seal-program; TrustArc Inc, *TrustArc's Agreement with the FTC*, 2014, available at: https://trustarc.com/trustarcs-agreement-with-the-ftc/.

[102] It has indeed been demonstrated that websites certified with the TRUSTe seal are more likely to be classified as untrustworthy compared to non-certified web platforms. See S. Listokin, *Does Industry Self-Regulation of Consumer Data Privacy Work?*, cit., 17-19.

[103] Some lobbyists and industrial groups, in fact, opposed this solution, believing that self-regulation was the only feasible option, even from a free-market perspective. However, such a stance cannot be reasonably supported until there is certainty that CBs, such as TrustArc, are capable of adequately monitoring the digital industry and wielding enforcement powers capable of penalising any non-compliance. See C. P. O'Kane, *Digital privacy and new media: An empirical study assessing the impact of Privacy Seals on personal information disclosure*, Bournemouth, 2019, 77-78, available at: https://eprints.bournemouth.ac.uk/34340/1/O%E2%80%99KANE%2C%20Conor%20Paul_Ph.D._2019.pdf.

[104] Indeed, in light of this, there was the failed attempt in 2022 to pass the American Data Privacy and Protection Act, which was intended to become the first federal law on online privacy. Although this federal bill represented an initial attempt to comprehensively regulate privacy, it didn't receive positive assessments and faced substantial criticism from industry associations as well as representatives from the State of California, which already has its own comprehensive data protection law in place.

[105] See R. Rodrigues, D. Wright, K. Wadhwa, *Developing a privacy seal scheme (that works)*, in *International Data Privacy Law*, vol. 3(2), 2013, 112, available at: https://doi.org/10.1093/idpl/ips037.

public authorities or the potential corrective intervention of the latter would ensure greater protection of informational privacy, reasonably ensuring the proper implementation of certification mechanisms, codes of conduct, or any other means of private self-regulation. In conclusion, concerning the certifications related to the protection of personal information within the US legal framework, it is worth referring to the new political agreement reached between the United States and the European Union aimed at making changes to US legislation to align it with the requirements outlined by the GDPR for cross-border transfer of personal data. The establishment of the EU-US Data Privacy Framework (hereinafter: DPF) served as the basis for the EU Commission's adoption of the adequacy decision on 10 July 2023, allowing the transfer of personal data to the United States without the additional safeguards required by art. 46 GDPR[106].

After the new requirement introduced by the Executive Order 14086 (hereinafter: EO-14086) to the data processing conducted by the US intelligence agencies[107], the new DPF aims to strengthen data privacy protection by correcting the critical issues previously raised by the CJEU. The Framework is precisely built upon certifications to attest to the ability of US businesses to adhere to the principles and guarantees outlined in the GDPR[108]. Data controllers and processors will be able to self-certify their compliance with the principles of the DPF in order to receive and process data originating from the EU. The mechanism will be administered by the US Department of Commerce, which will process certification applications and monitor whether participating companies continue to meet certification requirements [109]. Hence, European personal data can be transferred to any US organisations self-certified and included in the Data Privacy Framework List, as endorsed by the adequacy decision[110]. For entities not included in the List, the standard contractual

[106] See EU Commission, *Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows*, 2023, available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721; EU Commission, *Commission Implementing Regulation (EU) 2023/4745 - adequacy decision*, 2023, available at: https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_it.

[107] See The White House, Executive Order 14086 of October 7 2022, *Enhancing Safeguards for United States Signals Intelligence Activities*, available at: https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf. The EO-14086 incorporates into US law the principles that the processing of personal data by intelligence agencies should be governed by the criteria of necessity and proportionality in relation to their strategic objectives.

