Privacy by design and by default in software development in order to prevent unlawful processing of personal data.

Privacy certifications impact on software development and liabilities.

e-Legal Game

Digital edition 2020-2021

27 September 2021

AUTHORS

Arianna Alessi

Giuseppe Ciccarelli

Luca Cipolli

Lara Guidotti

Annalisa Marsano

TUTOR

Andrei Hanganu

EXECUTIVE SUMMARY

Privacy constitutes a core value of individuals and democratic societies. Due to the evolution in the Information and Communication Technologies (ITC) sector, new challenges to data protection have emerged, leading specifically to intense debates on how this value – and the related legal obligations – should be embedded into ICT systems and software from the very beginning of their design process.

This paper (the "**Paper**") provides a basis for better understanding the current state of the art in the field of privacy by design and by default and of privacy certifications. The Paper aims at bridging the gap between the relevant legal framework and the available technological implementation measures, by providing an inventory of existing privacy-by-design and by-default strategies and approaches, as well as of privacy certification mechanisms of various degrees of maturity, also mapping the allocation of liabilities among the actors involved and underlying all the corporate benefits (even in terms of sustainability) deriving from the adoption of such privacy solutions.

Chapter One analyses the origins and the legal framework of *(a)* **privacy-by-design and privacy-by-default principles** – developed for the first time in the 1990s by Ann Cavoukian, former Ontario's Data Protection Commissioner, and finally embedded in Article 25 and Recital 78 of the General Data Protection Regulation (EU) 2016/679 (hereinafter, "**GDPR**") – requiring that appropriate technical and organizational measures be taken to effectively implement data protection principles at the time the data processing means are determined, but also at the time of the processing itself; and *(b)* **privacy certifications**, as an accountability-based (and, therefore, voluntary) mechanism for data controllers or processors to demonstrate compliance of a processing operation with the GDPR and reduce information asymmetry with data subjects, thus ultimately adding credibility to a company.

In particular, the Chapter provides historical backgrounds, legal definitions but also practical examples in order to guide the reader in understanding the fundamental theoretical concepts underlying the present research, which are further developed, applied and contextualized in the following Chapters. With respect to privacy certifications, a focus is also made on the state of the art of its implementation across EU and certain critical aspects regarding harmonization among Member States in this area are pointed out.

Chapter Two gives an overview of all the most important existing **best practices and guidelines** related to privacy-by-design and by-default principles and certification mechanisms published by national and supranational supervisory authorities, which may help data controllers to overcome the practical difficulties connected to concrete implementation of such measures, considering the broadness of the provisions of the GDPR and the risks of inconsistencies in the national transposition of these provisions by the various EU Member States.

The guidelines analyzed on privacy by design and by default *(a)* provide several examples of existing privacy engineering methodologies useful for their implementation; *(b)* highlight the obligations incumbent on data controllers willing to adopt new solutions and on data processors, in order to ensure full compliance with the GDPR already at the design phase of such solutions; and *(c)* suggest specific steps to be followed for each data processing activity, such as organizing different training

on the GDPR and related legislations based on individuals' roles, defining data protection and information security requirements for any given project, adopting data-oriented design strategies (*e.g.*, "*minimise and limit*", "*hide and protect*", "*separate*", "*aggregate*", "*data protection by default*") or process-oriented strategies (*e.g.*, "*inform*", "*control*", "*enforce*", "*demonstrate*").

As concerns **privacy certifications**, Guidelines No. 1/2018 of the European Data Protection Board and Recommendations of the European Union Agency for Network and Information Security are worth to mention: both provide advice to the relevant stakeholders on, *inter alia*, the definition of certification and accreditation procedures and criteria, the interoperability of privacy certifications with other industrial standards, the establishment of mutual recognition mechanisms between the Member States, in a view to promote a common EU approach. National supervisory authorities have also developed useful guidelines on privacy certifications, such as the Italian Data Protection Authority (see decision No. 148 of 29 July 2020). Despite the existence of such guidance, still the currently available certification schemes related to data protection (*e.g.*, UNI/PDR 43:2018, ISDP 10003:2020, BS 10012/2017) have not been granted the *status* of certification mechanisms under Article 42 GDPR.

Chapter Three takes into consideration the **impact of data protection measures on software development**. After a description of the ways in which software developers may concretely incorporate the privacy-by-design and privacy-by-default principles into software applications and the role that privacy certifications may play in demonstrating GDPR's compliance by such applications, the Chapter focuses on the **allocation of liabilities** according to Article 82 GDPR, in the event that a data breach affects a third-party software processing personal data on behalf of a company, where the company acts as data controller and the software developer as data processor. Even though Article 25 GDPR seems only to expose the controller to the obligation to perform the measures required by the principles of privacy by design and privacy by default, the liability of the processor is actually extremely broad when the controller entrusts him with the data processed (the first legal instrument that allows the shifting of liability to data processor is, indeed, the act of appointment of the processor by the controller pursuant to Article 28 GDPR). In fact, both the controller and the processor are subject to different obligations and, according to the principle of accountability, must be able to prove that they have observed them, thereby giving rise to the division of liabilities under the GDPR. With particular reference to the case of a third-party software, it is possible to state that the company purchasing the software (in the quality of data controller) is liable - starting from the commissioning of a software development - to assess the security measures it intends to adopt and to verify the accuracy of the type of data processed, the procedures adopted with respect to the data management flow and the security of the environment in which data is hosted, whereas the software developer (in the quality of data processor) is liable for offering the data controller a software whose settings can meet the measures the data controller itself decides to adopt.

That said, Chapter Three further shows that, even if the software at issue is provided with a privacy certification, the company and the software developer may be similarly held liable *vis-à-vis* data subjects, as certification mechanisms under Article 42 GDPR **do not act as a ground for exemption but only as a mitigating factor of the enforcement action**. The same goes true even in case the certification has erroneously been issued by the certification body in the absence of the necessary requirements. The latter circumstance seems, however, not able to prevent the data controller or processor to seek adequate compensation – in accordance with the applicable national legislation –

from the certification body for failure to correctly carry out its activities, as resulting from *inter alia* certain EU and Italian case-law.

Finally, **Chapter Four** examines the sustainable value of data protection strategies for those organizations able to integrate privacy-by-design and privacy-by-default methods in their business processes. Indeed, the application of such principles in software development may lead to numerous, interconnected and mutually reinforcing advantages for companies in terms of sustainability. For once, the proper use and processing of big data **support the achievement of the Sustainable Development Goals** (or SDGs) as outlined in the United Nations Development Group's (UNDG) "*Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda*", an instrument of soft law aiming at *(a)* establishing common principles across UNDG to support the operational use of big data for achieving the SDGs; *(b)* serving as a risk-management tool taking into account fundamental human rights; and *(c)* setting principles for obtaining, retention, use and quality control for data from the private sector.

Moreover, this Chapter emphasizes that data protection is increasingly at the centre of public discourse in connection with human rights violations. Modern technologies allow States and business enterprises to conduct surveillance, analyse, predict and even manipulate people's behaviour to an unprecedented degree. As stated in the Guiding Principles on Business and Human Rights, companies have the responsibility to respect human right throughout their activities and business relationships, including supply chains and value. **Privacy-by-design and privacy-by-default principles** – allowing to reduce the data acquired, processed, and stored to the minimum needed – **reduce the risks of violating fundamental human rights** as recognized by the 2018 report of the UN High Commissioner for Human Rights named "*The right to privacy in the digital age*" which enlists these principles as "*essential tools for safeguarding the right to privacy*".

The sustainable advantages of this approach go further. In this regard, Chapter Four suggests that, since most of the companies generally collect more data than they really need to conduct their business operations, by implementing an effective privacy-by-design and privacy-by-default approach, data storage becomes more efficient and less demanding in terms of computing power, thus **saving energy**, allowing faster operations and **boosting companies' green footprint**. In addition, the bigger the amount of personal data (pertaining to customers, stakeholders, employees, etc.) processed, the higher the chances that a **security breach** of IT system may cause significant damages because: *(a)* organizations are seen as high-value targets for cyber adversaries focused on gathering sensitive data and using it for, *inter alia*, blackmail, extortion, identity theft, and other malicious purposes; and *(b)* if the attack is successful a larger number of individuals would be impacted. The implementation of privacy-by-design and privacy-by-default principles, as well as the use of privacy certifications and, ultimately, the outsourcing of software development to third parties able to adopt these data protection measures **allow to shrink the target of cyberattacks**. In addition, these accountability mechanisms make companies more sustainable given that they may **allocate more efficiently the resources in protecting data processed and, in the unfortunate circumstance in which a cyberattack breaches the defence, they are a key to significantly mitigate damages**.

In the light of the above, this Paper ultimately aims to demonstrate that **privacy is a crucial asset from a corporate standpoint**. Despite it could be thought that implementation of data protection measures may expose enterprises to huge costs, it should be considered that these costs may be completely set off by the remarkable benefits produced by GDPR's compliance. Benefits that, as mentioned, do not only count in terms of protection of the interests of a single undertaking, but also and, more importantly, in terms of protection of **fundamental interests of the society as a whole**, such as environment and human rights.

In this respect, it should not be forgotten that the approach to business has been totally re-shaped in the last few years: companies are no longer ranked (only) for their performances or revenues, rather (increasingly) for the **tangible footprint left on the growth and development of the global community**. And such emerging trends are now also taken into account by investors, which are growingly driven by ESG factors in the choice of the best investment transactions, considering **sustainable businesses as a low-risk and long-term return opportunity**.

Therefore, it appears essential for companies to adopt adequate privacy tools in order to operate and compete in this new context. By implementing effective privacy solutions and cybersecurity measures, organizations can stay **ahead of the curve** and, in doing so, **increase attractiveness, competitive advantage, and revenue streams, putting sustainability at the forefront of their business aims**.

To this end, the Paper brings forward the **following proposals**:

(i) data controllers should think about data protection since the earliest stages of planning a processing operation, even before determining the means of processing, developing a specific privacy-by-design strategy and guaranteeing a proper training on the matter for all the involved personnel, according to their respective roles;

(ii) organizations should obtain data protection certifications in order to demonstrate that privacy by design and privacy by default are ensured throughout all the life cycle of their processing activities, as the ability to obtain certified processing represents a competitive advantage for producers, processors and data controllers, as well as increases data subjects' trust in the processing of their personal data; and

(iii) data controllers should choose data processors (including software developers) able to demonstrate how their systems enable compliance with the requirements of privacy by design and privacy by default, specifying in the data processor's appointment act all the security measures the data controller intends to find in the service provided by the data processor.

LIST OF CONTENTS

Chapter 1 – Origins and relevant legal framework of privacy-by-design and privacy-by-default principles and of certification mechanisms. **7**

1.1. Framing the concepts. 7

1.2. European Legal Framework: GDPR provisions. 9

1.3. Privacy certifications under the GDPR. 11

Chapter 2 – Implementation of Privacy by Design, Privacy by Default and certification mechanisms: existing best practices and guidelines. **15**

2.1. Overview of best practices and guidelines for the implementation of privacy-by-design and privacy-by-default techniques. 15

2.1.1. Opinion No. 5/2018 Preliminary Opinion of the European Data Protection Supervisor (EDPS). 15

2.1.2. Guidelines No. 4/2019 of the European Data Protection Board (EDPB). 16

2.1.3. Report and Recommendations of the European Union Agency for Network and Information Security (ENISA). 20

2.1.4. Guidelines issued by Spanish and Norwegian Data Protection Authorities. 24

2.2. Overview of best practices and guidelines concerning privacy certifications. 28

2.2.1. Guidelines no. 1/2018 of the European Data Protection Board (EDPB). 28

2.2.2. Recommendations of the European Union Agency for Network and Information Security (ENISA). 31

2.2.3. Available certification schemes for data protection. 31

2.2.4. Data protection certification in Italy. 33

2.2.5. Codes of Conduct. 34

Chapter 3 – Impact of data protection measures on software development: where does liability stand? 35

3.1. The interplay between data protection measures and software development. 35

3.2. The treatment of liability under the GDPR. 36

3.3. Who is responsible for infringements of privacy-by-design and privacy-by-default measures in software developments? 38

3.4. How is the allocation of liability affected by certification mechanisms? 40

Chapter 4 – The path towards data sustainability. 44

4.1. A sustainable development approach to data protection. 44

4.2. Data sustainability: a green footprint. 46

4.3. Data sustainability: protection of human rights. 48

4.4. Data sustainability: cybersecurity. 50

Conclusions. 52

Bibliography……..54

1. Origins and relevant legal framework of privacy-by-design and privacy-by-default principles and of certification mechanisms.

1.1. Framing the concepts.

Since the 1970s the academia, and most prominently David Chaum, explored the field of technologies with embedded privacy features, which started to be proposed from the 1980s. In particular, the term "privacy-enhancing technologies" (PETs) was introduced for a category of technologies that minimizes the criticism connected to the processing of personal data[1]. By using PETs, indeed, the risks for the users' informational privacy would decrease and the legal data protection obligations of the entities responsible for the data processing would be fulfilled more easily.

In this spirit, in 2007 the European Commission issued a Communication[2] to promote PETs, and privacy-enhancing technologies have become a field of their own not only within computer science, computer security and cryptography, but also of law, social sciences or economics. However, the mere existence of PETs concepts or implementations has been proven insufficient to extensively address the challenge of supporting the individual's right to privacy; privacy cannot be exclusively guaranteed by technology, let alone by a few PETs components embedded in a bigger ICT (Information and Communication Technologies) system.

Privacy needs to be considered from the very beginning of system development. For this reason, in the 1990s a conceptual development was provided by Ann Cavoukian, former Ontario's Data Protection Commissioner[3], who developed for the first time the principles of "Privacy by Design" (hereinafter, "**Privacy by Design**" or "**PbD**") and "Privacy by Default" (hereinafter, "**Privacy by Default**") and later presented them at the 31st International Conference of Data Protection and Privacy Commissioners in 2009[4]. These principles were eventually internationally accepted at the 32nd International Conference of Data Protection and Privacy Commissioners, held in Jerusalem in 2010, with the adoption of the "*Resolution on Privacy by Design*"[5]. By this resolution, the principles of Privacy by Design and Privacy by Default were adopted as "*a holistic concept that may be applied*

[1] According to Article 4(1) of GDPR: "*'personal data' means 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, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

[2] Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), dated 2 May 2007, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52007DC0228 (last access to this link and all the other links included in this Paper on 17 September 2021).

[3] A. Cavoukian, *Creation of a Global Privacy Standard*, 8 November 2006, available at: http://www.ehcca.com/presentations/privacysymposium1/cavoukian_2b_h5.pdf.

[4] A. Cavoukian, *Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D*, 18 May 2010, available at: https://link.springer.com/content/pdf/10.1007%2Fs12394-010-0062-y.pdf.

[5] Resolution on Privacy by Design. 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem (Israel), 27-29 October 2010, available at: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf.

to operations throughout an organization, end-to-end, including its information technology, business practices, processes, physical design and networked infrastructure".

Ann Cavoukian defined Privacy by Design as the implementation of a project that considers the protection of personal data and privacy from the beginning, starting from the creation of the product or the execution of a service. The privacy-by-design framework employs an approach that is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. Privacy by Design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after[6].

In light of the above, for the sake of clarity, it is preliminarily useful to explain the interconnected concepts of Privacy by Design and Privacy by Default.

