ERA Forum (2020) 20:455–469
https://doi.org/10.1007/s12027-019-00578-6

ARTICLE

The symbiotic relationship between privacy and security in the context of the general data protection regulation

Emanuele Ventrella[1]

Published online: 11 September 2019

Abstract Traditionally, privacy and security are considered to be opposing values, constantly to be seen in contrast with each other. The purpose of this article is to demonstrate how technological development, instead of worsening the cleavage between privacy and security, allows considering the two principles to be inter-related and to affect each other reciprocally. By first theorising this relationship, the article will then take the GDPR as a case-study to demonstrate how effective data protection legislation considers the security of individuals, software and data to be crucial feature of such laws.

Keywords Privacy · Security · GDPR · Accountability · DPIA

1 Introduction

Traditionally, privacy and security are considered to be opposing values, constantly to be seen in contrast with each other. The perception of a dichotomous relationship has been further exacerbated with technological development entering into the framework. By impacting every aspect of modern human society, technology has detached both privacy and security from real world situations, allowing them to find their field of application in the arena of cyberspace. The purpose of this article is to demonstrate how technological development, instead of worsening the cleavage between privacy and security, allows considering the two principles as inter-related and reciprocally affecting each other. By theorising this relationship, the article will first focus on how the evolution of the concept of privacy led by the advancement of technology has

✉ E. Ventrella
emanuele.ventrella@alumni.luiss.it

[1] Data Protection Assistant, Brussels, Belgium

moved the two values closer together. Then, by illustrating how it works in practice, the article will employ the European Union General Data Protection Regulation (henceforth GDPR or Regulation)[1] as a case-study to show that the security of individuals, software and data assumes a crucial role for the fulfilment of data protection objectives.

2 The evolution of privacy

2.1 Privacy and technology

Since its first codification into written law in the United States, privacy has been intertwined with the development of new technologies. Appearing for the first time in an influential article by Samuel Warren and Louis Brandeis in the Harvard Law Review in 1890, "the right to privacy" was originally invoked as a reaction against the intrusive activities of American journalists having no respect for personal feelings and sexual relations. In that context, "recent inventions and business methods"—namely "instantaneous photographs and newspaper enterprise"—contributed to the invasion of private and domestic life, preventing the implementation of a "right to be left alone".[2]

In accordance with the Fourth Amendment of the Bill of Rights, Warren and Brandeis' view derived a right to privacy from the entitlement to individual freedom from unwarranted intrusion and focused on the harm caused by physical access to a person and his or her possessions. While subsequent development in U.S. constitutional law led to an account of privacy based on non-interference over one's intimate and personal decisions, the case-law based on the Fourth Amendment further expanded the concept defended by Warren and Brandeis.[3] As the employment of wiretapping, bulk surveillance and eavesdropping techniques by law enforcement authorities became more frequent, American jurisprudence needed to abandon a view on privacy that relied on the physical world and moved towards the notion of "reasonable expectation of privacy", as enunciated for the first time in the landmark case of *Katz v. United States*.[4]

In Europe the conceptualisation of privacy was likewise substantially defined by its relationship with technology. Originally, Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)[5] played a crucial role, including the protection of the fundamental right to privacy within in its primary purpose of protection against arbitrary interference with private and family

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

[2] *Warren; Brandeis*, [14], p. 195.

[3] *DeCew* [4]. In the book, the author derives from these distinct developments in US law the distinction between (1) constitutional or decisional privacy and (2) tort or informational privacy.

[4] *Katz v. United States*, 389 U.S. 347 (1967).