[108] The adequacy decision has been adopted after years of political discussion with the Commission and the US Government to assess if the US provides a level of data protection substantially equivalent to the EU. This evaluation follows the case law Schrems I and Schrems II of the CJUE, which invalidated the previously established US-EU treaty on data transfer due to the serious threats posed to the rights of EU citizens. These risks stem primarily from: the persisting primacy of US national security regulations over the principles of the Privacy Shield (and before the Safe Harbor); the lack of necessary limitations on the power of US intelligence agencies, particularly in light of proportionality requirements and bulk data collection (violating art. 52 of the Charter of Nice and causing excessive interference with fundamental rights under artt. 7-8 of the Charter); and the lack of judicial remedies for European data subjects, due to the absence of an independent and impartial judiciary (violating art. 47 of the Charter). For a comprehensive analysis of CJEU Case C-311/18 (Schrems II) and its consequences see R.A. Costello, *Schrems II: Everything Is Illuminated?*, in *European Papers*, vol. 5(2), 2020, 1045-1059, available at: https://www.europeanpapers.eu/it/europeanforum/schrems-II-everything-is-illuminated.

[109] See US Department of Commerce, *How to Join the Data Privacy Framework (DPF) Program*, available at: https://www.dataprivacyframework.gov/s/article/How-to-Join-the-Data-Privacy-Framework-DPF-Program-part-1-dpf.

[110] See US Department of Commerce, *Data Privacy Framework List*, available at: *https://www.dataprivacyframework.gov/s/participant-search*.

clauses or the binding corporate rules adopted under art. 46 GDPR will persist as appropriate safeguards for personal data transfers outside the EEA.

Despite slight improvements - for greater specification of privacy principles and enforcement assurances from public authorities - deep misgivings remain in the US approach to data protection: the DPF, substantially mirrors foregoing adequacy decisions, presenting various critical issues concerning both corporate data processing[111] and intelligence agency activities. With specific reference to the intelligence agency, EO-14086 emphasises the supremacy of national security, public interest, and the administration of justice, compelling US companies to disregard the DPF if it conflicts with these priorities. The EO-14086 sets out legitimate objectives that justify intelligence activities and specifies situations where such activities are prohibited. However, according to art. 52 of the Charter, restrictions on data subjects' rights must be defined, transparent, and foreseeable. Yet, within the EO-14086, legitimate objectives are vaguely formulated, allowing for broad interpretation and raising doubts about their compatibility with art. 52, as interpreted by the CJUE[112]. Furthermore, to uphold the essence of data subjects' rights, the EO-14086's preference for targeted data collection does not exclude the possibility of mass surveillance[113]. Despite prioritising necessity and proportionality, it lacks measures to prevent bulk collection, which raises concern for the EDPB because of the absence of prior authorization by an independent authority for bulk data processing and the lack of *ex post* judicial or independent authority oversight[114].

[111] Specifically, concerning the identified challenges related to the Data Protection Framework (DPF), the effectiveness of the right of access within the DPF is highlighted as an illustrative example. This right encompasses not only the right of access in its strict interpretation but also the rights of rectification and deletion of data. Additionally, numerous exemptions and limitations to this right exist, yet they lack clarity. The presence of exemptions of a broad nature, such as limitations imposed by judicial orders or to serve public interest, law enforcement, or national security objectives, poses difficulties in determining their precise scope. Consequently, the efficacy of data protection principles could be compromised. Moreover, it is pertinent to underscore the absence of any provisions pertaining to decisions solely reliant on automated processing, along with the requisite safeguards to prevent adverse impacts on data subjects. This deficiency in addressing automated decision-making mechanisms is a significant omission, as it neglects suitable measures essential for safeguarding individuals' rights and freedoms in algorithmic decision-making contexts. See EDPB, *Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework,* 2023, 16-22, available at: https://www.edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf.

[112] Furthermore, these objectives can be altered by the President in response to perceived national security threats, lacking predictability, while Section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333, criticised by the CJEU for enabling excessive intrusions into privacy and not adhering to the proportionality principle, remain unchanged, thus violating Articles 7-8 of the Charter. See M. Giacalone, *Verso Schrems III? Analisi del nuovo EU-US Data Privacy Framework*, in *European Papers*, vol. 8(1), 2023, 152-154, available at: https://doi.org/10.15166/2499-8249/644.