Privacy by Design refers to the practices of companies and organisations that aim at implementing technical and organisational measures, at the earliest stages of the design of the processing operations, in such a way that safeguards privacy and data protection principles from the start. For example, common tools to achieve such result are the use of pseudonymisation (*i.e.*, replacing personally identifiable material with artificial identifiers) and encryption (*i.e.*, encoding messages so only those authorised can read them).

Privacy by Default underlines the obligations of companies and organizations to ensure that personal data is processed with the highest level of privacy protection (for example, acquiring the minimum amount of personal data necessary for the process, limiting the storage period or the accessibility on a need-to-know basis), so that – by default – personal data is not made accessible to an indefinite number of persons. For instance, a social media platform should set users' profile default settings in the most privacy-friendly way by, for instance, limiting from the beginning the accessibility of the users' profile to the maximum possible extent. Therefore, Privacy by Default implies that personal data is protected automatically, even in the absence of intervention by the data subject, who has the possibility of changing the chosen option.

A practical example could be useful to better understand the above concepts. If a software development enterprise wishes to publish a basic calculator application, which can be downloaded and installed on smartphones, such application would not be compliant with the Privacy by Default principle if it requires users to allow the application to track their location as, clearly, the functionality of the application objectively does not need this access for the intended function. Further, let's assume that the application contains some PRO features that can be activated only by paying a certain amount. In such case, the Privacy by Default principle would not be respected in the case the application requires users to insert their credit cards' numbers and their personal information (name and address) by default, even if they just use the free version of the application.

The two concepts of Privacy by Design and Privacy by Default – which, as mentioned, are closely interconnected, complementary, mutually reinforcing each other – have been adopted by the EU legislation, and finally embedded in Article 25 and Recital 78 of the GDPR.

[6] A. Cavoukian, *Privacy by Design. The 7 Foundational Principles*, January 2011, p. 2, available at: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

1.2. European Legal Framework: GDPR provisions.

Tracing back in time, some elements of the principles of Privacy by Design and Privacy by Default can already be found in the Data Protection Directive 1995/46/EC (hereinafter, "**Directive**"): indeed, Recital 46 of the Directive highlights how the technical and organisational measures to be taken to protect rights and freedoms of people whose data is processed should be applied "*both at the time of the design of the processing system and at the time of the processing itself* [...]". The Directive was at last repealed and replaced by the more recent GDPR.

Recital 78 of the GDPR states that controllers should adopt internal policies and implement measures which meet, in particular, the principles of data protection by design and data protection by default in order to demonstrate compliance with the GDPR itself. Such measures are enlisted in a non-exhaustive manner, and encompass: minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. On the basis of this Recital, it can be said that public entities, when awarding contracts in public tenders, should prefer companies that provide products or services developed on the basis of the principles of Privacy by Design and Privacy by Default.

These statements are then articulated under Article 25 of GDPR, which is included in the Chapter defining the general obligations of the controllers[7], under the heading "*Data protection by design and by default*", and it incorporates into data protection rules the practice of considering privacy requirements from the first stages of product and service design. It therefore confers to it the status of a legal requirement having the rationale of protecting citizens' rights and freedoms with regard to their personal data from the early development stages of systems and products.

In particular, pursuant to Article 25(1) GDPR ("*Data Protection by Design*"), appropriate technical and organizational measures must be taken to effectively implement data protection principles at the time the data processing means are determined, but also at the time of the processing itself. Moreover, the necessary safeguards shall be integrated into the processing in order to meet the requirements of the GDPR and to protect the rights of data subjects at all times.

From this provision, it can be noted that it is not possible to identify an optimal predefined conduct, but a case-by-case analysis should be carried out in order to select the best course of action in each case, with a risk management approach and the balancing of the different elements listed in the article, namely: "*state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing"*.

A systematic and thorough evaluation of the processing is crucial when doing risk assessments, however timing is also important. Data protection by design shall be implemented "*at the time of*

[7] According to Article 4(7) of the GDPR 'controller' means "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*".

determination of the means for processing". Such time refers to the period when the controller is deciding how the processing will be conducted, the manner in which the processing will occur and the mechanisms which will be used to conduct such processing. It is of course in the controllers' best interest from a cost-benefit perspective, to take such principles into account sooner rather than later, as it could be challenging and costly to make later changes to plans.

The effective implementation of the principles shall be a priority also once the processing has started and during its whole life. The nature, scope and context of processing operations, as well as the risk may change over the course of processing, which means that controller must re-evaluate their processing operations through regular reviews and assessments of the effectiveness of their chosen measures and safeguards.

Moving forward, Article 25(2) GDPR ("*Data Protection by Default*") sets forth requirements for the pre-settings, or "default" settings, of technical and organizational measures of the controller so that the only personal data which is strictly necessary for each specific purpose of the processing is actually processed. In accordance with Article 6 GDPR, this applies in decisions concerning the amount of personal data collected, the period of its storage, and its accessibility.

The mentioned provision is particularly important in the circumstances controllers rely on third-party software or off-the-shelf software; in such case, the controller should carry out a risk assessment of the product and make sure that functions that do not have a legal basis or are not compatible with the intended purposes of processing are switched off.

Finally, Article 25(3) GDPR provides that a certification under Article 42 GDPR may be used to demonstrate compliance with the principles of data protection by design and by default, also in relation to the underlying technical and organizational measures (for a more detailed analysis on privacy certifications see Paragraph 1.3 below).

On a more systemic basis, it is important to underline that the data protection by design and by default requirements of Article 25 complement the controller's responsibility laid down in Article 24, a fundamental provision of the GDPR that regulates the "*Responsibility of the controller*". This article defines "who shall do what" to protect individuals and their personal data and establishes that a risk-based approach shall be adopted to identify what needs to be done to that purpose. More precisely, it provides for the controller to "*implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance* [...]*"* with the law. Again, these measures shall be designed "*taking into account the state of the art, the cost of implementation and 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*". It is in the balancing of these elements that the controllers may demonstrate their compliance with the GDPR.

Conclusively, in order to complete the framework in which the principles of data protection by design and by default operate, it must not be forgotten that the controllers' conduct in processing personal data shall, at all time, be informed by and compliant with the general principles outlined in Article 5 and Recital 39 of the GDPR, namely:

(i) Transparency: controllers shall clearly inform the data subjects about how they will collect, use and share personal data;

(ii) Lawfulness: the controller must identify a valid legal basis for the processing of personal data;

(iii) Fairness: an overarching principle which requires that personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data;

(iv) Purpose limitation: controllers must collect data for specified, explicit, and legitimate purposes, and not further process the data in a manner that is incompatible with the purposes for which data was collected;

(v) Data minimisation: only personal data that is adequate, relevant and limited to what is necessary for the intended purpose shall be processed;

(vi) Accuracy: personal data shall be accurate and kept up to date, and every reasonable step shall be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;

(vii) Storage limitation: data that allows for identification of the data subjects shall not be held for no longer than is necessary for the purposes for which personal data is processed;

(viii) Integrity and confidentiality: controllers should secure the protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

(ix) Accountability: controllers shall be responsible for and be able to demonstrate compliance with all of the abovementioned principles.

1.3. Privacy certifications under the GDPR.

In terms of accountability, an important role is played by privacy certifications, whose establishment is encouraged by Recital 100 of the GDPR.

GDPR introduces certification as a means for a data controller or processor to *(a)* demonstrate compliance of a processing operation with the GDPR; and *(b)* enhance transparency and reduce information asymmetry, since certifications, seals, and marks allow data subjects to "*quickly assess the level of data protection of relevant products and services*" (Recital 100 of the GDPR). In fact, certifications can add credibility to a company, as an element which may be used in order to demonstrate to its customers that processing of their personal data is conducted in compliance with the GDPR. Certifications could also reward privacy-aware technologies and offer a competitive advantage on the market to these technologies to the extent that they implement a specific processing operation which is compliant with the GDPR.

Under Article 42 of the GDPR, a certification mechanism must be granted in relation to processing activities, even in case such activities are an integral part of a product, system or service (*e.g.*, certification of data deletion process in product X)[8].

[8] European Union Agency for Network and Information Security, *Recommendations on European Data Protection Certification*, 27 November 2017, p. 15, available at:

As mentioned, the concept of certification is deeply connected to the newly introduced principle of accountability. Indeed, certifications and seals "*are treated as accountability-based mechanisms, due to their potential effect to facilitate scalability, compliance, transparency, and to some extent legal certainty*"[9]. The GDPR strongly emphasizes the concept of "accountability" of data controllers and processors, intended as the adoption of proactive behaviours that demonstrate the concrete adoption and implementation of measures aimed at ensuring the application of the GDPR. This is a great novelty for data protection as it entrusts data controllers with the task of deciding autonomously – in compliance with regulatory provisions and in the light of some specific criteria indicated in the GDPR – on the modalities, guarantees and limits of processing personal data. Moreover, the great attention on accountability required by certification mechanisms facilitates the transition from an *ex ante* to an *ex post* enforcement approach, since "*controllers are required to assess the risks arising from the processing operations and to implement appropriate and effective measures in order to show the compliance with the GDPR*" [10].

The GDPR does not define "*certification mechanisms, seals or marks*" and uses these terms collectively. A certificate is a statement of conformity. To have any clue on that, reference could be made to the definition of certification provided by the International Standards Organization (ISO) as "*the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements*"[11]. On the other hand, a "*seal or mark commonly refers to a logo or symbol whose presence (in addition to a certificate) indicates that the object of certification has been independently assessed in a certification procedure and conforms to specified requirements, stated in normative documents such as regulations, standards or technical specifications*"[12].

Pursuant to Article 42(3) of the GDPR, certification shall be voluntary, as it represents an accountability-based mechanism. Indeed, certifications are not aimed at eliminating or reducing the responsibility of the data controller or the data processor for compliance with GDPR (Article 42, paragraph 4, of the GDPR) but, rather, at certifying that – in a given period of time – a data controller or a data processor have adopted and implemented certain measures to ensure compliance of a specific processing operation with the GDPR. Specifically, certifications may be used to demonstrate compliance with, *inter alia*:

(i) the obligations of the data controller to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR (Article 24(1 and 2));

(ii) the provisions related to data protection by design and by default (Article 25);

---

https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification.

[9] *Id.*, p. 13.

[10] Directorate – General for Justice and Consumers Unit C.3 Data Protection and Unit C.4 International Data Flows and Protection, *Data Protection Certification Mechanisms. Study on Articles 42 and 43 of the Regulation (EU) 2016/679. Final Report*, February 2019, p. 16, available at: https://ec.europa.eu/info/sites/default/files/data_protection_certification_mechanisms_study_final.pdf.

[11] Available at: https://www.iso.org/certification.html.

[12] European Data Protection Board, *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*, version 3.0, 4 June 2019, p. 8, available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf.

(iii) the obligation of the data processor to provide sufficient guarantees to the controller (Article 28(5)); and

(iv) the provisions related to security of processing (Article 32).

If, on one hand, a certification may not serve *per se* as an exemption from liability of the data controller or data processor under the GDPR, on the other hand, the adherence to approved certification mechanisms is a factor supervisory authorities shall take into account as aggravating or mitigating circumstance when deciding whether to impose an administrative fine and on the amount of such administrative fine (Article 83(2), letter (j), of the GDPR).

The certification mechanism pursuant to Articles 42 and 43 of the GDPR involves the following actors:

(i) the data controller or data processor applying for certification;

(ii) the certification body;

(iii) the supervisory authority; and

(iv) European Data Protection Board.

In particular, under Article 42(5) of the GDPR a certification "*shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority*". The GDPR does not provide any specification on the circumstances under which the certification process is conducted by a certification body and those under which it is conducted by a supervisory authority. As typical in EU law, Member States and national supervisory authorities are free to organize certification at national level[13]. Of course, this freedom of Member States and national supervisory authorities may result in a risk of fragmentation of the certification mechanisms among Member States which could also affect to some extent the cross-border recognition of certifications (for an overview of best practices and guidelines aimed at overcoming such risk, see Chapter 2).

Article 42(5) of the GDPR provides that a certification shall be issued on the basis of criteria approved by the competent supervisory authority or by the European Data Protection Board (hereinafter, the "**EDPB**"). Where the criteria are approved by the EDPB, this may result in a common certification, the European Data Protection Seal (hereinafter, the "**EU Seal**"). Even though at the present date, an EU Seal has not been developed yet, it must be noted that its adoption would of course facilitate harmonization of certification criteria among Member States.

As mentioned, the GDPR does not make the issuance of certifications a mandatory task of the supervisory authorities. Instead, it allows for a number of different models. For example, a supervisory authority may decide for one or more of the following options:

(i) issuing certification itself, in respect of its own certification scheme;

(ii) issuing certification itself, in respect of its own certification scheme, but delegating whole or part of the assessment process to third parties;

[13] European Union Agency for Network and Information Security, 27 November 2017, *op. cit.*, p. 14.

(iii) creating its own certification scheme, and entrusting certification bodies with the certification procedure; and

(iv) encouraging the market to develop certification mechanisms[14].

Pursuant to Article 42(7) of the GDPR, certification shall be valid for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. In case of loss of the relevant requirements, certification shall be withdrawn.

Article 43 of the GDPR is devoted to certification bodies. In particular, this Article emphasizes the importance of having reliable, competent, and independent bodies carrying out the certification. In this respect, it is required that the certification bodies that provide data protection certifications are accredited by the national accreditation body or by the competent supervisory authority[15].

GDPR allows each Member State to determine who should be responsible to conduct the assessment leading to accreditation. In this regard, accreditation may be conducted:

(i) solely by the supervisory authority, on the basis of its own requirements;

(ii) solely by the national accreditation body appointed in accordance with Regulation (EC) 765/2008 and on the basis of ISO/IEC 17065/2012 and with additional requirements established by the competent supervisory authority; or

(iii) by both the supervisory authority and the national accreditation body (and in accordance with all requirements listed in No. (ii) above).

In conclusion, as it emerges from the above analysis, despite the recognized value and importance of privacy certifications, the applicable legal framework has still several gaps to be filled and full harmonization seems to be a far target.

[14] European Data Protection Board, *op. cit.*, p. 9.

[15] The GDPR does not define "accreditation". Article 2(10) of Regulation (EC) No. 765/2008, which lays down general requirements for accreditations, defines accreditation as "*an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity*".

2. Implementation of Privacy by Design, Privacy by Default and certification mechanisms: existing best practices and guidelines.

2.1. Overview of best practices and guidelines for the implementation of privacy-by-design and privacy-by-default techniques.

Article 25 of GDPR does not specify which measures the data controller should adopt in order to ensure that the processing of personal data meets – by design and by default – the GDPR's requirements, creating difficulties for its enforcement[16].

Given the complexity of putting these abstract legal principles into practice, several guidelines have been published by national and supranational supervisory authorities, to provide data controllers with useful recommendations on how to successfully implement such principles and identify the relevant best practices.

2.1.1. Opinion No. 5/2018 Preliminary Opinion of the European Data Protection Supervisor (EDPS).

On 31 May 2018, the European Data Protection Supervisor (hereinafter, the "**EDPS**"), with the aim of clarifying the steps that must be taken to achieve a privacy-by-design approach, as referred to in Article 25 of GDPR, published a "*Preliminary Opinion on Privacy by Design*" (hereinafter, the "**Opinion**")[17].