[5] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4.11.1950.

life, home and correspondence. Then, in 1981, a significant evolution was led by the Council of Europe's Convention 108 (CETS No. 108), which conceptualised privacy in terms of "data protection" by taking account of "the increasing flow across frontiers of personal data undergoing automatic processing".[6] The notion of data protection has clarified since then the relationship between privacy and technology, specifying what the object of the protection is and attributing to individuals a fundamental claim to their data, expanding in this way the writ of *habeas corpus* to a writ of *habeas data*.[7]

2.2 Privacy and security

Theorists within the academic field of information and computer ethics have debated for long whether privacy is an intrinsic or an instrumental value. While the first view would hold that privacy is good in itself and for its own sake,[8] the second—reductionist—view argues that the importance of privacy derives from—and is reducible to—other values or sources of values.[9] Because it is difficult to defend the view that privacy is important independently from other considerations, and because history has demonstrated that the right to privacy has been susceptible to be defeated in trade-offs with other rights, theorists have put forward alternative proposals to justify privacy. According to these accounts, privacy is conceived as mean for the realisation of—alternatively—property rights, security, autonomy, friendship, democracy, dignity or utility and economic value.

Although it might seem that theoretical speculation has no space in a discussion dominated by law and technology, on the contrary it is convenient to frame our justification of privacy in moral terms before analysing and commenting on the policies in place. Indeed, in trying to find answers to questions like "what kind of value is privacy?" and "why are personal data worth protecting?" such accounts have provided useful insights for legislators called upon to regulate the processing of personal data.[10] Especially when advancements in information and communication technologies (ICTs) have contributed to change social norms, these theoretical debates can be particularly useful to balance apparently opposing values in a correct way.

For the purpose of this article, it is worth considering James H. Moor's theory establishing privacy's relation with the core value of security. According to Moor, core values are shared and fundamental to human evolution, essential for the sustainability and flourishing of cultures and societies. Privacy being the expression of the core

[6] Council of Europe, Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series No. 108, 28.1.1981.

[7] *Rodotà* [10].

[8] *Rossler* [11].

[9] *Thomson* [12].

[10] Jeroen van den Hoven's distinction between the referential and attributive use of personal data is one of the best examples. By exporting these concepts from the philosophy of language and criticising the use of the definition of "personal data" employed by EU data protection laws, van den Hoven proposes that "instead of defining the object of protection in terms of referentially used descriptions, we need to define the object of protection in terms of the broader notion of 'identity relevant information"'. (*van den Hoven* [13].)

value of security, Moor justifies its interpretation in terms of protection of personal information in this way:

> "Without protection species and cultures don't survive and flourish. All cultures need security of some kind, but not all need privacy. As societies become larger, highly interactive, but less intimate, privacy becomes a natural expression of the need for security. We seek protection from strangers who may have goals antithetical to our own. In particular, in a large, highly computerised culture in which lots of personal information is greased it is almost inevitable that privacy will emerge as an expression of the core value, security."[11]

In the context of the cyber-revolution, the increased connectivity derived from the explosive use of computer technologies has conditioned both quantitatively and qualitatively the dissemination of personal information, making the relationship between privacy and security even more concrete. With our world increasingly relying on data, the risks of unauthorised access to personal information pose great dangers not only to our lives but also to the survival of our societies.

- On the one hand, a security breach allowing accidentally or intentionally the destruction, loss, alteration, or non-authorised disclosure of personal data can have a range of significant adverse effects, resulting in physical, material or non-material damage for individuals. Indeed, once our personal information ends up in the wrong hands, limitations to individual rights, discrimination, identity theft or fraud, financial loss and reputational damage become concrete challenges to our security.[12]
- On the other hand, the mass scale of big data analytic techniques has proven to have the potential of weakening the foundation of the democratic governance of our societies. Data mining and the extraction of patterns used to make decisions about users, as well as the possibility of profiling, influencing, nudging and otherwise changing behaviours represent challenges to the collective will that legitimises political power.[13]

While traditional violations of privacy put at risk the security of individuals, new forms of big data interference threaten the security of entire communities. Having

[11] *Moor*, [9], p. 29.

[12] These are some of the potential risks derived from personal data breaches as suggested by *Article 29 Working Party: Guidelines on Personal data breach notification under Regulation 2016/*679.