[113] See AA.VV., *Third Time Is the Charm? The Draft Data Privacy Framework for International Personal Data Transfers From the European Union to the United States*, 16-19, 2023, available at: https://ssrn.com/abstract=4477120.

[114] See *ivi*, 19-20; EDPB, *Opinion 5/2023*, cit., 5, 45-52; Despite the establishment of the Data Protection Review Court, concerns persist about effective redress mechanisms for data subjects regarding intelligence agencies. From one hand, the mechanism outlined in the EX- lacks provisions for complainants to access, rectify, or erase their personal data processed by intelligence services, nor does it offer avenues for seeking compensation for damages, undermining the efficacy of redress. On the other hand, placing the Data Protection Review Court within the executive branch raises concerns about potential US Government influence on its judicial activities, potentially compromising the independence and impartiality of the Court, as recognized by the recent interpretation of the ECtHR (Di Giovanni v Italy App no 51160/06 (ECtHR,

3.4 People's Republic of China: the PIPL and standards ruling for cross-border personal information transfer

In recent times, the People's Republic of China (hereinafter: PRC) has implemented a robust legal framework, particularly targeting the technological and ICT sectors, resulting in the introduction of significant regulations concerning information security (such as the Cybersecurity Law of 2016) and data protection (including the Data Security Law of 2021)[115]. This culminated in the enactment of the Personal Information Protection Law, which represents the first comprehensive data privacy legislation dedicated to safeguarding the personal information of individuals (hereinafter: PI)[116].

The Chinese approach to data protection, often described as a middle ground between the privacy-centric European model and the more minimalist US approach[117], places emphasis on the principles that personal information handlers[118] have to comply with: lawfulness, fairness, necessity and good faith, purpose limitation, transparency, accuracy and integrity and accountability[119]. Although these principles seem aligned with European ones, they present significant differences: with regard to the principle of lawfulness, for example, the PIPL provides in art. 14 that consent must be freely given, expressed, and fully informed, but unlike art. 8 GDPR, it does not ensure that this is also specific, making it difficult to exercise withdrawal since the data subject cannot withdraw consent to one element of a general consent form[120].

However, the PIPL also mirrors the GDPR with regards to cross-border data transfers. These transfers are only permitted if the PI processor has obtained a PI protection

9 July 2013)) and the CJEU (Judgement of 8 July 2022, BN v Getin Noble Bank, C-132/20, ECLI:EU:C:2022:235). See M. Giacalone, Verso Schrems III?, cit., 154-156.

115 Of particular mention are the Cybersecurity Law, enacted in the 2016 and covering all the principal aspects linked to the protection of the critical information infrastructure and security review of the network products and services, and the Data Security Act, promulgated on june 2021 and focused primarily on the protection of overall national data security and sets out high-level data management and protection systems and rules for national agencies, industry association, and other organisation. Besides these laws a series of implementation legislation and national standards has been drafted by the Chinese Government. See S. Yang, *Privacy, Data Protection and Cybersecurity: China*, in A.C. Raul (edt.) *Privacy, Data Protection and Cybersecurity Law Review*, 2022, 147-148. For a delve into the Chinese legal-tech framework see V. R. Creemers, *China's emerging data protection framework*, in *Journal of Cybersecurity*, 2022, 4-7, Available at: https://doi.org/10.1093/cybsec/tyac011.

116 According to art. 4 PIPL, personal data are all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymisation treatment.The definition is quite similar to the notion of personal data under art. 4 GDPR, although the latter does not explicitly mention anonymised information.