First of all, the Opinion analyses the obligations related to the principle of Privacy by Design, identifying four dimensions:

(i) any processing of personal data carried out, in whole or in part, with the help of IT systems should be the result of careful design, where safeguards for data subjects' rights should be taken into account both at the design stage and during the operational stage;

(ii) as there is no indication of mandatory security measures in the GDPR, companies should adopt a risk-based approach in order to select and implement the measures concretely needed to achieve an effective level of protection. In this respect, each organization is responsible for the choice of safeguards to be implemented, balancing the costs of the available measures (the "*state of the art*") against the risks to individuals' rights and freedoms that have been so identified. In any event, cost considerations can never lead to insufficient protection for individuals;

[16] L. A. Bygrave, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, in OSLO LAW REVIEW, Volume 4, No. 2-2017, pp. 105–120.

[17] European Data Protection Supervisor, *Opinion 5/2018. Preliminary Opinion on privacy by design*, 31 May 2018, available at: https://edps.europa.eu/sites/default/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

(iii) the measures identified must be adequate and effective, in the light of their purpose, which is to put into practice the data protection principles (*e.g.*, the principle of transparency, the subjective rights of data subjects, data minimization); and

(iv) the measures thus identified must be integrated within the processing itself, and not consist of merely "external" measures (such as privacy notices).

Furthermore, the Opinion provides several examples of existing privacy engineering methodologies useful for companies in implementing Privacy by Design and Privacy by Default:

(i) the "*Recommendations on Privacy and Data Protection by Design*", published in 2015 by the European Union Agency for Network and Information Security (hereinafter, "**ENISA**")[18], which provides a comprehensive overview of the state of the art in this field;

(ii) the "*Six protection goals for privacy engineering*", which provides a framework to identify safeguards for IT systems processing personal data and adds, besides the classical IT security triad of "confidentiality", "integrity" and "availability", three additional goals: "unlinkability", "transparency" and "intervenability";

(iii) the "*Introduction to Privacy Engineering and Risk Management in Federal Systems*", published by the National Institute of Standards and Technology (NIST)[19], which identifies a privacy risk model and three privacy system objectives on top of the classical security objectives represented by confidentiality, integrity and availability: predictability, manageability and disassociability. These three objectives help engineer systems to meet the privacy principles;

(iv) the "*LINDDUN Methodology*" developed by the University of Leuven[20], which emphasizes in particular the risk analysis aspects, complemented by a list of technology-neutral strategies that should be implemented to address the risks;

(v) the identification of "patterns" to engineer IT solutions to implement privacy requirements. This methodology draws inspiration from software development: design strategies are identified for commonly recurring privacy issues, and these issues can be broken down into further, more specific layers, if necessary[21].

2.1.2. Guidelines No. 4/2019 of the European Data Protection Board (EDPB).

On 20 October 2020, the European Data Protection Board (hereinafter, the "**EDPB**") adopted "*Guidelines No. 4/2019 on Article 25 Data Protection by Design and by Default*" (hereinafter, the "**Guidelines**")[22].

---

[18] European Union Agency for Network and Information Security, *Privacy and Data Protection by Design – from policy to engineering*, December 2014, published on 12 January 2015, available at: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.

[19] NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, January 2017, available at: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.

[20] University of Leuven, LINDDUN Methodology, see more at: https://www.linddun.org/.

[21] A list of such models is available at: https://privacypatterns.eu.

[22] Available at:

The Guidelines provide general guidance on the obligation to protect data by design and by default as better provided for in Article 25 of the GDPR. This is an obligation that concerns all data controllers, regardless of the size and complexity of the data processing.

The Guidelines analyse Article 25(1) of the GDPR, which provides for the principle of "Data protection by design". By virtue of this principle, the appropriate technical and organisational measures and the necessary safeguards adopted by the data controller are aimed at protecting the rights and freedoms of data subjects and ensuring that the protection of their personal data is integrated into the processing carried out.

Such appropriate technical and organisational measures and the necessary safeguards can be considered in a broad sense as any method or means that a data controller may employ in the processing. "Appropriate" means that the necessary measures and safeguards shall be suitable to achieve the purpose pursued, namely, to ensure compliance with data protection principles.

It is therefore understood that the requirement of adequacy is closely related to the requirement of effectiveness. In this respect, it is necessary to remind that a technical and organisational measure may be of any nature and may consist in adopting advanced technical solutions, staff training, pseudonymisation of personal data, storing available personal data in a structured and commonly computer-readable format, having malware detection systems in place, and so on.

Standards, best practices and codes of conduct recognised by associations and other bodies representing categories of data controllers may be helpful in determining appropriate measures. However, it is necessary for the data controller to assess the adequacy of the measures to be put in place taking into account the processing in question.

According to the EDPB, the adoption of appropriate technical and organisational measures is connected to the effective implementation of each of the general data protection principles under Article 5 of GDPR. Indeed, the concept of effectiveness is at the heart of Privacy by Design. This implies that the data controller, taking into account the context of the processing, should adopt specific and robust security measures and should be able to implement additional ones to reduce a potential increase in risk.

Furthermore, the data controller should be able to demonstrate (accountability principle) that it has put in place all technical and organisational measures to ensure compliance with the data protection principles set out in the GDPR. In this regard, the Guidelines suggest that, to this end, the data controller may determine the collection of so-called key performance indicators (KPIs) to demonstrate the effectiveness with which the data controller ensures data protection. KPIs can be quantitative (*e.g.*, reduction in complaints, reduction in response time when data subjects exercise their rights) or qualitative (*e.g.*, performance appraisals, expert evaluations). As an alternative to KPIs, the data controller can demonstrate the effective implementation of data protection principles by providing the rationale behind the assessment of the effectiveness of the chosen measures and safeguards.

---

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

The Guidelines then examine the elements referred to in Article 25(1) GDPR, which the data controller should take into account when determining measures for a specific processing operation:

(i) "*state of the art*": in the EDPB's view, it is a dynamic concept that cannot be statically defined at a given moment but must be constantly assessed in the context of technological progress. This criterion applies not only to technological measures, but also to organisational ones, since the lack of appropriate organisational measures – such as the adoption of internal governance policies, up-to-date training on technology, security management – can reduce or even undermine the effectiveness of a chosen technology;

(ii) "*the costs of implementation*" in selecting and applying appropriate technical and organisational measures: costs refer to resources in general, such as time and human resources;

(iii) "*the nature, scope, context and purposes of the processing*": the concept of "*nature*" concerns the intrinsic characteristics of the processing, while "*scope*" concerns the size and range of the processing. The "*context*" relates to the circumstances surrounding the processing which are likely to affect the data subject's expectations, while "*purposes*" relates to the aims of the processing;

(iv) "*risks of varying likelihood and severity to the rights and freedoms of natural persons arising from the processing*": the data controller must identify the risks that a potential breach of the principles might entail for the rights of data subjects and must determine their likelihood and severity in order to take appropriate measures to reduce and/or eliminate the risks identified; and

(v) temporal aspect: Article 25 of the GDPR provides that Privacy by Design shall be implemented "*both at the time of determining the means of processing and at the time of processing itself*". The reference to the "*moment of determining the means*" is interpreted as the period of time in which the data controller establishes the modalities in which the processing will be carried out and the most appropriate security measures for the purpose of effectively applying the principles enshrined in the GDPR and protecting the rights and freedoms of data subjects. The reference to "*at the time of the processing itself*" means that, once the processing has started, the data controller is required to regularly assess and evaluate the effectiveness of the chosen measures and safeguards. This obligation extends to any processing carried out by data processors, including those related to systems designated prior to the entry into force of the GDPR.

With regard to Article 25(2) of the GDPR on Privacy by Default, the EDPB states that the term "*by default*" in the processing of personal data refers to choices concerning configuration values/options set in a processing system (*e.g.*, software, devices, manual processing procedures). The data controller should choose and be responsible for implementing the default settings of a processing operation so that only processing that is strictly necessary to achieve the intended purpose is lawful. This means that – by default – the controller should not collect/process/store more data than it is necessary for the purposes set. The controller must predetermine for which specific, explicit and legitimate purposes personal data is collected and processed. Measures must be by default adequate to ensure that only personal data – necessary for each specific purpose of processing – is

processed. In addition, the EDPB explains that where the data controller uses third-party software, he/she must carry out a risk assessment of the product and ensure that functions that do not have a legal basis or are not compatible with the intended purpose of the processing are deactivated. The same considerations apply to organisational measures concerning processing: these should be designed to process only the minimum amount of personal data necessary for specific operations.

Article 25(3) of the GDPR provides for the possibility of using certification under Article 42 to demonstrate compliance with data protection by design and by default. In such a case, according to the EDPB, the elements that contribute to demonstrating compliance with Article 25(1) and (2) are the processes for determining the means of processing, governance and the technical and organisational measures to implement the data protection principles. The EDPB also points out that even if a processing operation is certified under Article 42, the data controller has an obligation to continuously monitor and ensure compliance with the criteria set out in Article 25.

Finally, the EDPB provides a series of recommendations to data controllers and processors in order to facilitate the implementation of the principles of Privacy by Design and Privacy by Default. Among these recommendations, the following are worth mentioning:

(i) data controllers should think about data protection since the earliest stages of planning a processing operation, even before determining the means of processing;

(ii) where a data controller employs a Data Protection Officer (DPO), the EDPB encourages the active involvement of the DPO with a view to integrate Privacy by Design and Privacy by Default into the procurement and development procedures, as well as into the whole lifecycle of the processing;

(iii) processing can be certified. The ability to obtain certified processing provides added value to the data controller when choosing between different processing software, hardware, services and/or systems from producers or data processors. Therefore, producers should demonstrate that Privacy by Design and Privacy by Default are ensured throughout the life cycle of their processing systems. The presence of a certification could also guide data subjects in their choices between different goods and services. As such, having the ability to obtain certified processing may represent a competitive advantage for producers, processors and data controllers, as well as increase data subjects' trust in the processing of their personal data;

(iv) producers and data processors should seek to facilitate the implementation of Privacy by Design and Privacy by Default in order to support the data controller's ability to comply with its obligations under Article 25. Therefore, data controllers should not choose manufacturers or data processors who do not offer systems that enable or support data controllers to comply with Article 25, as the latter may incur responsibility for failure to implement Article 25;

(v) manufacturers and data processors should play an active role in ensuring that the criteria for "*State of the Art*" are met and notify data controllers of potential changes to that state as they may affect the effectiveness of the measures put in place;

(vi) the EDPB recommends that data controllers require manufacturers and data processors to demonstrate how their hardware/software/services/systems enable compliance with the accountability requirements for Privacy by Design and Privacy by Default (*e.g.*, by using

specific key performance indicators to demonstrate the effectiveness of the safeguards in place);

(vii) the EDPB also stresses the need for a harmonised approach to implement principles and rights effectively, and encourages associations or bodies to develop codes of conduct under Article 40, including specific guidance on Privacy by Design and Privacy by Default; and

(viii) data controllers must be fair to data subjects and transparent about how they assess and ensure data protection by design and by default in implementation of the GDPR's accountability principle.

2.1.3. Report and Recommendations of the European Union Agency for Network and Information Security (ENISA).

On 12 January 2015, ENISA published a report on "*Privacy and Data Protection by Design – from policy to engineering*" (hereinafter, the "**Report**")[23].

The Report provides an overview of the ways in which businesses have implemented the principle of Privacy by Design into their products and services. To this end, the Report reviews existing approaches and strategies to implement Privacy by Design. In particular, the Report distinguishes between data-oriented strategies and process-oriented strategies.

Data-oriented strategies are:

(i) *Minimise*: the most basic privacy-by-design strategy is minimising, meaning that the amount of processed personal data should be restricted to the minimum possible extent;

(ii) *Hide*: the second privacy-by-design strategy states that any personal data, and its interrelationships, should be hidden from plain view. The rationale behind this strategy is that by hiding personal data from plain view, it cannot easily be abused;

(iii) *Separate*: the third design strategy states that personal data should be processed in a distributed fashion, in separate compartments whenever possible. By separating the processing or storage of several sources of personal data belonging to the same person, it would not be possible to obtain complete profiles of one person; and

(iv) *Aggregate*: the fourth privacy-by-design pattern states that personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful. Aggregation of information over groups of attributes or individuals restricts the degree of detail in the personal data that remains.

Process-oriented strategies are:

(i) *Inform*: this strategy corresponds to the important notion of transparency and states that data subjects should be adequately informed whenever personal data is processed;

[23] European Union Agency for Network and Information Security, December 2014, *op. cit.*.

(ii) *Control*: this strategy states that data subjects should be able to supervise the processing of their personal data. Control goes beyond the strict implementation of data protection rights, however. It also governs the means by which users can decide whether to use a certain system, and the way they monitor what kind of information is processed about them;

(iii) *Enforce*: according to the seventh strategy, a privacy policy compatible with legal requirements should be in place and enforced. This relates to the accountability principle and ensures that a privacy policy is in place. This is an important step in ensuring that a system respects privacy during its operation; and

(iv) *Demonstrate*: the final strategy requires a data controller to be able to demonstrate compliance with the privacy policy and any applicable legal requirements.

The Report gives a structured overview of some important privacy techniques, including the following ones:

(i) *Authentication*: user authentication is the process by which users in a computer system are securely linked to principals that may access confidential information or execute privileged actions. Once this link is securely established, communications can proceed on the basis that parties know each other's identity and a security policy can be implemented. Authentication is key to securing computer systems and is usually the very first step in using a remote service or facility and performing access control. Strong authentication may also be a key privacy mechanism when used to ensure that only a data subject, or authorised parties, may access private information;

(ii) *Secure private communications*: all types of communications from the user should be protected; personal information or sensitive user input should be encrypted to preserve its privacy (and security);

(iii) *Communications anonymity and pseudonymity*: end-to-end encryption may be used to protect the content of communications but leaves meta-data[24] exposed to third parties. In this regard, ENISA mentions several methodologies that can also hide meta-data;

(iv) *Storage privacy*: storage privacy refers to the ability to store data without anyone being able to read them, except the party having stored the data and whoever the data owner authorises. User authentication and access control lists managed by the operating system are the most common way to guarantee some level of storage privacy;

(v) *Transparency-enhancing techniques*: transparency-enhancing techniques cannot be realised by technological tools alone but need to be intertwined with processes that provide the necessary information. Since transparency in this context aims at individuals' understanding of data processing and related risks to provide a fair basis for informational self-determination, specific attention has been paid to usability as well as accessibility and inclusion when designing transparency mechanisms and determining the ways to communicate information; and

[24] Meta-data is information "about" the communication, such as who is talking to whom, the time and volume of messages, the duration of sessions or calls, the location and possibly identity of the network end-points.

(vi) *Intervenability-enhancing techniques*: "intervenability" means the possibility to intervene and encompasses control by the user, but also control by responsible entities over contractors performing data processing on their behalf. For Privacy by Design, it is essential to assist users and support their intervention possibilities.

Later, on 28 January 2019, ENISA published its "*Recommendations on shaping technology according to GDPR provisions. Exploring the notion of data protection by default"*[25] (hereinafter, the "**Recommendations**"), in which it highlighted the different types of obligations incumbent on data controllers willing to adopt a new solution and those incumbent on producers of services and applications (such as software).

In fact, while the GDPR expressly requires data controllers to process data on the basis of a privacy-by-design approach, there is no direct obligation under the GDPR for producers of products, services and applications, but they should support data controllers in achieving full compliance with the GDPR, in turn ensuring proper design and implementation of pre-settings. Therefore, according to ENISA, producers of services and applications should refrain from using design patterns that may lead to pre-settings or choices that do not comply with the fundamental principles laid down in the GDPR as well as the relevant best practices, and instead ensure that they incorporate adequate security and data protection measures into their designs and provide appropriate guidance and support to data controllers and end-users.