[13] Being inspired by Council of Europe Recommendation CM/Rec (2010)13, the GDPR defines "profiling" as an automated processing operation "consisting of the use of personal data to evaluate certain personal aspects relating to a natural person [. . .]". By requiring that it must involve some sort of assessment or judgment about an individual or a group of individuals, the GDPR considers profiling more than a simple classification of data in reason of its inherent evaluation of personal aspects used to identify—"to analyse or predict"—characteristics of present or future behaviour. It represents a broadly used practice in an increasing number of sectors—both public and private—helping decision-makers to increase efficiencies and save resources by extracting patterns and placing data subjects into certain categories and groups that allow to predict their likely behaviour, interests, or ability to perform a task. Having raised several questions about the accuracy of its predictions, as well as its inherent risk of discrimination leading to unjustified denial of goods and services, the processes of profiling and automated decision-making are addressed by specific norms of the GDPR.

to protect against these highly technical challenges, legislators find themselves increasingly in need of juridical instruments oriented towards the security of people, software and data. For this reason, data protection laws should start displaying more characteristics in common with cybersecurity policies, allowing technology to shape not only what privacy ought to protect but also how this protection needs to happen. By taking the GDPR as a case-study, the following paragraphs will show how the concepts of privacy and security are converging under the influence of technological advancements.

3 The revolution of the general data protection regulation (GDPR)

3.1 The fundamental right to data protection

On 25 May 2018, the General Data Protection Regulation came into force, finally repealing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Although the objective of the Directive had been that of harmonising fundamental rights related to data protection and to ensure the free flow of personal data within the internal market, differing national interpretations and applications led to fragmentation and a lack of legal clarity. By directly applying to its addressees and not requiring further implementation measures by EU Member States, the Regulation constitutes a suitable legal instrument for EU citizens willing to enforce their fundamental right to data protection as outlined by Art. 8 of the Charter of Fundamental Rights of the European Union [14] and Art. 16 of the Treaty on the Functioning of the European Union (TFUE).[15]

By not mentioning the word "privacy" in any of its eleven chapters and ninety-nine articles, the GDPR marks the definitive emancipation of the right to data protection from the right to privacy, detaching it also from the "right to be left alone" and the protection of secrecy about personal matters. Constituting a direct response to the rapid technological advancements that allow making use of personal data on an unprecedented scale, the GDPR represents an essential step towards the development of a European data-driven economy within the context of the Digital Single Market

[14] According to Art. 8 of the Charter of Fundamental Rights of the European Union "(1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority."

[15] By expanding the field of application of data protection prescriptions to the sectors of external security, Art. 16 TFUE states that "(1) Everyone has the rights to the protection of personal data concerning them. (2) The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union."

strategy.[16] While the Directive considered data to be the property of the data subject and aimed to regulate—-statically—its exchange with controllers, the Regulation aims to govern—dynamically—a much more intertwined technological context, with the purpose of neither restricting nor prohibiting the free movement of personal data within the Union.[17]

In this sense, the GDPR assumes the character of a *lex generalis* and addresses the serious risk of circumvention led by technological evolution by establishing technologically neutral measures to protect natural persons.[18] By "taking into account the state of the art" and the "costs of implementation", the GDPR prescribes controllers with the obligation to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk".[19] In this way and for the first time in data protection legislation, the GDPR requires controllers to process personal data securely, transforming what once were good and best practices into legal requirements. Introducing a real "security principle" within the context of data protection, Art. 5(1)(f) asserts that personal data is to be *"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"*.