117 See E. Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?*, in *Penn State Journal of Law & International Affairs Penn State Journal of Law & International Affairs*, vol. 8.1, 2020, 51-55, available at: https://elibrary.law.psu.edu/jlia/vol8/iss1/6/.

118 Even though not expressed in the PIPL they are identified as any organisation or individual that independently determines the purpose and method of processing.

119 Artt. 5-9 PIPL. In particular, the latter provide that personal information handlers shall be responsible for the PI processing activities and take necessary measures to safeguard the security of the personal information they process.

120 Aside from this general consent requirement, the PIPL require a specific and individual consent in these cases: parental consent is required for processing personal information of minors below the age of 14; separate consent is required for the processing of sensitive personal information, providing personal information to third parties, publicising personal information and for PI cross-border data transfer.

certification from a certification body recognized by the Cyberspace Administration of China[121]. The certification structure established by the PIPL bears similarities to the European approach: certification, issued by a third-party entity, is viewed as an external standardisation mechanism separate from national regulations. However, it is legally linked to these regulations through recognition as a method to facilitate cross-border data transfers[122].

Drawing on this framework, the National Information Security Standardization Technical Committee has released the "Cybersecurity Standards Practical Guide – Security Certification Specifications for Cross-Border Processing of Personal Information V2.0". This publication delineates fundamental principles and protocols governing PI protection certification for entities handling data and overseas recipients engaged in cross-border data transfers, alongside measures for safeguarding the rights of data subjects[123]. It is crucial to note that this document does not function as a certification mechanism per se, but rather establishes the groundwork for certification agencies to oversee the cross-border processing activities of PI handlers. Moreover, it furnishes guidance to the latter concerning the regulation of their cross-border processing endeavours associated with PI. Specifically, it delineates the principles that processors and overseas recipients are obliged to adhere to within the framework of the PRC's PI protection regulations.

In the same way as in the European regulation, certifications are a voluntary adherence tool, albeit one capable of enhancing the safeguarding and efficiency of cross-border PI transfers. Indeed, PI handlers and their overseas counterparts are mandated to execute legally binding and enforceable agreements to ensure the protection of the rights and interests of PI subjects. Under this arrangement, the involved parties are obligated to: apprise data subjects of cross-border PI processing activities (including the purpose and extent of such processing); take technical and management measures to prevent possible security risks for PI; respect the rights of PI subjects provided for by the PIPL and introduce methods for them to protect their rights - such as the introduction of an arbitration or a mediation mechanism for dispute resolution; and ensure that the level of PI protection is not lower than China's relevant laws and regulations.[124]. This final provision exemplifies the resemblance between the PIPL and the GDPR. In the European

[121]Article 38 of the PIPL outlines additional conditions required to legitimise data exports. These include undergoing a security assessment organised by the Cyberspace Administration of China (CAC), obtaining certification from an accredited body, or entering into a contractual agreement with the foreign party to ensure compliance with the standards outlined in the PIPL.

[122] The proposed scheme, therefore, should fall within the realm of co-regulation tools.

[123] See National Information Security Standardization Technical Committee, *Security Certification Specifications*, December 2022, Available at: https://www.tc260.org.cn/upload/2022-12-16/1671179931039025340.pdf. For an english translation see Latham & Watkins Privacy & Cyber Practice, *China Clarifies the Personal Information Protection Certification Regime*, 2023, available at: https://www.lw.com/en/people/admin/upload/SiteAttachments/China-Clarifies-the-Personal-Information-Protection-Certification-Regime.pdf. Thus, on March 16, 2023, the NISSTC released the Information security technology-Certification requirements for cross border transmission of personal information, as an official set of standards of the Security Certification Specifications.

[124] See Dezan Shira & Associates, *PIPL 2023/24 Cross-Border Data Transfer in China Handbook*, 2024, 17-23, available at: https://www.asiabriefing.com/store/book/pipl-cross-border-data-transfer-china-handbook.html.

regulatory framework, the assessment of the adequacy of the level of protection is a crucial aspect. This evaluation serves as the basis for the Commission's potential adoption of an adequacy decision, or alternatively, requires data controllers to implement supplementary safeguards, as outlined in Art. 46 GDPR.

As of now, despite its established legal framework, neither China has received an adequacy decision nor has the Commission initiated proceedings to adopt such a decision for the transfer of personal data to China. Additionally, challenges have arisen regarding data transfers from the EU to China, exacerbated by concerns regarding Chinese access to user information on the TikTok platform[125]. These worries prompted the Irish Data Protection Commission (DPC) to commence an inquiry by the end of 2021 into TikTok's transfers of personal data to China and its compliance with the GDPR's stipulations for such transfers to third countries[126].

In conclusion, PRC's multifaceted legal framework appears to align with European principles in several aspects. Notably, the PIPL introduces a certification mechanism for cross-border data transfers, similar to the GDPR. However, China's cybersecurity and market standards authorities have not yet published a list of approved certification bodies or clear guidelines on certification procedures, so further action is needed to clarify how agencies will conduct certifications to ensure compliance by both agencies and target companies.

IV. FINAL REMARKS

Certifications represent a pivotal tool to allow the correct implementation of the principles which so profoundly characterise the new European approach to the protection of personal data. Moreover, they actually demonstrate the general effort to ensure that the entire lifecycle of personal data meets specific guarantees and is always aimed at protecting the individual.

Although a complete and exhaustive study goes beyond the goals of this paper, the relationship between certification schemes and liability of data controllers and processors is worth a brief mention to complete the present overview of certifications. In this context, there are four possible hypotheses: administrative liability, in the event of inspections and possible sanctions by the Data Protection Authority; civil liability, towards the data subject; contractual liability between data controller and data processor; contractual liability, between the certifying body and the certified subject. The GDPR states in a very clear

[125] See J. Czarnocki, F. Giglio, E. Kun, M. Petik, S. Royer, *Government access to data in third countries - Final Report*, 2021, 12-25, available at: https://www.edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf, The authors arrive at the conclusion that the Chinese legal system lacks adequate safeguards for foreigners' data, which are comparable to those found in the EU. Specifically, their analysis of the PRC Constitution, along with secondary legislation, underscores the unrestricted government access to personal data facilitated by China's centralised power structure under the Communist Party of China. Moreover, the prioritisation of national security and public order over privacy protection grants the government broad discretion in accessing personal data.

[126] However, currently there is no information available regarding the ongoing investigations by the DPC on TikTok's compliance with GDPR in relation to the transfer of personal data to China. For a delve see M. Cantero Gamito, *Do Too Many Cooks Spoil the Broth? How EU Law Underenforcement Allows TikTok's Violations of Minors' Rights*, in *Journal of Consumer Policy*, vol. 46, 2023, 281–305, available at: https://doi.org/10.1007/s10603-023-09545-8.

manner that the adoption of certification schemes, although demonstrating compliance with the legislative framework, in no way reduces the liability of the data controller or data processor (see art. 42, par. 4). However, it is undeniable that these mechanisms may reduce exposure and mitigate risks of violations; therefore, they constitute useful elements in the judicial context, to demonstrate that the processing is effectively based on standards of diligence, and this should at least limit the amount of compensation[127] or administrative fines[128].

In addition, the informational value of the certification mark could grant a competitive edge and bolster the reputation of the certified subject[129]. The decision of third parties (such as data subjects, controllers or processors) could be influenced by the publicity of the positive conformity assessment, leading them to place greater trust in the certified subject and its data processing, due to the presence of the certification, and thus giving it a considerable advantage over other competitors[130].

The provision of certifications within the EU regulation on personal data is a novelty, even if a few certification schemes were already present on the European market before the GDPR. This is also true in the US, where the approach based on self-assessment and the adoption of technical models for integrating state legislation has long been adopted in various sectors[131]. To summarise, beyond the territorial context, the certifications can be categorised into: "generic", i.e. addressed to all data controllers regardless of the type of processing actually implemented (see, for example, EuroPriSe©; GDPR-CARPA; ISDP©10003; EuroPrivacy; TRUSTe); "sectoral", i.e. exclusively intended for specific treatments (for example ACCS and AADCS; HITRUST)[132]. A further distinction can be made with reference to the geographical scope of application: some certifications are valid only at a national or regional level, while others are valid in all Member States. Moreover: some certifications are approved by national Data Protection Authorities based on a pre-established regulatory framework; while others have an exclusively inter-private value, usually the result of self-regulation systems. Certification remains intrinsically voluntary: it is, therefore, a suggested but not mandatory tool.

---

127 See G. M. Riccio, *Commento art. 42-43 GDPR*, cit., 609-611; R. Leenes, *Article 42. Certification and Art. 43. Certification bodies*, cit., 751-752.

128 See art. 82, par. 2, lett. j); EDPB, *Guidelines 1/2018*, cit., 6; E. Lachaud, *What GDPR tells about certification*, cit., 7-8.

129 According to some scholars, certification under the GDPR may be considered an instrument of 'trust and confidence'. See L. Bolognini, S. Ziegler, seminar The Mechanism of Certifications with the GDPR - The First European Data Protection Seal: Europrivacy Certification, 2022, available at: https://www.federprivacy.org/attivita/webinar-sul-meccanismo-delle-certificazionicon-il-gdpr-e-il-primo-sigillo-europeo-sulla-protezione-dei-dati. The CNIL, the French SA, already qualifies certifications and codes of conduct as 'confidence indicators'. See CNIL, *Privacy seals*, online: https://www.cnil.fr/en/privacy-seals.

130 See S. SILEONI, *I codici di condotta e le funzioni di certificazione*, cit., 933- 935.

131 See S. Vigliar, *Regole di responsabilità e self-assessment: analisi comparatistica del complesso equilibrio tra diritto e tecnica nei modelli di prevenzione del danno*, in *Cardozo Electronic Law Bulletin*, 2018, 1.

132 See G. M. Riccio, *Commento art. 42-43 GDPR*, cit., 607-609. EU Commission, Directorate-general for justice and consumers, G. Bodea, K. Stuurman, M. Brewczyńska, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: final report*, cit., 35-38.

The comparative analysis may have shown how some systems present mechanisms similar to the one only recently introduced in the EU. This is especially the case in which the regulatory framework presents similarities to the GDPR, for instance in terms of structure and approach to personal data protection regulation. We are therefore referring to the UK, which maintains a regulatory approach similar to the continental one despite Brexit, and to Canada, where the regulatory instruments tend to come closer to the European legal drafting and where the concept of data protection by design was originally established. The US scenario, instead, presents a framework in which the certification tool is certainly weaker, as it is of an intrinsically private nature. This can likely be explained by the lack of a general reference regulation to which the value of the certification scheme could possibly be linked. In the PRC, finally, there is strong control by public authority over data circulation and cross-border data transfer, leading to the adoption of a distinctive certification mechanism.

To sum up, if the GDPR is aimed at finding the proper balance between the protection of the individual's fundamental rights and the free movement of data, the codification of certifications amongst its provisions must be positively welcomed as powerful tools that perfectly advance this goal. As the paper tried to illustrate, at the present stage the tool could be perfected both in terms of more detailed and precise certification criteria and obligations, and with regards to the issuing procedure and audit methods. Some of these aspects are indeed currently left to the discretion of scheme owners and certification bodies. These scenarios require accurate interventions, in order for these tools to effectively work and enhance the transparency and security of processing on a large and general scale. They also play a fundamental role in generating reliance of users on digital services, and therefore guaranteeing that concept of "trust" which is pivotal to many dynamics of the digital world and in particular to the EU ecosystem.