The Recommendations give great importance to the design phase of IT systems or services as well as to the default properties and functionalities that will significantly affect the first use of the systems or services, *i.e.*, pre-settings that will not require any activity or choice from the user at first use. These elements are considered vitally important as they form the basis on which the user will initiate his or her first interaction with the system or service, and if users are unable or unwilling to configure the settings based on their own choices, the pre-settings will, in effect, determine the long-term use of the service or system (so-called "*Privacy Engineering*"). In this context, ENISA acknowledges that the choice of correct and fit-for-purpose defaults is not entirely simple as it requires an assessment of the need for each purpose and a balancing with other requirements that may be equally important (*e.g.*, usability).

In the process of building IT systems or IT-based services, the developers need to decide on the possible ways of implementing the desired functionality. To this end, functions can be divided into two categories:

(i) Functions "wired in", which cannot be configured or changed after the system/service has been built; or

(ii) Functions depending on the configuration, whose configuration (activation and usage parameters) can be adapted to the needs of users.

With regard to configurable functions, therefore, developers must determine which of them must be pre-configured, *i.e.*, set to specific values that are assigned to a configurable setting of the system

[25] European Union Agency for Network and Information Security, *Recommendations on shaping technology according to GDPR provisions. Exploring the notion of data protection by default,* December 2018, published on 18 January 2019, available at: https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2.

or service, until that setting is changed by user intervention. ENISA clarifies that the default settings relevant for ensuring compliance with the GDPR are, thus, all those that are able to determine the default way in which an application or device processes the user's personal data, such as with regard to access to contact data, use of a device's camera or microphone, geo-location data of a mobile app.

In any case, ENISA emphasises that the possibility for users to change their default data protection settings is an indispensable requirement and should be established whenever default settings have been implemented in the IT service or system offered for the first time, as it is the case for changing security defaults (*e.g.*, changing the default password for the first time).

ENISA also remarks that when designing a solution, developers are faced with a number of decisions about the functionalities of the solution under construction. In short, for each configurable setting, it must be decided whether it is pre-settable or not, and for each pre-setting, it shall be verified that all the requirements set out in Article 25 of the GDPR are met. Although the developer of the solution plays a decisive role in this phase, ENISA stresses that also the data controller who will use that solution, by virtue of the general principle of accountability, shall be able to understand the default settings of the solution in use and all the possible configuration choices in order to modify the default values to increase the level of protection of personal data. This means that the data controller shall also be in a position to assess whether a default setting is adequate or not.

The Recommendations recall some best practices for setting default values, giving some concrete examples for each of the four areas of measures mentioned in Article 25 of the GDPR:

(i) Minimum amount of personal data: the best practice is "*The less processing, the better*";

(ii) Minimum extent of the processing of personal data: some best practices are "*The less processing, the better*" and "*User empowering tools*";

(iii) Minimum period of storage of personal data: the best practice is "*Storage – the shorter, the better*"; and

(iv) Minimum accessibility of personal data: some best practices are "*Restricting access on the basis of necessity*", "*Limiting ways of sharing*", "*No public by default without active intervention*".

Finally, ENISA clarifies that such indications can be taken into consideration to raise the level of attention on specific cases, but should not be considered a "*legal evaluation of legitimacy*" in the choice of the best default settings to adopt, which will be evaluated, however, case by case.

2.1.4. Guidelines issued by Spanish and Norwegian Data Protection Authorities.

On 17 October 2019, the Spanish Data Protection Authority (hereinafter, "**AEPD**") published its Guide on Privacy by Design (hereinafter, the "**Guide**")[26], addressed to all the actors involved in the processing of personal data, such as suppliers, service providers, product and application developers or device manufacturers.

First of all, the Guide highlights Privacy by Design Foundational Principles (first defined by Ann Cavoukian as discussed in Chapter 1) and outlines practical steps for embedding them into GDPR compliance plans:

Foundational Principle	AEPD Guidance
1. Proactive not Reactive; Preventative not Remedial	PbD involves anticipation. Foreseeing events and risks that affect privacy before they materialize. Processes involving personal data must be conceived and designed from the beginning bearing in mind the risks for the rights and freedoms of data subjects, so that proactive measures can be taken.
2. Privacy as the Default Setting	Data subjects should remain protected even where they do not modify privacy settings. PbD overlaps with the Privacy by Default principle, as they both entail setting the systems and processes in a way that personal data is automatically protected. As the Guide explains: "*This principle, in practical terms, is based on data minimization throughout the stages of processing: compilation, use, retention and distribution*".
3. Privacy Embedded into Design	Applications, products and services, as well as the business practices and processes must be built on the protection of personal data and privacy. These concepts must be embedded naturally.
4. Full Functionality: Positive-Sum, not Zero-Sum	Privacy is not in opposition to business benefit or its usability. A win-win approach is a must when addressing new solutions for fully functional, effective and efficient solutions both at business and privacy levels.

[26] Agencia Española de Protección de Datos, *A Guide to Privacy by Design*, October 2019, available at: https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf.

5. End-to-End Security: Full Lifecycle Protection	Privacy protection must be guaranteed throughout the life cycle of the data, and its security involves the confidentiality, integrity, availability and resilience of the systems that store them. Privacy also guarantees unlinkability, transparency and the data subject's capacity to intervene and control the processing. It is essential to analyse all processing activities and apply appropriate security measures in order to achieve the "Full Lifecycle Protection".
6. Visibility and Transparency: Keep it Open	This principle reinforces the idea that diligence and accountability must be demonstrated by ensuring that the processing is aligned with the information provided to the data subject.
7. Respect for User Privacy: Keep it User-Centric	Any adopted measure must focus on guaranteeing privacy and data protection. As the Guide explains, this entails "*designing user-centric processes, applications, products and services, anticipating their needs. The users must play an active role in managing their data…however their inaction must not imply reduced privacy*".

The Guide also explains how traditional goals for designing secure and trustworthy systems to protect them from unauthorised processing (*i.e.* confidentiality, integrity and availability) are no longer enough as many new risk factors linked to authorised data processing have recently come into play (*e.g.*, the loss of control in decision-making, excessive data collection, re-identification). Nowadays it is necessary to widen the scope of analysis and the goals following GDPR's reinforced focus on risk analysis. To guarantee satisfaction of GDPR principles in this context, controllers should consider:

(i) **Unlinkability**: "*process data in such a manner that the personal data within a domain cannot be linked to the personal data in a different domain, or that establishing such a link involves a disproportionate amount of effort*". This relates to the GDPR principles of data minimisation, storage limitation, and integrity and confidentiality;

(ii) **Transparency**: "c*larify data processing such that the collection, processing and use of information can be understood and reproduced by all the parties involved and at any time during the processing*". This relates to the GDPR principles of purpose limitation, and lawfulness, fairness and transparency; and

(iii) **Intervenability**: "*ensure that it is possible for the parties involved in personal data processing, and especially the subjects whose data are processed, to intervene in the processing*

whenever necessary to apply corrective measures to the information processing". This relates to the GDPR principles of purpose limitation, accuracy, integrity, confidentiality and accountability.

The Guide also refers to the concept of Privacy Engineering[27], which entails three major stages:

(i) **Privacy requirements definition:** Specify the privacy properties, concept and requirements to be fulfilled by the system. This is where the privacy-by-design strategies come into play;

(ii) **Privacy design and development:** Bring the privacy requirements definition down to earth by designing the architecture and implementing system elements. In this stage, it is important to refer to privacy-by-design patterns, which manifest privacy-by-design strategies as reusable solutions to solve common privacy problems. In addition, we also find here Privacy Enhancing Technologies (PETS). These technologies, following the AEPD definition, consist of "*a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system*"; and

(iii) **Privacy verification and validation:** Integrate, test, evaluate, maintain and confirm that privacy requirements have been duly implemented and meet the stakeholders' expectations.

Finally, the Guide outlines that establishing a data protection governance framework does not represent an obstacle to innovation, but rather offers advantages and opportunities for organisations and the market.

Also, the Norwegian Data Protection Authority (hereinafter, "**Datatilsynet**") issued, on 20 August 2019, guidance on Privacy by Design (hereinafter, the "**Guidance**")[28]. The Guidance covers seven stages or activities (training, requirements, design, coding, testing, release and maintenance), and for each of these activities it includes a practical checklist in order to comply with the privacy principles:

(i) **Training**: the Guidance recommends training on the GDPR, on related legislation (*e.g.*, e-Privacy), on information security frameworks (*e.g.*, ISO 27001), on the framework for software development (*e.g.*, Microsoft Security Development Lifecycle), on security testing (*e.g.*, OWASP Top 10), on threat and risk assessment documentation requirements (*e.g.*, Microsoft Threat Modelling Tool). It moreover recommends differentiated training based on individuals' roles: a basic understanding of privacy and information security is crucial for all employees, while developers must be competent in, for instance, the topic of secure coding;

(ii) **Requirements**: Organisations should define the data protection and information security requirements for any given project. The checklist for requirements contains an impressively detailed (but non-exhaustive) list of action items on, for example, what needs to be done before the requirements are set, requirements for meeting the principles of data protection,

[27] Systematic process with a risk-oriented focus whose goal is to translate into practical and operational terms the principle of Privacy by Design within the life cycle of information systems entrusted with personal data processing.

[28] Datatilsynet, *Guidelines on Data Protection by design*, August 2019, available at: https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/.

requirements to protect the rights of data subjects, etc.. In relation to security in general, the checklist mentions five security principles: confidentiality, integrity, accessibility, resilience and traceability (C, I, A, R, T). The specific security requirements will then typically be linked to one or more of those security principles (*e.g.*, identification of users in the context of access control = T; strong password requirements = C, I, A). The checklist mentions the OWASP Application Security Verification Standards as a useful illustration of security requirements for use in software development, as well as ISO 27034 as an example on how to find an acceptable level of risk;

(iii) **Design**: The design-related checklist refers to the subdivision introduced by ENISA (in its 2014 report on privacy and data protection by design[29]) between data-oriented design requirements ("*minimise and limit*", "*hide and protect*", "*separate*", "*aggregate*", "*data protection by default*") and process-oriented design requirements ("*inform*", "*control*", "*enforce*", "*demonstrate*"), with practical implementation examples. In addition, the checklist recommends *(a)* analysing and reducing the attack surface of the software under development; and *(b)* threat modelling, with notably a reference to the STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege) and DREAD (damage, reproducibility, exploitability, affected users and discoverability) methodologies;

(iv) **Coding**: The coding checklist focusses on four main areas: *(a)* the use of approved tools and libraries; *(b)* scanning dependencies for known vulnerabilities or outdated versions; *(c)* manual code review; and *(d)* static code analysis with security rules. The checklist includes useful recommendations on, for instance, what to include in a list of tools and libraries, as well as examples of tools for static code analysis;

(v) **Testing**: At the testing stage, the checklist includes general test recommendations as well as specific guidance on security testing (dynamic testing, fuzz testing, penetration testing or vulnerability analysis; testing in multiple instances; automatic execution of test sets before release). In addition, the checklist stresses the importance of reviewing the attack surface of the software under development;

(vi) **Release**: At the release stage, the focus should lie on *(a)* an incident response plan; *(b)* a full security review of the software; and *(c)* a process involving approval of release and archiving. In relation to the incident response plan, the checklist sets out detailed recommendations on the life cycle of deviations and related procedures for detecting, analysing and verifying, reporting and handling incidents, followed by the need for normalising (restoring management, operation and maintenance to their normal state); and

(vii) **Maintenance**: In relation to maintenance, the key recommendation relates to incident response (extensively addressed by the previous checklist). For the surplus, the checklist mentions topics such as continuous assessment of vulnerability detection measures, metrics, etc..

[29] European Union Agency for Network and Information Security, December 2014, *op. cit.*.

2.2. Overview of best practices and guidelines concerning privacy certifications.

As already mentioned in Chapter 1, Article 42 GDPR provides that Member States, supervisory authorities and the relevant EU institutions shall encourage the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with GDPR by controllers and processors.

Differently from privacy-by-design and by-default techniques, privacy certifications represent voluntary measures that enterprises may decide to adopt for proving their degree of data protection compliance.

Two practical consequences stem from the voluntary nature of certifications: *(a)* compliance with GDPR must take place irrespective of the existence of – and in any case prior to – certification; and *(b)* certification does not reduce the responsibility of the controller or processor to comply with the GDPR and any granted certification does not prejudice the tasks and powers of the competent supervisory authorities.

Although the scope and the goal of certification are clearly outlined by Articles 42 and 43 GDPR, some aspects are left to the discretion of Member States and/or of the competent supervisory authorities, such as the identification of the most appropriate certification model, the appointment of the accreditation authority in each jurisdiction, the definition of the accreditation requirements. As stated above, the broad discretion given to Member States by the GDPR hinders the implementation in practice of certifications.

For these reasons, some European and national organizations have developed best practices for supporting national and supranational supervisory authorities, certification and accreditation bodies, controllers/processors and all the interested stakeholders in their respective roles and activities.

2.2.1. Guidelines No. 1/2018 of the European Data Protection Board (EDPB).

With a view to build a consistent and harmonized approach among the various Member States, the EDPB has provided guidance on the interpretation of Articles 42 and 43 GDPR and on the implementation of certification mechanisms[30].

As a starting point, the EDPB has clarified the definition of certification as referring to a third-party attestation related to processing operations by controllers and processors, as well as the difference between a certification and a seal or mark (*i.e.*, the former is to be meant as a statement of conformity, whilst the latter as a logo or symbol signifying the successful completion of the certification procedure).

The EDPB has also given advice on the role *(a)* of supervisory authorities – either as certification bodies or as responsible for monitoring certification procedures – suggesting a strict separation between the tasks related to certification and the powers of investigation and enforcement under the

[30] European Data Protection Board, *op. cit.*.

GDPR; and *(b)* of certification bodies, which must be fully independent, impartial and accredited either at national or at EU level[31].

With regard to the definition of certification criteria, the EDPB has preliminarily dealt with the approval of the relevant criteria by the competent supervisory authority or by the EDPB itself in the case of a EU Seal, stating – as a general rule – that such approval should be aimed at: *(a)* properly reflecting the requirements and principles concerning the protection of natural persons, which underlies the legal framework on the processing of personal data; and *(b)* contributing to the consistent application of the GDPR.

To this end, supervisory authorities should treat all requests for approval of certification criteria in a fair and non-discriminatory way, on the basis of a publicly available procedure which specifies the general conditions to be met and the steps of the approval process.

As far as the EU Seal is concerned, the EDPB has further stressed the need to establish customizable criteria capable of considering national legal requirements and sector specific regulations (where applicable), without compromising the intended EU-wide applicability of this certification mechanism.

For the concrete development of certification criteria, the EDPB has suggested to focus on verifiability, significance and suitability of such criteria to their intended purpose (*i.e.*, demonstrating compliance with the GDPR rules) and to the scope of certification, which may vary depending on the type of processing operations and the specific sector addressed by certification. Indeed, certification under GDPR may be directed either to processing operations *stricto sensu* or to broader sets of operations, which may involve corporate governance processes as integral parts of a processing operation (*e.g.*, the governance process for handling complaints as part of the processing of employee data for salary payment).