3.2 Accountability and a risk-based approach

In order to demonstrate how data protection legislation is highly intertwined with the security of individuals and data, and how the GDPR considers the enforcement of security measures to protect personal data to be central to its scope, the principle of accountability should be taken as starting point. As thoroughly defined by Opinion 3/2010 of the Art. 29 Working Party (WP29), "a statutory accountability principle would explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations [...] and demonstrate this on request". [20] While this formulation in the context of data protection is not in itself new, but rather derives from OECD privacy guidelines adopted in 1980, the GDPR provides specific legal affirmation of accountability-based mechanisms both in Recital 78 and Art. 24(1). The latter states:

> "*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and*

[16] Connections between the data protection regulation and the Digital Single Market are evident since EC President Junker's 2014 Political Guidelines "A New Start for Europe, My Agenda for Job, Growth, Fairness and Democratic Change" in which he states "[...] We must make much better use of the great opportunities offered by digital technologies, which know no border. To do so we will need [...] to break down national silos in telecoms regulation, in copyright and data protection legislation [...]. To achieve this, I intend to take [...] ambitious legislative steps towards a connected Digital Single Market, notably by swiftly concluding negotiations on common European data protection rules [...]."

[17] Art. 1(3) of the GDPR.

[18] Recital 15 of the GDPR.

[19] Art. 32(1) of the GDPR.

[20] Opinion 3/2010 on the principle of accountability (WP 173), p. 3 [2].

organisational measures and be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."

According to the Regulation, the controller is called upon to identify the security measures that are suitable to protect the processing of personal data and to continuously monitor these measures' consistent appropriateness for the risks highlighted by technological developments. Minimising the risk of unauthorised access, misuse and loss of personal data, the implementation of these measures should foster compliance with the obligation of the Regulation, and be a useful tool for data protection authorities in their enforcement tasks. In this sense, the obligations deriving from the Regulation do not operate in an indiscriminate manner but take into consideration the risks that might arise in a specific processing, as well as the nature, scope, context and purposes of that processing. By offering controllers the opportunity to consult data protection authorities in case the technical and organisational measures employed would not sufficiently mitigate risks, the GDPR considers *risk* as the central parameter for the definition of further obligations.[21]

Therefore, the principle of accountability is strictly connected with a risk-based approach to data protection, consisting of the identification and analysis of risks to the rights and freedoms of data subjects, and which is antecedent to the definition and design of appropriate security measures.[22] By considering state of the art technology, the personalisation of both technical and organisational measures should derive from a twofold analysis of risks which is composed by their assessment and their management: first, the impact of threats and vulnerabilities should be evaluated, then verification, checking, minimisation or elimination should finally ensure that the measures taken will guarantee appropriate levels of security and confidentiality.

3.3 Data protection impact assessment (DPIA)

Permitting the enforcement of accountability, and in line with the risk-based approach of the Regulation, the Data Protection Impact Assessment (DPIA) is one of the most relevant and innovative instruments of the GDPR.[23] The DPIA is a mechanism for building and demonstrating compliance with the Regulation which aims to describe the envisaged processing and its purpose, to evaluate its necessity and proportionality, to assess risks deriving from it to the rights and freedoms of data subjects, and to enlist the appropriate measures addressing those risks.[24] This kind of assessment is not due for any form of processing of personal data, but only for those "likely to result in a high risk to the rights and freedoms of natural persons", particularly when

[21] *Gellert* [6].

[22] Recital 83 of the GDPR further attributes to the controller or processor the evaluation of inherent risks in order to implement measures that mitigate them, maintaining security and preventing processing in infringement of the Regulation.

[23] Its significance and role are clarified in Recital 84: "In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk [...]".

[24] Art. 35(7) of the GDPR.

new technologies are employed.[25] In particular, Art. 35(3) offers useful examples of cases in which the processing might require a DPIA:

(a) *a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning a natural person or similarly significantly affect a natural person;*
(b) *processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or*
(c) *a systematic monitoring of a publicly accessible area on a large scale*.

With the adoption of guidelines,[26] the General Data Protection Regulation has further elucidated the notion of processing operations that are "likely to result in a high risk", providing a more concrete set of criteria to be taken into consideration for determining the necessity of a DPIA:

1. evaluation, scoring, profiling or predicting techniques that would require the processing of data subject's personal information concerning "the performance at work the economic situation, health, personal preferences or interest, reliability or behaviour, location or movements";[27]
2. processing operations aiming to take automated decisions on data subjects, and which would produce legal effects or may similarly affect in a significant way the natural person;[28]
3. processing operations used to monitor, observe, or control data subjects in a systematic way—for, especially if information is collected in public (or publicly accessible) spaces, individuals might be unaware of being subjected to such processing and it may be unavoidable for them;
4. operations processing sensitive data or data of a highly personal nature, such as, for example, political opinions, biometric data, medical records, criminal convictions or offences;
5. data processed on a large scale. In other words, when the number of data subjects concerned, the volume of data, the retention or permanence, and/or the geographical extent of the processing activity might represent contributing factors to assess the high risk of the processing operation;
6. operations processing data by matching or combining datasets which might exceed the reasonable expectation of data subjects;
7. processing operations whose data may concern vulnerable data subjects, including children, employees, asylum seekers etc. This kind of processing may increase the power imbalance between controllers and data subjects;
8. processing operations requiring the innovative use of new technological or organisational solutions like, for example, the combined use of finger prints and face

[25] Art. 35(1) of the GDPR.

[26] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248 rev. 01) [1].

[27] Recital 71 and 91 of the GDPR.

[28] Art. 22(1) of the GDPR.

recognition techniques for improved physical access control. Indeed, the GDPR highlights that "the achieved state of technological knowledge" can lead to new forms of data collection and usage that may generate high risks to the rights and freedoms of individuals; and

9. processing operations that prevent data subjects "from exercising a right or using a service or a contract".[29]

While the Art. 29 Working Party considers that, in most cases, when two of these criteria are met a Data Protection Impact Assessment will be mandatory, data controllers can decide whether a processing that meets only one of these criteria requires a DPIA. In both cases, a data controller can still consider the processing operation not to be "likely to result in a high risk" but should be able to justify and document the decision for not carrying out a DPIA. A DPIA should be carried out "prior to the processing", nonetheless it should represent a continual process that is regularly reviewed and re-assessed. By always seeking the advice of the Data Protection Officer (DPO), the controller should also seek—where appropriate—the views of data subjects or their representatives. The controller may also require a consultation with the supervisory authority, especially whenever sufficient measures to reduce the residual risks of the processing cannot be found. Finally, although this is not legally required by the GDPR, the controller can decide to publish the DPIA, fostering transparency and trust in its processing operations.

3.4 Data breach notification

Although the DPIA has the characteristics of a well-consolidated risk management practice,[30] breaches to the security of personal data may always occur, resulting in a concrete threat to the security of data subjects as well as a practical challenge for data controllers. According to the GDPR, a personal data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".[31] While this assumes that all personal data breaches derive from security incidents, the Art. 29 Working Party specifies in its guidelines that not all security incidents have to involve personal data breaches. According to Opinion 03/2014, personal data breaches can be divided into three—not mutually exclusive—categories:

a. "Confidentiality personal data breach"—consisting in the unauthorised or accidental disclosure of access to personal data;
b. "Integrity personal data breach"—consisting in the unauthorised or accidental alteration of personal data.
c. "Availability personal data breach"—consisting in the unauthorised or accidental destruction or loss of access of personal data.

[29] Recital 91 and Art. 22 of the GDPR.

[30] e.g. ISO 31000:2009, Risk management—Principles and guidelines, International Organisation for Standardisation (ISO).

[31] Art. 4(2) of the GDPR.

When a personal data breach occurs, the controller should activate immediately all defensive measures—both operative and organisational—to mitigate and manage the crisis, including a potential notification to the supervisory authority and a communication to data subjects. Indeed, in most cases, supervisory authorities and data subjects are often unaware of the occurrence of a personal data breach, preventing them from taking action and protecting themselves from detrimental consequences. By imposing a notification requirement on controllers, the GDPR affirms the rights of individuals and limits the negative impact of a personal data breach. According to article 33(1) of the GDPR:

> "*in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons*."