Certification criteria should also be designed in a way that enables practical application, without however disregarding the underlying legal and compliance aspects, such as lawfulness of processing, data subjects' rights, obligation to notify potential data breaches, the technical and organizational measures in place to ensure security of processing pursuant to Article 32 GDPR[32].

---

[31] For further information on the accreditation procedure and requirements managed at national level, see European Data Protection Board, *op. cit.*.

[32] Article 32 GDPR provides as follows: "*1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

In this respect, in the EDPB's view, at least four different factors can be relevant for the design of certification procedures and criteria:

(i) the organization and legal structure of the controller or processor;

(ii) the department, environment and people involved in the processing operation(s);

(iii) the technical description of the elements to be assessed; and

(iv) the IT infrastructure supporting the processing operation including operating systems, virtual systems, databases, authentication and authorization systems, routers and firewalls, storage systems, communication infrastructure or Internet access and associated technical measures.

Not only certification criteria should be uniform and verifiable, but they should also be flexible and scalable for application to different types and sizes of organizations on a risk-oriented basis: in other words, such criteria should be equally applicable to small, medium or large processing operations, and should reflect the varying degree of risk and severity for the rights of the data subjects involved.

Additionally, according to the EDPB's guidelines, interoperability of certification mechanisms with other existing standards (*e.g.*, ISO standards) could help a controller or processor to guarantee better compliance with the GDPR provisions. Nonetheless, when combining industry standards with certification mechanisms, it should be considered that the former are normally aimed at protecting the company's security and organization, whereas the latter are grounded on the protection of fundamental rights of natural persons.

As a last remark, certification criteria – despite reliable over time – should be subject to revision in the event of amendments to the applicable legal framework, new case-law of the EU Court of Justice, evolutions in the technical state of the art.

Similar principles should be followed in the determination of the conformity procedure to be carried out by certification bodies, with particular regard to the applicable methodology assessment. These procedures should identify the appropriate level of evaluation (in terms of depth and granularity) and provide adequate information on the data to be collected and the methods of collection (*e.g.*, requests for documentation, on-site inspections and audits, indirect accesses), in order to ensure transparency both for the applicant and for the supervisory authority (in case of subsequent reviews of the performed assessment). Also, roles and responsibilities of the parties involved must be clearly defined and distinguished.

---

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law".

2.2.2. Recommendations of the European Union Agency for Network and Information Security (ENISA).

After the entry into force of the GDPR and before the expiry of its implementing period, ENISA has drawn recommendations for the development of the European data protection certification, based on the analysis of existing certification schemes and of the relevant GDPR provisions, that are meant to provide high-level guidance to the competent EU bodies, national supervisory authorities, certification bodies, and controllers/processors[33].

In the first place, ENISA has pointed out the cruciality to adopt an aligned approach – both among national supervisory authorities and among the latter *vis-à-vis* the EDPB – on each aspect of certification (ranging from scope to criteria), by possibly taking into account successful existing certification models, with a view to increase awareness in data subjects.

The promotion of an EU approach could moreover help to face criticism posed by proliferation of national certifications in relation to market recognition, trust, economic factors and legal uncertainty.

To this end, mutual recognition mechanisms and procedures between the various jurisdictions should be incentivized, such as the creation of a common register of all issued/withdrawn certifications in all EU Member States.

ENISA has further recommended the European Commission and the EDPB to encourage the establishment of adequate safeguards *(a)* to minimize the risk of function creeps and conflicts of interest as regards the involvement of national supervisory authorities in the process of accreditation and certification (*e.g.*, separation of the staff conducting certification from the staff conducting supervisory activities); and *(b)* to ensure transparency, trustworthiness and quality of the certification procedure (*e.g.*, publicly available summary reports on certification activities; transparent fees; publicity of criteria, requirements and methods for evaluation).

EU and national institutions are also invited to jointly promote an EU scalable approach with approved and widely accepted criteria (which may motivate SMEs to undertake certification despite their limited resources), as well as to exchange best practices even if applicable to other connected fields, such as cybersecurity.

Finally, ENISA has suggested to provide guidance on some open topics, including – *inter alia* – compatibility of certifications based on international standards and non-EU certifications with GDPR, transparency thresholds, complaint mechanisms, post-certification surveillance measures.

2.2.3. Available certification schemes for data protection.

Certifications may be classified depending on their target: products and services (including software), governance processes or management systems.

[33] European Union Agency for Network and Information Security, 27 November 2017, *op. cit.*.

Certifications targeting governance processes or management systems differ from certifications targeting processing operations (either processing as such or as part of a service or a product), since the former are more "process-oriented" than "goal-oriented".

A "goal-oriented" certification is intended as a certification mechanism that does not primarily focus on the measures adopted by the company, rather on the adequacy of such measures to achieve certain pre-determined goals. In this sense, privacy certifications envisaged by Articles 42 and 43 GDPR may be characterized as "goal-oriented".

For the time being, there are still no certification schemes totally falling within the scope of Article 42 GDPR and recognized as such at EU or national level. Indeed, according to a study of the University of Tilburg, whose results were published by the European Commission in February 2019[34], currently only two of the existing certification mechanisms related to data protection may be regarded as compliant with the purpose pursued by Article 42 GDPR.

Among the currently available certification mechanisms and compliance measures related to data protection, the following are worth to mention:

(i) **UNI/PDR 43:2018**: an industry prudent practice aimed at defining actions for the lawful processing of personal data through ICT tools and at certifying compliance of a process, product or service (including a software) with mandatory data protection requirements, on the basis of ISO 17065 standard. Certification based on UNI/PDR 43:2018 may be required by any interested enterprise – irrespective of its legal form, size and industry sector – which processes personal data through electronic devices and systems;

(ii) **ISDP 10003:2020**: a certification mechanism based on ISO 17065 standard, developed by an independent certification body, for certifying processing of personal data in relation to the protection of fundamental rights of natural persons and of the free movement of data;

(iii) **BS 10012/2017**: a data protection management system created by the British Standard Institute, which can be integrated with certification models as based on the High-Level Structure approach[35]. This is aimed at providing essential elements for the implementation of a data protection management system that allows compatibility with GDPR rules and with the company's business strategies, resources and infrastructure management, procurement processes, etc.;

(iv) **ISO/IEC 27001**: standard applicable to a single business process (*e.g.*, in human resources), a particular service or the whole business process of an organization, which defines the criteria for a management system on information security; and

(v) **ISO/IEC 27701:2019**: standard designed in accordance with the criteria of ISO/IEC 27001 and ISO/IEC 27002, promoting implementation of a Privacy Information Management System (PIMS) to be integrated with IT Security management systems.

[34] Directorate – General for Justice and Consumers Unit C.3 Data Protection and Unit C.4 International Data Flows and Protection, *op. cit.*.

[35] Approach adopted by ISO in 2014, which grants to the standards developed by ISO a common structure so that they may be integrated with each other.

2.2.4. Data protection certification in Italy.

With decision No. 148 of 29 July 2020, the Italian Data Protection Authority (hereinafter, the "**IDPA**") has approved additional accreditation criteria for certification bodies in order to certify compliance with GDPR rules by undertakings that process personal data for the provision of products or services[36].

Such accreditation criteria are intended to complement those set forth by the international EN-ISO/IEC 17065:2012 standard, as expressly provided by Article 43(1)(b) GDPR.

The IDPA has appointed ACCREDIA as responsible for accreditation, being it the only Italian accreditation authority under Regulation (EC) No. 765/2008. Already in March 2019, the IDPA and ACCREDIA signed a protocol for the exchange of information regarding accreditation and certification activities pursuant to Articles 42 and 43 GDPR.

The additional accreditation criteria identified by the IDPA require certification bodies to prove, *inter alia*:

(i) that their respective certification agreements impose on clients to comply with the criteria approved by the IDPA or the EDPB, to ensure transparency towards the IDPA, to not limit liability under GDPR, to grant certification bodies access to information and processing operations, to promptly inform certification bodies and the IDPA in case of significative changes to the *status quo ante*;

(ii) to be fully impartial and independent;

(iii) the absence of any conflict of interest in the performance of certification activities;

(iv) to have in place adequate measures to mitigate potential risks deriving from certification activities;

(v) to publish clear information on the applied certification criteria and procedures and on the processes for handling complaints;

(vi) to engage duly authorized, competent and trained personnel in the performance of certification activities;

(vii) to make use of standardized or comparable evaluation methods; and

(viii) to establish periodic post-certification surveillance and a complaint mechanism for the stakeholders concerned.

[36] Italian Data Protection Authority, Decision No. 148 of 29 July 2020, at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445086 (Italian language only).

2.2.5. Codes of Conduct.

For the sake of completeness, it should be noted that, besides privacy certifications, other voluntary measures for ensuring compliance with GDPR are the so-called “Codes of Conduct” referred to in Article 40 of the GDPR.

Codes of Conduct represent self-regulatory instruments that set out data protection rules for categories of data controllers and processors and they can be a useful tool for accountability, providing a detail of more appropriate behaviour not only from a legal but also from an ethical point of view. In general, the rules are not binding, but the authority of the body issuing them makes them widely applicable.

Even though practical difficulties have also arisen with regard to the implementation of Codes of Conduct, recently some steps forward have been made with the issuance of two EU Cloud Service Provider Codes of Conducts promoted by the Cloud Infrastructure Services Providers in Europe (CISPE) and the Cloud Select Industry Group (CSIG), approved by the EDPB in May 2021. While the Code promoted by CISPE is specifically aimed at regulating IaaS services (Infrastructure as a Service), the other project is broader and regulates not only IaaS services, but also PaaS (Platform as a Service) and Saas (Software as a Service) services. Furthermore, both Codes: *(a)* do not apply directly to consumers, although their adoption will have a positive impact on data protection standards applying to non-professional users; *(b)* provide for an independent monitoring body and for sanctions; and *(c)* prescribe a number of security requirements, periodic checks and audits and the fulfilment of additional requirements[37].

In this sense, it should be further mentioned that some Italian companies operating in different sectors are developing, together with the Italian Data Protection Authority, a Code of Conduct on Teleselling, which identifies rules of conduct on the protection of personal data for the performance of direct telephone marketing activities, carried out directly or entrusted to a third party under a specific contract.

[37] For more details on the issue, please see EDPB’s Opinions, available at: https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202116_eucloudcode_en.pdf and https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202117_cispecode_en_0.pdf.

3. Impact of data protection measures on software development: where does liability stand?

3.1. The interplay between data protection measures and software development.

As it stems from the previous Chapters, data protection measures may play a crucial role in the development of software intended to process personal data.

In the first place, software developers shall mandatorily ensure that their products are equipped with settings and features in line with the principles of Privacy by Design and Privacy by Default. Implementing these principles in software development is a multidisciplinary exercise, where technical, organizational and legal concerns need to be properly addressed.

As a starting point, it is essential that the company has adopted and actually implemented a defined set of security and privacy policies in order for the application owners and developers to be able to appreciate the specific sets of security and privacy requirements to be embedded in software applications. The acknowledgement of privacy in the organization (*e.g.*, the appointment of a privacy officer, or the performance of privacy risk assessments on a regular basis) and the adoption and actual implementation of a proper privacy policy are "*two fundamental cornerstones that the organization needs to have in place before the software system procurement phase starts*" as the former "*will ensure that sufficient attention and resources are put in place to protect privacy and the latter will serve as a basis for deriving appropriated privacy requirements when the software development process starts*"[38]. This process will need the involvement of a wide range of stakeholders, such as regulators, end-users, application developers, business owners, software vendors, third parties and consultants.

After specific privacy requirements are defined and validated through the organization's privacy policy, existing PbD best-practices shall be incorporated into the code by the software development team[39]. Moreover, when designing and implementing a software application it must be ensured that the end-users have the control over his/her personal data. This means enabling data subjects to change their privacy settings, give and withdraw consent, and extract, amend and delete personal data that has already been disclosed.

Data protection measures involving software may also take the form of a certification: as illustrated in Chapter 2, a privacy certification may attest conformity of a software's settings and features with GDPR rules. The presence of a certification related to a software may moreover help data controllers to select the best option for their needs on a risk-based approach. Indeed, pursuant to Article 28(5) GDPR, adherence of a processor to an approved certification mechanism may be used as an element by which to demonstrate to the data controller that it has implemented sufficient guarantees for the data subjects' rights.

[38] K. Bernsmed, *Applying Privacy by Design in Software Engineering – A European Perspective*, in SOFTENG 2016, *The Second International Conference on Advances and Trends in Software Engineering*, 2016, p. 73.

[39] *Ibidem*.

However, the use of a third-party software for the processing of personal data could give rise to certain interpretative and applicatory difficulties, especially in the event of a data breach occurring notwithstanding the existence of the necessary data protection measures.

In such cases, who should be held liable under the GDPR?

3.2. The treatment of liability under the GDPR.

The matter of liability is of the utmost importance for the enforcement of data protection law and it is strictly related to the roles of the data controller (*i.e.*, the one who determines the purposes and means of the processing of personal data) and the data processor (*i.e.*, the one who processes personal data on behalf of the controller).

Nevertheless, similarly to the other concepts laid down in the GDPR, the notion of liability lacks a clear and specific definition, which increases the degree of fragmentation among the Member States, thus further jeopardizing the GDPR's harmonization spirit.

Notwithstanding this ambiguity, as stressed by some commentators, the GDPR has moved some steps forward on liability compared with the previous legislative framework[40].

Under Directive 1995/46/EC, liability was exclusively allocated on the part of controller as a form of "strict" liability, whereas no provision regulated liability exposure of the processor, which could not face any consequences in case of disregard of the controller's instructions.

The controller was, hence, liable for any violation of the Directive resulting from the operations carried out by a processor acting on its behalf, as a result of the fact that the controller's duty of care towards data subjects could not be transferred to an independent contractor ("non-delegable duty of care"). Nor such liability could have been escaped by demonstrating an absence of fault in the controller's choice or supervision of the processor, due to the strict nature of liability.

The GDPR has broken with the past by introducing in Article 82[41] a "cumulative" liability regime among controllers and processors based on their respective roles in the processing. Specifically,

---

[40] B. V. Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, 7 (2016) JIPITEC 271 para 1; G. M. Riccio, F. Pezza, *Certifications Mechanism and Liability Rules under the GDPR. When the Harmonisation Becomes Unification*, in De Franceschi - Schulze, *Digital Revolution - New Challenges for Law*, Nomos, 2019, p. 140-151.

[41] Article 82 GDPR provides as follows: "*1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.*

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

while the controller is still the primary responsible, the processor has become directly liable *vis-à-vis* data subjects in case of failure to comply with the obligations imposed on it. This implies that, where both the controller and the processor are involved in the processing and are responsible for damages caused to a data subject, the latter may seek full compensation from each of them alternatively, without prejudice to the right of the one who paid the entire damage to claim back from the other that part of the compensation corresponding to its part of responsibility for the damage (Article 82(4) and (5) GDPR).

Controller's liability has again been construed as a strict liability: the controller remains generally liable for any damages arising from an unlawful processing of personal data and it may be only exempted, wholly or partially, "*if it proves that it is not in any way responsible for the event giving rise to the damage*" (Article 82(3) GDPR). This last sentence should be read as referring exclusively to events beyond the controller's field of action, such as force majeure events consisting in abnormal occurrences which cannot be foreseen and avoided by any reasonable means.

Processor's liability may instead be regarded as "proportional", as it may be held liable only in relation to "his segment" of the processing operation and insofar as it is – at least partially – responsible for the harm caused.