Therefore, the obligation to notify a data breach should not be automatic but should derive from an analysis of the risks on the rights and freedoms of natural persons. In case the personal data breach is likely to result in a high risk, controllers should—together with notifying the supervisory authority—communicate "without undue delay" the personal data breach to exposed individuals as well. If controllers do not respect the timing of the obligation, supervisory authorities are entitled to apply all the available corrective measures: *i.e.*, issue warnings, reprimands or fines, impose a temporary or definitive limitation to the processing, order the rectification or restriction of processing, withdraw certification or order the suspension of data flows.[32]

Further demonstrating how data protection legislation is converging with cybersecurity measures, the obligation to notify a personal data breach under the GDPR resembles—and sometimes is associated with—other similar notification obligations under different legal instruments. Although varying between Member States, these requirements inter-relate with the GDPR and include:

- Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation);[33]
- Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive);[34]
- Directive (EU) 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the ePrivacy Directive); [35]

[32] Art. 58(2) of the GDPR.

[33] Art. 19(2) of the eIDAS Regulation requires trust service providers to notify supervisory bodies when breaches of security or losses of integrity impact significantly on the trust service provider or on the personal data stored therein.

[34] Art.14 and Art.16 of the NIS Directive require digital service providers and operators of essential services to notify security incidents to their competent authorities.

[35] Art. 3 of the ePrivacy Directive required that providers of publicly available electronic communication services ought to notify breaches to competent national authorities.

- Directive 2009/136/EC (the Citizens' Rights Directive) and Regulation 611/2013 (the Data Breach Notification Regulation).

3.5 Privacy by design and privacy by default

As argued by *Cavoukian*, the "privacy by design" approach illustrates the idea that privacy concerns have to be kept in mind from the initial phase of design of technological systems processing data. In this way, "data protection needs to be viewed in proactive rather than reactive terms",[36] making privacy considerations preventive and *ex ante* instead than remedial and *ex post*. With privacy as a default setting, data protection requirements are embedded into the architecture of information communication technology, ensuring that personal data is automatically protected in any given system or business practice.

Although some elements of the "privacy by design" principle could already be found in the Data Protection Directive 95/46/EC,[37] for the first time Art. 25 of the GDPR formalises "data protection by design and by default" into formal law, by including it in the general obligations of controllers and processors. According to the Regulation, controllers shall implement appropriate measures—both technical and organisational—by taking into account data protection concerns not only when determining the means for processing and during the processing itself,[38] but also when developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task.[39]

With technologies becoming more convoluted and unintelligible, the burden of responsibilities of privacy compliance can hardly be borne by the average user. The "privacy by design" approach implies that a project's design needs to be carried out taking into consideration the final recipient of the technology. Being a user-centric methodology for data protection compliance, it incorporates the protection of individuals and their personal data in the requirements of the whole project lifecycle. Therefore, the use of Privacy Enhancing Technologies (PETs)—i.e., ICT systems that base from scratch their design on the minimisation of risks derived from personal data misuse—is favoured by the Regulation. According to this view, the development of ICT systems and services integrating safeguards and implementing data protection principles allows effectively combating threats to the security of individuals such as identity theft, fraud, and discriminatory profiling.[40]

3.6 Pseudonymisation

The concept of pseudonymisation is defined in Art. 4(5) of the GDPR as:

[36] *Cavoukian*, [3], p. 126.

[37] Recital 46 of the Data Protection Directive.

[38] Art. 25 of the GDPR prescribes the moment in time in which the implementation of the specific measures defined in Art. 24 should occur.

[39] Recital 78 of the GDPR.

[40] Preliminary Opinion on privacy by design (Opinion 5/2018) [5].

> "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*".

This represents a well-established data protection and security practice which disassociates the identity of a data subject from its processed personal data. This de-identification process replaces a particular set of characteristics relating to the data subjects with so-called *pseudonyms* that do not allow the direct derivation of the original *personal identifier*—i.e., information or pieces of information that make identification possible.[41] Granting in some cases the possibility of a re-identification, pseudonymisation maintains an association between personal identifiers and pseudonyms, providing that the "additional information" necessary to reverse the process is secured. The GDPR puts a lot of emphasis on the securing of the additional information, stating that controllers should separate it from the pseudonymised data—either logically or physically—allowing the possible destruction of such association when the intention is to make the process irreversible.

The notion of pseudonymisation is often confused with that of anonymisation, leading to the common mistake of considering pseudonymised data as deserving the same level of protection as anonymous data. On the contrary, while anonymisation is a process that irreversibly alters personal data in a way that it can no longer be reconnected to the data subject, removing definitively the association between the identifying dataset and the identity of the data subject, pseudonymisation is based on the existence of this association.[42] The GDPR explicitly clears up this misinterpretation in Recital 26, where it states that pseudonymised data continues to be conceived of as personal data by reason of the fact that it remains attributable to a natural person with the use of "additional information". Indeed, pseudonymisation techniques start with a single input (the original dataset) and result in a couple of outputs (the pseudonymised dataset and the additional information) that can together re-establish the original input. While the pseudonymised dataset is a modified version of the original dataset where initial identifiers have been substituted with pseudonyms, the additional information provides the link between pseudonyms and the identities of the data subjects. This decoupling of the original dataset into two parts allows the two different outputs to have a relationship regarding the specific data subject if they are in combination with each other. Therefore, all the relevant data protection principles foreseen by the Regulation apply both to indirect identifiers related to a data subject and to pseudonymised data.

Recognising the possible benefits of pseudonymisation, the Regulation refers to it fourteen times both as a data-protection-by-design mechanism and as a technique promoting the security of operations processing personal data:

[41] According to the ISO/TS 25237:2017 standard, a pseudonym is "a personal identifier that is different from the normally used personal identifier and is used with pseudonymised data to provide dataset coherence linking all the information about a data subject, without disclosing the real world person identity".

[42] Hintze, El Emam [7].

- Art. 25(1) considers pseudonymisation an appropriate technical and organisational measure implementing effectively data protection principles and integrating the necessary safeguards into the processing. By favouring respect for the principles of necessity, data minimisation, data accuracy, as well as supporting the data protection goal of unlinkability (which promotes the reduction of personal data linked across different data processing domains), pseudonymisation techniques represent the perfect exemplification of data protection by design.
- Art. 32(1) considers pseudonymisation—as well as encryption—an appropriate technical and organisational measure for ensuring appropriate levels of security. Allowing concealment of the identity of the data subject and reducing the risks to the rights and freedom of individuals, pseudonymisation enhances the security and integrity of personal data.

Finally, it has been pointed out by several sources that, within the provisions of the GDPR, pseudonymisation allows a certain degree of "relaxation" of some of the controller's obligation.[43] Indeed, in five different sections of the Regulation it appears that:

1. pseudonymisation may facilitate the processing of personal data beyond their original collection purpose;[44]
2. pseudonymisation may reduce the possibility of identifying individuals when personal data breaches occur, decreasing the risk of harm to data subjects and positively impacting the process of risk evaluation which is functional to notify personal data breaches to data protection authorities;[45]
3. pseudonymisation represents a relevant safeguard for processing personal data for archiving purposes in the public interest, as well as for scientific or historical research purposes or statistical purposes;[46]
4. pseudonymisation may avoid controllers providing a data subject with access to data, with rectification and erasure of data, with restrictions on processing or with data portability;[47] and
5. pseudonymisation may be considered a mitigating factor for supervisory authorities calculating potential fines.[48]

4 Conclusion

In conclusion, the article has demonstrated that the GDPR's focus on security goes beyond Art. 32 on the "Security of Processing". Not only does the Regulation include among its principles the security of personal data, but considerations about the security of individuals are also at the basis of the risk evaluation on which the principle of

[43] Maldoff, [8].