Another remarkable innovation brought by the GDPR is the clause contained in Article 2(4) GDPR, which recognizes the applicability of the liability exemptions for internet service providers (ISPs) set forth in Directive 2000/31/EC (so-called "E-Commerce Directive"), thus resulting in the absence of liability for mere distribution or storage activities carried out by ISPs as intermediaries.

Irrespective of the exposed person, pursuant to Article 82(1) GDRP, data subjects are entitled to seek compensation for both material and non-material damages. The right to compensation has been therefore extended to non-pecuniary damages also at EU level, although some Member States already envisaged this possibility at national level.

The GDPR does not however provide guidance on the definition and calculation of recoverable damages. The only relevant provision is Recital 146, which in turn refers to the case-law of the EU Court of Justice for the interpretation of the concept of damage. This ultimately shift to the Member States the burden of defining recoverable damages and determining their calculation methods, considering that tort law falls outside the EU competences and the EU judges had very few occasions to express their opinion on such matter. Of course, the said approach may lead to potential unequal treatments in case the unlawful behaviour would affect data subjects established in different jurisdictions, as it could happen for a multinational company.

With regard to the burden of proof, data subjects seeking compensation must succeed in demonstrating the following elements: *(a)* the performance of an unlawful act (*i.e.*, an unlawful

---

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2)".

processing operation or another act in contrast with GDPR provisions); *(b)* the existence of damages; and *(c)* a causal relationship between the unlawful act and the damages incurred.

On the other side, controllers and processors are only allowed to prove that the conditions for benefiting from the liability exemption under Article 82(3) GDPR are fulfilled.

3.3. Who is responsible for infringements of privacy-by-design and privacy-by-default measures in software developments?

The issue of data protection liability emerges already in the design phase of the processing and is, therefore, deeply intertwined with the principles of accountability, Privacy by Design and Privacy by Default.

According to Article 25 of the GDPR, the controller is obliged to perform the measures required by the principles of Privacy by Design and Privacy by Default, measures that the controller must be able to prove (accountability) in order to avoid the obligation to compensate the damaged data subject. The processor is not even mentioned in this Article.

It seems from the above that liability is concentrated more on the controller than on the processor, considering that the principle of accountability is apparently referred only to the controller. Actually, the liability of the processor is extremely broad when the controller entrusts him with all or a large part of the data processed, especially when Article 25 is read together with other provisions of the GDPR. In fact, both the controller and the processor are subject to different obligations and, according to the principle of accountability, must be able to prove that they have observed them, thereby giving rise to the division of liabilities provided for in Article 82 of the GDPR.

Pursuant to Article 28(1) of the GDPR, the data controller is responsible for identifying processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subjects. Among “sufficient guarantees”, there are certainly the requirements of Privacy by Design and Privacy by Default: the data controller shall, thus, appoint data processors that are able to demonstrate compliance with the accountability principle, *i.e.*, the products, services and applications provided to the data controller have been designed taking into account the protection of personal data[42].

The first legal instrument that allows the allocation of liabilities between data controller and data processor is the act of appointment of the processor by the controller (which may not only be in the form of a contract, but also of another legal act). The choice of the processor by the controller should be based on verification of the existence of sufficient guarantees in terms of appropriate technical and organizational measures in place to comply with the GDPR. It should be also highlighted that the processor is liable for any damage, even if it has not acted in accordance with the instructions received from the controller. According to Article 82 of the GDPR it is further necessary that the processor carefully evaluates the content of the act of appointment, which, in any case, must be

[42] E. Covelli, *Privacy by Design in the relationship between data controller and data processor*, in Cybersecurity360, 21 March 2019, available at: https://www.cybersecurity360.it/legal/privacy-dati-personali/la-privacy-by-design-nel-rapporto-tra-titolare-e-responsabile-del-trattamento-dati-le-soluzioni/ (Italian language only).

conferred by the controller after an in-depth assessment of the skills and characteristics of possible data processors in order to make a valid selection. The act of appointment helps to define the limits of the scope of liability of the two parties. The drafting of the act of appointment, which takes place at the time of designing the data processing procedures, is hence an example of the aforementioned principle of Privacy by Design[43].

In this context, the figure of the software developer (or software house) – that is the subject that, in its quality of data processor, creates, on behalf of the data controller, products or technologies that will then process the personal data – becomes particularly relevant.

In fact, one of the most interesting concepts introduced in the GDPR concerns the obligation of software compliance with data protection legislation: as already discussed above, it is essential that the tools used to manage personal data comply with GDPR principles. If the concept of Privacy by Design is now well known, the borders of the liability of software developers, on the one hand, and software buyers on the other, are less so.

The data controller is burdened, starting from the purchase or the commissioning of a software development, with the obligation to assess the security measures it intends to adopt; it will have to verify, from the beginning, the accuracy of the type of data processed, the procedures that are upstream with respect to the data management flow and the security that characterizes the environment where the data is hosted in all its peculiarities. However, this concept of "control from the beginning", incumbent on the data controller, is not always realistically applicable, as responsibility for compliance control often has to be transferred to the supplier.

Since these measures vary according to the choices made in accountability by the controller, the supplier shall guarantee the possibility of setting the different functions. For example, with regard to automated deletion in an application, the deletion deadline cannot be decided by the supplier but must be imposed, and therefore set, by the controller. The levels relating to the authorization profiles cannot, likewise, be decided by the supplier, but must instead be the result of the controller's own assessment. Therefore, the supplier who provides software to a data controller must ensure that the product can be made compliant with the legal requirements. It can achieve this aim in two ways:

(i) by applying the principle of Privacy by Design from the development and release of the application (*e.g.*, guaranteeing confidentiality by means of various levels of access and protection); or

(ii) by guaranteeing the data controller the possibility of determining, according to its own criteria, the most appropriate level of the measure to be implemented.

It follows that the data controller is liable for the software purchased, as it must be compliant with the law (*i.e.*, not have settings in violation of the law, *e.g.*, data erasure); the supplier is in turn liable for offering the data controller a software whose settings can meet the measures the data controller itself decides to adopt.

[43] D. De Rada, *La responsabilità civile in caso di mancato rispetto del GDPR. Privacy by default, privacy by design e accountability nell'ottica del Diritto Privato*, in Federalismi.it, December 2019.

If, on the other hand, the supplier releases “closed software” that cannot be customized, it increases its responsibility with regard to the security criteria applied and, necessarily, the impossibility of intervention by the customer (data controller) must be formalized contractually.

In the light of the above, it is clear that it is not possible to determine *ex ante* who is liable in the event of the sale or purchase of a software if the measures applied are insufficient. It will be necessary to specify the technical and organizational variables and to commensurate the responsibility with the autonomy of the controller on the one hand, and the level of setting possibilities provided by the supplier, on the other[44].

Finally, the essential elements for identifying liability in software development are as follows:

(i) preliminary assessment by the controller of the software with respect to the principles and measures applied to personal data and consequent to the choices made; and

(ii) compliance assessment of the software by the supplier with respect to the type of data processed, technical measures set and settable, organizational procedures for release, data loading and system administration, contractualization of specific liabilities as a direct consequence of the actions applicable to the software.

3.4. How is the allocation of liability affected by certification mechanisms?

As indicated above, the issue of liability has not been entirely regulated by the EU legislator, which has left some room for manoeuvre to Member States, with the risk of inconsistencies within the EU internal market.

Indeed, even though certain Member States have not expressly referred to their respective domestic legislation for determining the scope and content of liability, still liability rules are necessarily influenced by the national legislative and political landscape in which they are intended to operate.

By way of example, the French act transposing the GDPR provisions does not specify the criteria to be used for the assessment of liability nor the defences available and the recoverable damages. However, the French legislator – implementing one of the opening clauses of the GDPR – has introduced a collective action to obtain compensation for damages arising out of a data breach, by expanding the scope of the pre-existing class action. To activate such remedy, it is therefore necessary to follow the relevant French national rules.

In this fragmented context, certification mechanisms may play a vital role in the harmonization of data protection rules and their enforcement policies.

Some commentators have argued that the unifying function of certifications is twofold, since they would act not only *ex ante*, in the physiological phase where organizations choose voluntarily to

[44] V. Frediani, *GDPR and Software*, in Key4biz, 19 April 2019, available at: https://www.key4biz.it/gdpr-e-software-chi-paga-in-caso-di-non-conformita/255175/ (in Italian language only).

comply with privacy standards, but also *ex post*, in the pathological phase where organizations are called by the competent authorities to prove their degree of compliance[45].

In the latter scenario, the existence of a certification mechanism issued by an independent third-party can mitigate the consequences of a GDPR infringement, as providing objective evidence of the efforts made by the controller or the processor for complying with data protection law. In other words, "*by constituting an element to be considered by the authorities when imposing a fine (and the amount of the fine), certifications, due to their technical nature, would inevitably introduce an element of certainty in the assessment of the duty of care of the operators*"[46].

As it stems from the foregoing, the adoption of a certification mechanism under Article 42 GDPR may only act as a mitigating factor of the enforcement action, but it does not exclude or in any way limit the responsibility of the controller or processor *vis-à-vis* data subjects in case of violations, due to the nature of such responsibility as strict liability without any subjective connotations.

In this respect, one may ask whether it could be made a comparison between data protection certification mechanisms and organizational and management models pursuant to Italian Legislative Decree No. 231/2001 (so-called "231 Models").

The above-mentioned Legislative Decree has indeed introduced a quasi-criminal liability for companies in respect of certain offences perpetrated, in the company's interest or benefit, by its directors, employees and/or other corporate representatives. In particular, under Article 6(1), the company is not liable if it can prove that, *inter alia*, the management body has adopted and effectively implemented, prior to the commission of the offence by the above-mentioned directors, employees and/or representatives, organizational and management models suitable for preventing the categories of offences that have occurred. It means that the adoption and effective implementation of 231 Models may totally exempt the company from liability under Italian Legislative Decree No. 231/2001.

On the contrary, as described above, this automatism does not apply to data protection certifications: adherence to approved certification mechanisms may not serve *per se* as an exemption from liability, but rather it may solely be taken into account by the competent authority to decide whether to impose an administrative fine and on the amount of such fine. Therefore, differently from other harmonised standard certifications used in the EU, certifications pursuant to Article 42 GDPR do not offer any presumption of conformity with the legislation.

Once and again, under Article 82(3) GDPR, the only way for a data controller or processor to escape liability is to prove that the event giving rise to the damage is totally beyond the operator's control.

Then, what happens in case a data breach involves a third-party software that has obtained a data protection certification? May such a circumstance reduce the liability exposure of data controllers and/or processors under the GDPR towards data subjects?

The answer to this question seems to be negative.

[45] G. M. Riccio, F. Pezza, *op. cit.*.

[46] *Ibidem*.

As previously mentioned, where a company purchases a software and makes use of it, the company acts as data controller, whereas the software developer exercises the role of data processor, as the person processing personal data on behalf of the company.

In line with Article 82 GDPR, it seems that the company and the software developer may be held jointly liable for infringement of the obligation to adopt appropriate technical and organizational measures to ensure an adequate level of security; obligation which is referred to both the data controller and the data processor under Article 32 GDPR.

The existence of a certification in such a circumstance does not appear to represent a ground for exemption, either on the software developer's side because the certification mechanism only serves as an element to prove its compliance with GDPR (without any further legal effects, as already clarified above), or on the company's side because it has the duty to carefully verify if the software's design, features and functionalities meet the GDPR's requirements, without the possibility to invoke a sort of legitimate expectation defence.

The same conclusions seem also applicable in case a data protection certification has erroneously been issued despite the absence of the necessary requirements.

In fact, in decision No. 148 of 29 July 2020 setting out additional accreditation criteria for the issuance of privacy certifications, the IDPA expressly imposes on certification bodies to demonstrate that certification agreements "*do not limit the client's liability in relation to compliance with the GDPR and do not prejudice the tasks and powers of the IDPA in accordance with Article 42, paragraph 5 of GDPR*"[47].

As such, liability of the data controller or processor under the GDPR *vis-à-vis* data subjects seems not exemptible in the presence of a potential default of the certification body.

But does this similarly prevent a data controller or processor to seek adequate compensation from the certification body for failure to correctly carry out its activities?

In this regard, it is worth mentioning that certification bodies – in order to obtain accreditation – are required to hold an adequate insurance coverage against third-party claims and to establish readily accessible complaint mechanisms for all the interested parties (which may include their clients). This means that they may incur liability in the performance of their tasks.

The qualification of such liability and the consequent activable remedies are of course a matter of national law, as also recognized by the EU Court of Justice in a case concerning a certification body operating in the medical devices sector (so-called "notified body")[48].

With reference to Italy, the liability of the certification body towards the certified enterprise may be grounded on Article 1218 of the Italian Civil Code on contractual liability, considering that the certification body is contractually obliged to provide complete and faithful information on the existence of certain requirements in a product, service or process, which results in the obligation to detect possible non-conformities and to deny certification if this is the case.

[47] Italian Data Protection Authority, *op. cit.*, p. 3.

[48] CJEU, Judgement of 16 February 2017, C-219/15 *Elisabeth Schmitt VS TÜV Rheinland LGA Products GmbH*.

The certification body may additionally be held responsible towards other affected third parties on the basis of Article 2043 of the Italian Civil Code, regulating tort liability, since the issuance of an erroneous certification may have the effect of spreading misleading information and of creating legitimate expectations in the market.

In this respect, it is interesting to note that, in a case of 2012 (which represents, at the date of this Paper, the only Italian case-law on certification bodies' liability), the Court of Piacenza partially upheld the request for compensation of damages against a certification body brought by a manufacturer, which marketed a product after having received an attestation of conformity by the sued certification body, later proved wrong by in-depth evaluations of a national supervisory authority[49].

The Court of Piacenza examined the certification body's liability in the light of the principles regarding professional liability, by qualifying the obligations lying upon it as both obligations as to the result to be achieved and obligations as to the means.

Application of these same conclusions to privacy certifications may not however occur automatically and it should be carefully verified, taking always into account the voluntary nature of this kind of certifications, the absence of legal effects connected to them and the relevance of the data subjects' rights involved.

[49] Court of Piacenza, ruling of 3 May 2012, No. 297.

4. The path towards data sustainability.

4.1. A sustainable development approach to data protection.

In 1987, the United Nations published *Our Common Future*, also known as the Brundtland Report from the name of the former Norwegian Prime Minister at that time serving as Chair of the World Commission on Environment and Development (WCED). The report introduced for the first time the concept of "sustainable development", which was defined as "*development that meets the needs of the present without compromising the ability of future generations to meet their own needs*"[50].

In the United Nations' opinion, sustainable development would be composed of three interdependent and mutually reinforcing pillars: economic development, social development and environmental protection[51]. The economic aspect of sustainability implies the need to use available resources in the most efficient way in order to make products and offer services by adding value to people's lives. The social aspect of sustainability implicates the need to treat both ourselves and the others with fairness and respect. Environmental sustainability concerns protecting the biophysical system maintaining and nurturing life on earth[52]. Indeed, a sustainable solution extends beyond financial impacts and goals, implying also impacts and goals on the society and environment, as three dimensions to be equally considered and pursued.

In particular, when we look at data protection, the social aspect becomes relevant as the "*wellbeing of society as a whole implies the wellbeing of every individual, or at least of its vast majority*"[53]. In other words, companies are learning that the creation of financial value is increasingly connected to the societal value as nowadays consumers care about sustainable and fair business practices. In this context, "*it is confirmed that personal data, the driving force of the digital revolution and global economy, and the practices surrounding its value extraction urgently necessitate an ethical and sustainable approach*"[54].

Indeed, the proper use and processing of big data support the achievement of the Sustainable Development Goals (or SDGs) included in the 2030 Agenda[55]. Specifically, in November 2017, the

---

[50] Report of the World Commission on Environment and Development: Our Common Future, Oxford University Press, 1987.

[51] UN Department of Economic and Social Affairs – Division For Sustainable Development, *Johannesburg Plan of Implementation*, 15 December 2004, available at: https://www.un.org/esa/sustdev/documents/WSSD_POI_PD/English/POIChapter1.htm.

[52] V. Vijay, M. Fekete Farkas, *The Era of Big Data and Path towards Sustainability*, Conference Paper, June 2018, available at: https://www.researchgate.net/publication/325996293_The_Era_of_Big_Data_and_Path_towards_Sustainability.

[53] D. M. Parrilli, *It's time to talk about privacy sustainability*, 18 September 2020, available at: https://uxdesign.cc/its-time-to-talk-about-privacy-sustainability-df0ae3ea820d.

[54] P. Balboni, K. Francis, *Data Protection as a Corporate Social Responsibility. From Compliance to Sustainability to Generate Both Social and Financial Value*, 22 October 2020, Maastricht, The Netherlands, available at: https://www.maastrichtuniversity.nl/data-protection-corporate-social-responsibility.

[55] The Sustainable Development Goals (SDGs) or Global Goals are a group of 17 interlinked global goals designed as a "*plan of action for people, planet and prosperity*". The SDGs were set up in 2015 by the United Nations General Assembly and are intended to be achieved by the year 2030. They are included in a United Nations Resolution adopted, on 25 September 2015, by General Assembly: *Transforming our world: the 2030 Agenda for Sustainable Development*. The 17 SDGs are: (1) No Poverty, (2) Zero Hunger, (3) Good Health and Well-being, (4) Quality Education, (5) Gender Equality, (6) Clean Water and Sanitation, (7) Affordable and Clean Energy, (8) Decent Work and Economic Growth, (9) Industry,

United Nations Development Group (UNDG) published a document titled "*Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda*"[56] setting out a general guidance on data privacy, data protection and data ethics for the UNDG concerning the use of big data, collected in real time by private sector entities as part of their business offerings, and shared with UNDG members for the purposes of strengthening operational implementation of their programs to support the achievement of the 2030 Agenda (hereinafter, the "**UNDG Guidance Note**"). The UNDG Guidance Note is aimed at *(a)* establishing common principles across UNDG to support the operational use of big data for achieving the SDGs; *(b)* serving as a risk-management tool taking into account fundamental human rights; and *(c)* setting principles for obtaining, retention, use and quality control for data from the private sector.

These are the common nine principles set out by the UNDG Guidance Note together with a summary of their description contained therein:

(i) **Lawful, legitimate and fair use:** Data should be obtained, collected, analysed or otherwise used through lawful, legitimate and fair means (*e.g.*, adequate consent of the data subject; conformity with law; furtherance of international organizational mandates);

(ii) **Purpose specification, use limitation and purpose compatibility:** Any data use must be compatible or otherwise relevant, and not excessive in relation to the purposes for which it was obtained. In determining compatibility, the following criteria could be considered: *(a)* how deviation from the original purpose may affect individual(s) or group(s) of individuals; *(b)* the type of data used (*e.g.*, public, sensitive or non-sensitive); or *(c)* measure taken to safeguard the identity of data subjects (*e.g.*, pseudonymization, masking, encryption);

(iii) **Risk mitigation and risks, harms and benefits assessment:** A risks, harms and benefits assessment that accounts for data protection and data privacy as well as ethics of data use should be conducted before a new or substantially changed use of data (including its purpose) is undertaken. An assessment of harms should consider such key factors as: *(a)* the context of data use, including social, geographic, political and religious factors; *(b)* the likelihood of occurrence of harms (either physical, emotional or economic); *(c)* potential magnitude of harms; and *(d)* potential severity of harms. Where possible, the assessment should be completed by a diverse team of experts (*e.g.*, legal, ethics and security experts as well as subject-matter experts) and, where reasonably practical, a representative of the group(s) of individuals who could be potentially affected. Use of data should be based on the principle of proportionality. In particular, any potential risks and harms should not be excessive in relation to the positive impacts (benefits) of data use;

(iv) **Sensitive data and sensitive contexts:** Stricter standards of data protection should be employed while obtaining, accessing, collecting, analysing or otherwise using particular categories of personal data;

Innovation and Infrastructure, (10) Reducing Inequalities, (11) Sustainable Cities and Communities, (12) Responsible Consumption and Production, (13) Climate Action, (14) Life Below Water, (15) Life On Land, (16) Peace, Justice, and Strong Institutions, (17) Partnerships for the Goals.

[56] United Nations Development Group, *Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda*, November 2017, available at: https://unsdg.un.org/resources/data-privacy-ethics-and-protection-guidance-note-big-data-achievement-2030-agenda.

(v) **Data security:** Taking into account available technology and cost of implementation, robust technical and organizational safeguards and procedures should be implemented to ensure proper data management throughout the data lifecycle and prevent any unauthorized use, disclosure or breach of personal data (*e.g.*, aggregation, pseudonymization, masking, limited access on a "need-to-know" basis). Prior to data use, vulnerabilities of the security system (including data storage, way of transfer, etc.) should be assessed. Special attention should be paid when using cloud services, especially with regard to the data security setup and physical locations at which data is stored. Usage of non-cloud storage should be considered for sensitive data;

(vi) **Data retention and data minimization:** Data access, analysis or other use should be kept to the minimum amount necessary to fulfil its purpose. This principle also applies to data retention and deletion of data, which should be done in an appropriate manner taking into consideration data sensitivity and available technology;

(vii) **Data quality:** All data-related activities should be carried out with an adequate level of quality and transparency. Data quality must be assessed for biases to avoid any adverse effects, where practically possible, including giving rise to unlawful and arbitrary discrimination. Automatic processing of data, including the use of algorithms, without human intervention and domain expertise should be avoided when data is analysed for decision-making that is likely to have any impact on individual(s) or group(s) of individuals to avoid potential harms resulting from low quality of data. A periodic assessment of data quality is recommended during the data life cycle. Furthermore, it is important to establish an internal system of constant data updating and deletion of obsolete data, where appropriate and practically possible;

(viii) **Open data, transparency and accountability:** Open data is an important driver of innovation, transparency and accountability. In this context, appropriate governance and accountability mechanisms should be established to monitor compliance with relevant privacy and cybersecurity laws. Furthermore, all the elements of the processing of personal data concerned should be clearly and publicly described, unless there are legitimate grounds not to do so; and

(ix) **Due diligence for third-party collaborators:** It is recommended that a process of due diligence be conducted to evaluate the data practices of any potential third-party collaborators.

As further discussed below, a sustainable development approach to data protection also involves the protection of the environment, human rights as well as data security.

4.2. Data sustainability: a green footprint.

In the era of big data, most of the companies generally collect more data than they actually need to conduct their business operations. As a consequence, a large amount of stored data is unused as it is redundant, obsolete or trivial[57]. By implementing an effective Privacy by Design and Privacy by

[57] N. Correa, *The greening of privacy: Key steps to data sustainability*, 21 April 2021, available at: https://techbeacon.com/security/greening-privacy-key-steps-data-sustainability.

Default approach (*i.e.*, developing software which collects only data actually needed for the requested service), companies may make data storage more efficient while also pursuing sustainability goals by saving energy. Indeed, a sustainable approach to data protection boosts companies' green footprint.

Let's look at a practical example.

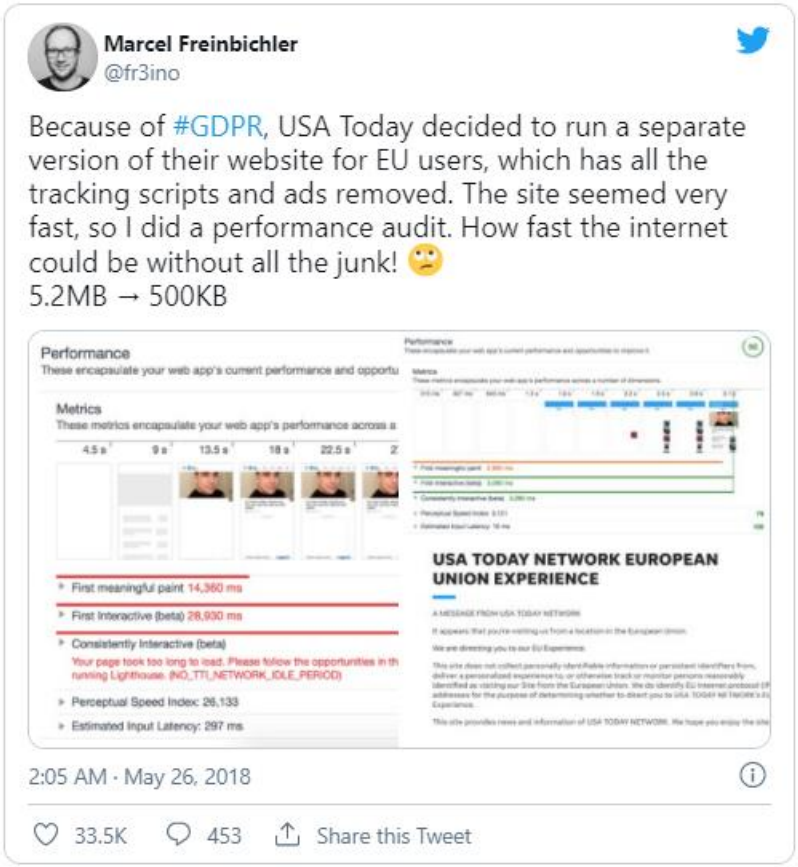

Image extracted from: https://www.mightybytes.com/blog/is-gdpr-good-for-the-environment/

On 25 May 2018, the effective date of GDPR, the Austrian web developer Marcel Freinbichler observed that the GDPR-compliant website of USA Today, specifically developed for EU users, was significantly faster than the original. In particular, by removing all its tracking codes, the GDPR-compliant site was "*one-tenth of its original size and page load time dropped from 45 seconds to three seconds*"[58].

By focusing on the above-mentioned example from an environmental standpoint, the web developer and digital sustainability expert Chris Adams, calculated that if "*we had the lighter, GPDR friendly, ad-and-tracking-free version of the site as the norm, if we just looked at the bandwidth savings, then we'd be saving something like the annual carbon footprint of a typical European, according to the*

[58] T. Frick, *Is GDPR Good for the Environment?*, available at: https://www.mightybytes.com/blog/is-gdpr-good-for-the-environment/.

World Bank, every month. Or if you prefer, something like a flight between New York and Chicago every day"[59].

It is clear that, with the adoption and enforcement of lean practices of data collection, data use, and data storage described in the previous Chapters, companies can achieve sustainability goals, while also ensuring better security (as further discussed in Paragraph 4.4 below) and privacy[60].

4.3. Data sustainability: protection of human rights.

Data protection seems to be facing ever increasing challenges in the modern, highly digitized world. Owning information has always been associated with having power, however never before data has been collected, traded, and exploited in such an extensive manner as at the present time. Technologies, owned by public and (more often) private actors, progressively penetrate the social, cultural, economic and political fabric of modern societies threatening to create an intrusive digital environment in which both States and business enterprises are able to conduct surveillance, analyse, predict and even manipulate people's behaviour to an unprecedented degree. While it cannot be denied that data-driven technologies bring forth numerous advantages to society and to individuals[61], risks related to them cannot be ignored.

This is the reason why it seems that data protection is increasingly at the centre of public agendas, both at the international and regional levels. For instance, in July 2015 the UN Human Rights Council mandated a Special Rapporteur on the right to privacy and in numerous resolutions the UN Human Rights Council and the UN General Assembly have expressed concerns about the risks to privacy emanating from State surveillance measures and business practices[62]. At the regional level, several legislations and guidelines have been issued to prevent violation of privacy and undue data sharing, for instance, to name few, the California Consumer Privacy Act, the African Union Commission Personal Data Protection Guidelines for Africa and, of course, the European Union's GDPR. Nonetheless, at the same time, many Governments have adopted laws or proposed legislation that increase their surveillance powers while also shrinking the civic space, often in ways that fall short of applicable international human rights standards[63]. These legislations typically allow public authorities to mandate digital and social media companies, to share personal data for alleged "security or public order reasons". While sometimes these interferences with users' privacy are justified, as in the case of crime prevention or fight against terrorism, recent years have witnessed increasing abuses by authoritarian states, that collect critical information to target critical voices and oppress political dissent. Human Rights organizations are growingly denouncing how data sharing

[59] mrchrisadams, *How much CO2 can you save when you remove ad-tracking from news sites?*, 27 May 2018, available at: https://blog.chrisadams.me.uk/posts-output/2018-05-27-how-much-co2-can-you-save-when-you-remove-ad-tracking-from-news-sites/.

[60] N. Correa, *op. cit.*.

[61] The 2030 Agenda asserts that "*Quality, accessible, timely and reliable disaggregates data will be needed to help with the measurement of progress (SGDs) and to ensure that no one is left behind. Such data is key to decision making*". See "*Transforming our World: The 2030 Agenda for Sustainable Development*" (A/RES/70/1, p. 11).

[62] See, for example, General Assembly resolutions No. 68/167, 69/166 and 71/199 and Human Rights Council resolutions No. 28/16 and 34/7 and decision No. 25/117.

[63] See, for example, A. Seibert-Fohr, *Digital surveillance, metadata and foreign intelligence cooperation: unpacking the international right to privacy*, 25 April 2018, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3168711.

by corporate actors often results in arbitrary detentions and other gross violations of human rights[64]. These actions clearly violate human rights protections.

In some regional legislations the concept of data protection is envisaged as an autonomous right, for example under Article 8 of the EU Charter of Fundamental Rights. Most often, however, international instruments consider data protection as part of the broader concept of right to privacy[65], defined as "*the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals*" [66].

Under international law, the primary duty to ensure compliance with human rights, including right to privacy and data protection, rests with states. Nonetheless, companies are far from being exempted from respecting human rights obligations. Pillar II of the Guiding Principles on Business and Human Rights (hereinafter, the "**Guiding Principles**"), a body of guidelines endorsed by the Human Rights Council in its resolution 17/4 of 16 June 2011, provides an authoritative blueprint for all enterprises, regardless of their size, sector, operational context, ownership and structure, for preventing and addressing all adverse human rights impacts, including on right to privacy. It sets out the corporate responsibility of enterprises towards internationally recognized human rights, stating that "*business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved*" [67].

The responsibility to respect applies throughout a company's activities and business relationships, including supply chains and value. The Guiding Principles also state that companies should, *inter alia*, express their commitment to meet this responsibility through a statement of policy approved by senior managers and disseminated internally and externally, and also should carry out "human rights due diligence" in order to identify, prevent, mitigate and account for how they address their adverse human rights impacts. Even though these guidelines constitute soft-law, recent trends show that countries – especially in the EU context – are increasingly introducing binding legislation on due diligence and corporate responsibility, including for companies' extraterritorial operations. In addition, the new proposed EU legislation on mandatory human rights due diligence is a further step in this direction. With regards to data protection, this legal advancement will make sure that the European safeguards will be applicable also in operations happening overseas or on the digital sphere, where questions of jurisdictions had typically prevented meaningful interventions.

Amongst the measures to be taken in order to prevent and mitigate the violation of human rights – through the breach of the privacy and data protection – the implementation of the Privacy by Design

---

[64] Amnesty International UK, *Vietnam: Facebook and YouTube 'complicit' in State censorship,* press release dated 2 December 2020, available at: https://www.amnesty.org.uk/press-releases/vietnam-facebook-and-youtube-complicit-state-censorship; Business & Human Rights – Resources Centre, *Arrest of activist Disha Ravi raises concerns over the privacy of Google users in India*, 1 March 2021, available at: https://www.business-humanrights.org/en/latest-news/arrest-of-activist-disha-ravi-raises-concerns-over-the-privacy-of-google-users-in-india/.

[65] See, for example, Article 12 of the Universal Declaration of Human Rights; Article 17 of the International Covenant on Civil and Political Rights; Article 16 of the Convention on the Rights of the Child; Article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families; and Article 22 of the Convention on the Rights of Persons with Disabilities

[66] Office of the High Commissioner for Human Rights, *The right to privacy in the digital age: report*, 3 August 2018, available at: https://undocs.org/A/HRC/39/29.

[67] Guiding Principle 11, available at: https://globalnaps.org/ungp/guiding-principle-11/.

and Privacy by Default principles plays a key role. As explained extensively in this Paper, these concepts are cornerstones to modern data protection, allowing to reduce the data acquired, processed, and stored to the minimum needed, thus reducing the risks of violating fundamental human rights. This argument is even recognized and endorsed by the 2018 report of the UN High Commissioner for Human Rights named "*The right to privacy in the digital age*" (hereinafter, the "**UN Report**"). The UN Report, in the section giving advises to States on how to implement proper data privacy legislative framework, explicitly recommends States, in setting requirements related to the design of products and services, to impose the principles of Privacy by Design and Privacy by Default, which are "*essential tools for safeguarding the right to privacy*" [68].

In the light of the above, it is then clear that the application of the Privacy by Design and Privacy by Default shall be implemented by companies in order to be more sustainable, with specific refence to their impacts towards the protection of human rights, and support the achievement of the SDGs, as discussed in Paragraph 4.1 above.

4.4. Data sustainability: cybersecurity.

We live in a hyper-connected and digitized environment, a world where potentially every aspect of our lives – from personal data to behavioural patterns – can be acquired, analysed and stored. At the same time, the increasing computing capacity of Information and Communications Technologies (ICTs), and their pervasiveness, speed up the rate at which a huge amount of data is accumulated.

This amount of data poses great challenges and risks to whom is in charge of acquiring and processing it, especially in terms of cybersecurity. The bigger the amount of personal data (pertaining to customers, stakeholders, employees, etc.) processed, the higher the chances that a security breach of IT system may cause significant damages because: *(a)* organizations are seen as high-value target for cyber adversaries focused on gathering sensitive data and using it for, *inter alia*, blackmail, extortion, identity theft, and other malicious purposes; and *(b)* if the attack is successful a larger number of individuals will be impacted. This seems even more daunting considering that the cyber-attacks are becoming more frequent[69], more sophisticated and have developed a tendency to aim at infrastructures in order to disrupt products and services that are key to our everyday lives[70] .

Such risks may not be worth to be taken at all, especially when the data collected is unnecessary to the scope, redundant, trivial or obsolete. Moreover, even if some data is necessary, companies should aim to craft the right balance between making use of big data technologies and protecting individuals' privacy and personal data. As discussed in Paragraph 4.2 above, a lean data approach

[68] Office of the High Commissioner for Human Rights, *op. cit.*, p.10.

[69] C. Brooks, *Alarming Cybersecurity Stats: What You Need To Know For 2021*, 2 March 2021, available at: https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=51b83e0958d3;

[70] R. Iyengar and C. Duffy, *Hackers have a devastating new target*, 4 June 2021, available at: https://edition.cnn.com/2021/06/03/tech/ransomware-cyberattack-jbs-colonial-pipeline/index.html; See also European Union Agency for Network and Information Security, *Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected*, press release dated 20 October 2020, available at: https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020.

based on the privacy-by-design and by-default principles gives companies and organizations an opportunity to better align data security and privacy requirements with corporate sustainability.

In the European Union, the relevance of the privacy-by-design and by-default principles is highlighted by the work of ENISA which has repeatedly issued reports and recommendation papers to indicate private and public actors how to properly implement such principles, even before the GDPR era[71]. These principles have always been at the centre of academic and institutional discourses on data protection and cyber security[72].

The implementation of privacy-by-design and by-default principles, as well as the use of privacy certifications and, ultimately, the outsourcing of software development to third parties able to adopt these data protection measures allow to shrink the target of cyberattacks. In addition, these accountability mechanisms make companies more sustainable given that they may allocate more efficiently the resources in protecting data processed and, in the unfortunate circumstances in which a cyberattack breaches the defence, they are a key to significantly mitigate consequent damages. Moreover, the adoption of the abovementioned data protection measures is extremely important in relation to the investment strategies of companies. Indeed, investors are increasingly integrating ESG factors into investment decisions in the hope that sustainable businesses offer less risk and long-term return on investment.

When investors decide to invest in a company, they carry out in-depth due diligences in which one of the most relevant aspect considered is compliance with data protection and cybersecurity legislation. The implementation of effective cybersecurity measures is essential for a company's performance, especially one that is likely to receive increased investment. The effectiveness of the privacy safeguards on systems adopted by the target company against possible data breaches makes the transaction highly profitable with a high value of sustainability. By implementing the said privacy solutions, organizations can stay ahead of the curve and, in doing so, increase attractiveness, competitive advantage, and revenue streams, putting sustainability at the forefront of their business aims.

[71] See for example, European Union Agency for Network and Information Security, December 2018, *op. cit.*; European Union Agency for Network and Information Security, *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data* analytics, 17 December 2015, available at: https://www.enisa.europa.eu/publications/big-data-protection; European Union Agency for Network and Information Security, December 2014, *op. cit.*. See also above Paragraphs 2.1.3 and 2.2.2 of this Paper.

[72] See D. Polverini, F. Ardente, I. Sanchez, F. Mathieux, P. Tecchio, L. Beslay, *Resource efficiency, privacy and security by design: A first experience on enterprise servers and data storage products triggered by a policy process*, in *Computers & Security*, Volume 76, July 2018, p. 295-310, available at: https://www.sciencedirect.com/science/article/pii/S0167404817302614.

Conclusions.

The above analysis shows that, in a context in which companies are developing services based on an intensive use of personal data and whose impact on privacy is strengthened by the use of disruptive technologies, the adoption of effective and efficient technical and organisational measures has become an essential instrument for the protection of fundamental rights and freedoms of data subjects.

As seen, protection of data subjects' rights and freedoms shall be guaranteed already from the initial stages of the development and design of a product or service, through the effective implementation of the principles of Privacy by Design and Privacy by Default. Such implementation involves the use of a specific methodology focused on risk management and accountability that helps to determine privacy requirements by means of practices, procedures and tools.

Ensuring privacy from the very beginning of the development phase of a software or IT application does not represent an obstacle to innovation. On the contrary, it offers advantages and opportunities for all the actors involved[73]:

(i) for organizations, it means improving efficiency, optimizing processes, establishing a cost-reduction strategy and obtaining a competitive edge;

(ii) for the market, it means the development of long-term sustainable economic models; and

(iii) for the society as a whole, it means being able to access the benefits of technological progress without compromising individual freedoms and independence.

Another tool that significantly contributes to the spreading of data protection sensitiveness in a globalized world is represented by certification mechanisms, which grant tangible benefits to individuals, organizations and, finally, the overall digital ecosystem[74].

Specifically, as mentioned above, by acting as an element to demonstrate compliance with GDPR certifications *(a)* enhance consumers' confidence; *(b)* ensure higher transparency on the company's processing practices; *(c)* mitigate the risks of fines by the Data Protection Authorities; and *(d)* may serve as an effective risk-management tool in B2B relationships.

However, the applicable legal framework still suffers from loopholes and a certain degree of fragmentation, which significantly hamper the evolution of privacy certifications into real bridges between different legal and accountability regimes.

Elimination of such inconsistencies is crucial for the achievement of sustainability goals and, ultimately, for the increase of competitiveness in the data-driven economy.

[73] Agencia Española de Protección de Datos, *op. cit.*.

[74] Centre for Information Policy Leadership GDPR Implementation Project, *Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms*, 12 April 2017, available at: https://iapp.org/media/pdf/resource_center/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf.

Indeed, principles like transparency, lawfulness, data minimization, accuracy, integrity and confidentiality, accountability represent a value for a company, are indicators for a "responsible" company and can be included in the sustainability indices that companies must document in formal reporting for stakeholders and lenders. The ability to manage data becomes a quality sought for the strategic guidance of companies (data stewardship). The ability to supervise risks and opportunities in the management of a company's data becomes a quality required to the members of the board of directors and managing directors. Data stewardship priorities include cybersecurity, the use and governance of artificial intelligence and machine learning systems, as well as privacy and ownership issue, data collected, managed and used.

Nowadays, companies are no longer judged and evaluated exclusively on the basis of conventional metrics (*e.g.*, financial performance or the quality of their products or services), rather they are increasingly assessed based on their relationships with their employees, customers and communities, as well as on their impact on society at large. This new approach contributed to transform companies from *business* enterprises into *social* enterprises[75].

A social enterprise is "*an organization whose mission combines revenue growth and profit making with the need to respect and support its environment and stakeholder network. This includes listening to, investing in, and actively managing the trends that are shaping today's world. It is an organization that shoulders its responsibility to be a good citizen (both inside and outside the organization), serving as a role model for its peers and promoting a high degree of collaboration at every level of the organization*"[76].

Being a *social* enterprise is not a matter of altruism, rather it allows to boost brand's reputation and consumers' trust and to attract and retain critical employees. By implementing a sustainable business model, a company also attracts investors interested in making sustainable investments. All the foregoing creates a virtuous circle which leads a *social* enterprise to experiment a more robust growth and, as a result, higher returns to shareholders and, more generally, value for all stakeholders and communities where the *social* enterprise operates.

[75] Deloitte Insights, *The rise of the social enterprise. 2018 Deloitte Global Human Capital Trends*, p. 2, available at: https://www2.deloitte.com/content/dam/insights/us/articles/HCTrends2018/2018-HCtrends_Rise-of-the-social-enterprise.pdf.

[76] *Ibidem*.

Bibliography

- A. Cavoukian, *Creation of a Global Privacy Standard*, 8 November 2006.
- A. Cavoukian, *Privacy by Design. The 7 Foundational Principles*, January 2011.
- A. Cavoukian, *Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D*, 18 May 2010.
- A. Seibert-Fohr, *Digital surveillance, metadata and foreign intelligence cooperation: unpacking the international right to privacy*, 25 April 2018.
- Agencia Española de Protección de Datos, *A Guide to Privacy by Design*, October 2019.
- Amnesty International UK, *Vietnam: Facebook and YouTube 'complicit' in State censorship,* press release dated 2 December 2020.
- C. Adams, *How much CO2 can you save when you remove ad-tracking from news sites?,* 27 May 2018.
- C. Brooks, *Alarming Cybersecurity Stats: What You Need To Know For 2021*, 2 March 2021.
- Centre for Information Policy Leadership GDPR Implementation Project, *Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms*, 12 April 2017.
- CJEU, Judgement of 16 February 2017, C-219/15 *Elisabeth Schmitt VS TÜV Rheinland LGA Products GmbH*.
- Court of Piacenza, ruling of 3 May 2012, No. 297.
- D. De Rada, *La responsabilità civile in caso di mancato rispetto del GDPR. Privacy by default, privacy by design e accountability nell'ottica del Diritto Privato*, in Federalismi.it, December 2019.
- D. M. Parrilli, *It's time to talk about privacy sustainability*, 18 September 2020.
- D. Polverini, F. Ardente, I. Sanchez, F. Mathieux, P. Tecchio, L. Beslay, *Resource efficiency, privacy and security by design: A first experience on enterprise servers and data storage products triggered by a policy process*, in *Computers & Security*, Volume 76, July 2018, p. 295-310.
- Datatilsynet, *Guidelines on Data Protection by design*, August 2019.
- Deloitte, *The rise of the social enterprise. 2018 Deloitte Global Human Capital Trends*, p. 2.
- Directorate – General for Justice and Consumers Unit C.3 Data Protection and Unit C.4 International Data Flows and Protection, *Data Protection Certification Mechanisms. Study on Articles 42 and 43 of the Regulation (EU) 2016/679. Final Report*, February 2019, p. 16.

- E. Covelli, *Privacy by Design in the relationship between data controller and data processor*, in Cybersecurity360, 21 March 2019.
- European Data Protection Board, *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*, version 3.0, 4 June 2019.
- European Data Protection Supervisor, *Opinion 5/2018. Preliminary Opinion on privacy by design*, 31 May 2018.
- European Union Agency for Network and Information Security, *Privacy and Data Protection by Design – from policy to engineering*, December 2014, published on 12 January 2015.
- European Union Agency for Network and Information Security, *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data* analytics, 17 December 2015.
- European Union Agency for Network and Information Security, *Recommendations on European Data Protection Certification*, 27 November 2017, p. 15.
- European Union Agency for Network and Information Security, *Recommendations on shaping technology according to GDPR provisions. Exploring the notion of data protection by default,* December 2018, published on 18 January 2019.
- European Union Agency for Network and Information Security, *Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected*, press release dated 20 October 2020.
- G. M. Riccio, F. Pezza, *Certifications Mechanism and Liability Rules under the GDPR. When the Harmonisation Becomes Unification*, in De Franceschi - Schulze, Digital Revolution - New Challenges for Law, Nomos, 2019, p. 140-151.
- Italian Data Protection Authority, Decision No. 148 of 29 July 2020.
- K. Bernsmed, *Applying Privacy by Design in Software Engineering – A European Perspective*, in SOFTENG 2016, *The Second International Conference on Advances and Trends in Software Engineering*, 2016, p. 73.
- L. A. Bygrave, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, in OSLO LAW REVIEW, Volume 4, No. 2-2017, pp. 105–120.
- N. Correa, *The greening of privacy: Key steps to data sustainability*, 21 April 2021.
- NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, January 2017.
- Office of the High Commissioner for Human Rights, *The right to privacy in the digital age: report*, 3 August 2018.

- P. Balboni, K. Francis, *Data Protection as a Corporate Social Responsibility. From Compliance to Sustainability to Generate Both Social and Financial Value*, 22 October 2020, Maastricht, The Netherlands.
- R. Iyengar and C. Duffy, *Hackers have a devastating new target*, 4 June 2021.
- Resolution on Privacy by Design. 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem (Israel), 27-29 October 2010.
- UN Department of Economic and Social Affairs – Division For Sustainable Development, *Johannesburg Plan of Implementation*, 15 December 2004.
- United Nations Development Group, *Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda*, November 2017.
- V. Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, 7 (2016) JIPITEC 271 para 1.
- V. Frediani, *GDPR and Software*, in Key4biz, 19 April 2019.
- V. Vijay, M. Fekete Farkas, *The Era of Big Data and Path towards Sustainability*, Conference Paper, June 2018.
- World Commission on Environment and Development, Report "*Our Common Future*", Oxford University Press, 1987.