[44] Art. 6(4) of the GDPR.

[45] Art. 33 and Art. 34 of the GDPR.

[46] Art. 89(1) of the GDPR.

[47] Art. 11 and Art. 12(2) of the GDPR.

[48] Art. 83(2) of the GDPR.

accountability is founded. Being concrete expressions of the principle of accountability and the risk-based approach, innovative data protection measures like DPIA and data breach notifications show how the GDPR puts emphasis both on the security of data subjects and on the security of processing operations. Through preliminary assessment of risks to individuals and consequent implementation of appropriate security measures, security concerns should encourage controllers to plan in advance—aiming to prevent incidents—and react in a timely manner whenever a privacy violation occurs. Finally, the employment of ICT solutions that—"by design"—integrate security measures implementing data protection safeguards has been prescribed as a way to ensure compliance with the obligations of the Regulation. Through detaching data subjects from personal data and resulting in the minimisation of risks to the rights and freedoms of individuals, the adoption of security measures like pseudonymisation may allow a "relaxation" of some of the data protection requirements of the GDPR.

Albeit theoretically grounded, the abovementioned discussion may have important implications for practitioners which will need to be further analysed in future publications. By acknowledging that the proper implementation of data protection always requires data security measures, professionals should question whether data protection should be considered a separate area of responsibility and expertise to data security. Furthermore, in recognition of the fact that data protection requires a combination of both legal compliance and technical solutions for practical implementation, cooperation between Data Protection Officers and information security officers should be promoted and enhanced.[49]

References

1. Article 29 Working Party: Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" (2017). for the purposes of Regulation 2016/679 (WP248 rev. 01) (2017). Available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
2. Article 29 Working Party: Opinion 3/2010 on the principle of accountability. WP (WP 173) (2010). Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf
3. Cavoukian, A.: Privacy by Design: the Definitive Workshop. Identity in the Information Society (2010)
4. DeCew, J.W.: Pursuit of Privacy: Law, Ethics, and the Rise of Technology. Cornell University Press, Ithaca (1997)
5. European Data Protection Supervisor (EDPS): Protection Supervisor (EDPS): Preliminary opinion on privacy by design (Opinion 5/2018) (2018). Available at https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf
6. Gellert, R.: Understanding the notion of risk in the general data protection regulation. Computer Law Secur. Rev. (2018). Available at https://www.sciencedirect.com/science/article/pii/S0267364917302698

[49] On various occasions, including at the Europol´s Data Protection Experts Network ERA conference "Freedom and Security—Killing the Zero Sum Process", the Data Protection Officer of the European Union Agency for Law Enforcement Cooperation (Europol) has put forward this argument.

7. Hintze, M., El Emam, K.: Comparing the benefits of pseudonymisation and anonymisation under the GDPR. J. Data Protect. Privacy 145–158 (2018). Available at https://www.ingentaconnect.com/content/hsp/jdpp/2018/00000002/00000002/art00005
8. Maldoff, G.: Top 10 Operational Impacts of the GDPR, Part 8: Pseudonymization (2018). Available at https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/
9. Moor, J.H.: Towards a theory of privacy in the information age. Computer Soc. (1997)
10. Rodotà, S.: Tecnologie e Diritti, il Mulino, Bologna (1995)
11. Rössler, B.: Privacies: Philosophical Evaluations. Stanford University Press, Stanford (2004)
12. Thompson, J.J.: The right to privacy. Philos. Publ. Affairs **4**, 295–314 (1975)
13. van den Hoven, J.: Information technology, privacy, and the protection of personal data. In: van den Hoven, J., Weckert, J. (eds.) Information Technology and Moral Philosophy, pp. 301–322. Cambridge University Press, Cambridge (2008)
14. Warren, S., Brandeis, L.: The right to privacy. Harvard Law Rev. **4**(5), 193–220 (1890). Available at https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents