The International Journal of Human Rights

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/fjhr20

Informational privacy post GDPR – end of the road or the start of a long journey?

Aysem Diker Vanberg

To cite this article: Aysem Diker Vanberg (2021) Informational privacy post GDPR – end of the road or the start of a long journey?, The International Journal of Human Rights, 25:1, 52-78, DOI: 10.1080/13642987.2020.1789109

To link to this article: https://doi.org/10.1080/13642987.2020.1789109

THE INTERNATIONAL JOURNAL OF HUMAN RIGHTS
2021, VOL. 25, NO. 1, 52–78
https://doi.org/10.1080/13642987.2020.1789109

Routledge
Taylor & Francis Group

Informational privacy post GDPR – end of the road or the start of a long journey?

Aysem Diker Vanberg

School of Law and Criminology, University of Greenwich, London, UK

ABSTRACT

The General Data Protection Regulation (GDPR) is a far-reaching legal instrument that regulates the collection and use of personal data by private actors, individuals and by governments. In this respect, the GDPR is indeed a key legal instrument for protecting informational privacy. This article will analyse and discuss the impact of the GDPR on the right to privacy particularly in the context of data protection. It also explores whether the GDPR in itself is adequate to ensure the right to privacy in the European Union (EU) and whether the protection provided by the GDPR can be supplemented by other means. The article finds that while the GDPR is a significant step in the right direction to protect informational privacy, it is certainly not the end of the journey. It argues that on its own, the GDPR cannot fully address the imbalance of power between data subjects and data controllers. Hence, it needs to be complemented by other regulatory tools such as the ePrivacy Regulation, EU competition law and Consumer Protection rules. Furthermore, some provisions in the GDPR must be revisited in the near future to ensure they do not become obsolete.

ARTICLE HISTORY
Received 4 May 2020
Accepted 22 June 2020

KEYWORDS
European Union; GDPR; privacy; ePrivacy Regulation; human rights; right to privacy

1. Introduction

Sound data protection laws are crucial for protecting fundamental human rights including the right to privacy. Nevertheless, due to the advancement of technology coupled with the rise of data centric business models, the right to privacy is under threat. The General Data Protection Regulation (GDPR) a far-reaching legal instrument regulating the collection and use of personal data by private actors, individuals and by governments. In this respect, the GDPR is a key legal instrument for protecting informational privacy.[1]

This article will analyse and discuss the impact of the GDPR on the right to privacy, particularly in the context of data protection. It also aims to explore whether the GDPR in itself is adequate to ensure the right to privacy in the European Union (EU) and whether the protection provided by the GDPR can be supplemented by other means. There are a vast number of articles written on the GDPR and various aspects of it. However, there is no article in the literature that specifically analyses the impact of the GDPR on informational privacy. In this respect, the article fills this gap. The article

CONTACT Aysem Diker Vanberg a.dikervanberg@greenwich.ac.uk

highlights that GDPR is a significant step in the right direction to protect informational privacy, however it cannot fully address the imbalance of power between data subjects and data controllers. To deal with this shortcoming, the article suggests that the GDPR needs to be complemented by other regulatory tools such as the ePrivacy Regulation, EU competition law and other consumer protection laws.

In order to achieve its objective, the article will first discuss the origins of the right to privacy and the two systems in the EU that includes the European Convention on Human Rights (ECHR) and the EU System and the divergence and differences between these two systems. The article will then discuss the General Data Protection Regulation and the key provisions of the GDPR pertaining to informational privacy. Subsequent to this, the article will consider some of the issues pertaining to the GDPR and informational privacy. Finally, conclusions are drawn and recommendations made to ensure that the GDPR has teeth in achieving its desired goals, particularly in strengthening informational privacy.

2. The origins of the right to privacy and its development in Europe

The right to privacy is not a newly developed concept. As noted by Çınar from the earliest days of mankind, human beings have always shared public spaces with others whilst retaining a personal and private life, as encapsulated by the right to privacy.[2]

The right to privacy is a fundamental human right contained in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR).[3] The main issue pertaining to the right to privacy is that there does not seem to be consensus on its limitations and what it entails. As stressed by Post,[4] 'privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all'. Nevertheless, numerous prominent scholars attempted to find some common understanding as to what is meant by privacy.[5]

In their seminal article entitled Right to Privacy,[6] Warren and Brandeis articulate the right as the right to be let alone. In the digital age, everything a person does online generates or implicates data that can compromise their right to privacy. Hence, arguably the right to be left alone as articulated by Warren and Brandeis is difficult to ensure, particularly with the rise of online media and services that are financed via data-driven targeted advertising and rely on a business model of collecting data. According to Cornell,[7] the right to privacy involves several key components. These include territorial and bodily integrity, personal autonomy and private entity, such as within a private sphere for seeking information as well as making intimate and private decisions related to religion, sexuality and the protection of personal data.

Finally, the American privacy scholar Solove made an attempt to approximate the concept of privacy and refers to six main categories that can all be used when referring to privacy. According to Solove, the right to privacy entails: (1) the right to be left alone, (2) limited access to self, (3) secrecy, (4) control over personal information, (5) personhood – protection of identity and dignity, and (6) intimacy.[8]

In Europe, there are two systems in place, working in parallel, that safeguard the protection of fundamental human rights including the right to privacy and the protection of personal data. These systems are governed by the Council of Europe and by the EU.

3.1. The European convention on human rights

The first system that safeguards the right to privacy and data protection is the ECHR, an international agreement between the 47 States of the Council of Europe. There are also third states which are members of the ECHR such as Russia, Turkey, and the Switzerland. Complaints by individuals pertaining to alleged breaches of human rights, including the right to privacy is heard by the European Court of Human Rights (ECtHR) in Strasbourg. The ECHR had a significant impact in shaping the case law in the EU, as all the member states of the EU are members of the ECHR. Furthermore, both the General Court and the CJEU, from time to time, refer to Article 8 of ECHR in their judgments, which shows the ongoing influence of the ECHR on the EU legal system .[9]

Article 6 (2) TEU introduced by the Treaty of Lisbon concerns the accession of the EU to ECHR. It reads as follows:

> The Union shall accede to the [ECHR]. Such accession shall not affect the Union's competences as defined in the Treaties.

The draft Accession Agreement of the EU to the ECHR between the 47 Member States of the Council of Europe and the EU was finalised on 5 April 2013. Pursuant to Article 218 (11) of the Treaty on the Functioning of the EU (TFEU), the European Court of Justice (CJEU) were asked to give its opinion on the compatibility of the draft agreement with EU law. The CJEU has identified some problems in relation to the draft agreement. The Court delivered its opinion on 18 December 2014.[10] Referring to Protocol No 8 relating to Article 6(2) of the Treaty on European Union (TEU), the Court retracted that the accession agreement had to fulfil certain conditions to make provision for preserving the specific characteristics of the EU and of EU law, as well as to ensure that accession does not affect EU institutions' competences or the powers.[11] In that context, the Court concluded that accession to the ECHR was likely to upset the underlying balance of the EU and undermine the autonomy of EU law. The CJEU also noted that the advisory opinion mechanism foreseen by Protocol 16 to the ECHR would affect the autonomy and effectiveness of the preliminary ruling procedure provided for in the TFEU.[12]

For the time being no new accession agreement has been drafted. Nevertheless, the Parliament and the Commission still emphasise the need for EU accession to the ECHR.[13]

3.2. The European Union system

The second system that safeguards the protection of fundamental human rights including the right to privacy is the Court of Justice of the European Union (CJEU) based in Luxembourg, which is a EU institution. Respect of human rights is part of the constitutional principles of the EU.

In 2009, with the enactment of the Treaty of Lisbon, the Charter of Fundamental Rights of the European Union (the Charter) entered into force.[14] The fundamental human rights including the right to privacy and data protection are laid down in the Charter.

The Treaty of Lisbon provides a legal basis for data protection legislation covering all aspects of Union Law.[15] Article 16(2) TEU provides that EU legislature shall lay down the rules relating to the processing of personal data. Below the article will analyse the approaches to the right to privacy and the right to data protection under the ECHR and the EU.

3.3. Approaches to the right to privacy and the right to data protection

3.3.1. The ECHR approach

Both the ECHR and the Charter have a provision on privacy. Article 8 of the ECHR provides that:

(1) Everyone has the right to respect for his private and family life, his home and his correspondence.
(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The ECtHR has interpreted the above provision in a fairly flexible way more than a purely negative obligation of the 'right to be let alone' as envisaged by Warren and Brandeis[16]. The ECtHR has interpreted the interests protected by Article 8(1) dynamically. Article 8 encompasses a wide variety of information such as traffic data on telephone calls,[17] video surveillance images[18] and e-mails sent from work,[19] which were all seen to fall within the scope of private life.

In order to establish the existence of an interference with protected interest under Article 8(1) ECHR, the Court takes into consideration several factual circumstances. The mere storage of data relating to private life of an individual may amount to violation of Article 8(1) ECHR. In Leander,[20] the storage of data concerning the applicant's private life in police files, the fact that they were shared with his employer, and consequently the refusal to allow the applicant to contest that data, amounted to an interference with the right to privacy. This position was reaffirmed in S. and Marper[21] when the Court held that mere retention and storage of personal data by public authorities has a direct impact on the private life of the individual concerned and cannot be justified by its future use. When examining whether there has been an interference with Article 8(1) the Court considers whether the use of information goes beyond which was reasonably foreseeable by the applicant. In Perry v UK, a security camera covertly filmed the applicant, after he refused to take part in an identification parade[22].

Article 8(1) ECHR sets out the general principle and Article 8(2) ECHR allows interference with the right to respect for private and family life, home and correspondence as long as it is compliant with the law and is necessary in a democratic society.

The scope of the right is determined by taking into consideration whether there is a reasonable expectation of privacy. Expectation of privacy can be slightly lower when the person in question is a public figure. In Bohlen v Germany, the applicant, a famous German musician and artistic producer, complained of Germany's failure to protect him against the use of his first name by a tobacco company in an advertisement campaign without his consent. The court concluded that the applicant was a public figure who could not claim the same degree of protection of his private life as an individual not in the public eye[23]. This however does not entail that well known figures do not have the right to privacy[24]. The right to privacy is not an absolute right and there might be clashes between Article 8 and other Convention rights such as the freedom of expression

incorporated under Article 10 of the ECHR. When balancing Article 8 of the ECHR and the freedom of expression protected by Article 10, the ECHR applies several criteria. They include whether sharing the information (interference with the right) contribute to a debate of general interest; how well known the person concerned is, the method of obtaining the information, the reliability of the information, the content, form and consequences of the publication and the severity of the sanction imposed[25]. In other words, if there is a general interest in disclosing information coupled with other factors, freedom of expression may be given priority over the right to privacy.

3.3.2. The European Union approach

Article 7 of the Charter states that 'Everyone has the right to respect for his or her private and family life, home and communications'. According to both the ECtHR and the CJEU the term private life needs to be interpreted broadly.[26]

The right to respect for private life had been and continues to be significant principle of EU law.[27]

Article 8 of the Charter concerns the fundamental right to the protection of personal data. Article 8 of the Charter asserts that:

(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.

Case law of the CJEU that concerns Article 7 and Article 8 of the Charter offer valuable insight.

In one of its early decisions, in Rundfunk,[28] the CJEU noted that 'the mere recording by an employer of data by name relating to the remuneration paid to employees cannot constitute an interference with private life' under Article 8 ECHR. The Court suggested that such recording would constitute personal data processing and fall under the data protection rules. It is worth noting that in this case CJEU explicitly made reference to Article 8 ECHR.

Article 52(1) of the Charter accepts that limitations may be imposed on Charter rights, as long as they are provided by law, respect the essence of those rights and are proportionate (necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.).

Bavarian Lager[29] concerns the conflict between the right of access to documents and data protection law. Bavarian Lager was created to import bottled German beer for public houses and bars in the UK. However, the company could not sell their products easily because most of those establishments in the UK were bound by exclusive purchasing contracts with certain breweries. UK regulations required British breweries to allow public house managers to buy beer from another brewery if the beer was cask-conditioned ('Guest Beer Provision' (GBP)). However, most beers produced outside the UK, like the applicant's, were sold in bottles.[30]

Bavarian Lager lodged a complaint with the Commission in regard to the restriction on imports and claimed that the UK is in violation of EU law. Subsequent to this complaint, the European Commission initiated infringement proceedings against the UK. Nevertheless, following a meeting attended by Commission officials, UK government officials and some industry representatives, these proceedings were dropped. Bavarian Lager was informed of this. Bavarian Lager made several requests under Regulation No 1049/2001 (Access to Documents Regulation) to the Commission for access to documents placed on the file, including full minutes of the meeting with British authorities, including the names of the industry participants.[31] The Commission agreed to disclose the minutes of the meeting but blanked out some names. The Commission held that the applicant had not demonstrated the need for such disclosure as required under Article 8 of the Regulation No 1045/2001 (the former Personal Data Protection Regulation) and argued that Article 4(1) (b) privacy and integrity of the individual exception of Regulation No 1049/2001 (Access to Documents Regulation) applied. The applicant appealed the Commission's decision before the General Court. The General Court asserted that, even though professional activities are excluded from the scope of Article 8 of the ECHR, the mere fact that a document contains personal data does not mean that the privacy or the integrity of the persons is affected.[32] The Court stated that the attendees were at the meeting as representatives of an industry association and the opinions they expressed in the meeting were not attributable to them personally.[33] Hence, the disclosure of the names of the participants would not undermine the protection of their private life and their integrity pursuant to Article 4 (1) (b).[34] The Commission appealed the judgment of the General Court. In the appeal, the CJEU concluded that the General Court erred in limiting the application of the exception in Article 4 (1) (b) to situations in which the privacy or the integrity of the individual would be infringed for the purposes of Article 8 of the ECHR and the ECtHR. In reaching this conclusion, the CJEU relied on the recital 15 of the Personal Data Regulation, which states that Article 6 TEU (which captures Article 8 of the ECHR) applies to processing activities falling outside the scope of Personal Data Regulation. In other words, according to the CJEU, if an activity falls under the Personal Data Regulation, Article 8 of the ECHR is not applicable. Therefore, the CJEU asserted that, where a document requested pursuant to Regulation 1049 contains personal data, the provisions of the Personal Data Regulation become applicable in its entirety.[35] In the light of above, the CJEU held that the Commission was right to require the applicant to demonstrate the necessity of the data disclosure under Article 8 of the Personal Data Regulation and if the applicant failed to do so, the Commission did not have disclose the name of attendees.

In Schecke,[36] the CJEU concluded that by imposing a legal obligation to publish personal data relating to each natural person who was a beneficiary of aid from certain agricultural funds, the Council and the Commission had exceeded the limits imposed by the principle of proportionality. The CJEU found that the requirement breached Art. 8(1) Charter on right to protection of personal data and Art. 7 on right to respect for private life. While the measures were legal and pursued an objective of general interest, and enhanced transparency regarding the use of Community funds the measures could not meet the proportionality criterion. The objective of transparency could not automatically take priority over the right to protection of personal data. According to the CJEU, this balancing act had not been performed.

Another seminal EU case that concerns Article 7 and Article 8 of the Charter is the Digital Rights Ireland case.[37] The Irish law implemented Directive 2006/24/EC (the Data Retention Directive) concerning the retention of data relating to electronic communications, obliging Member States to retain data relating, among other things, to data necessary to trace and identify the source of communication, data necessary to identify the destination of a communication, data necessary to identify the type of communication, and data necessary to identify the location of mobile communication equipment. The Irish High Court referred a question to the CJEU asking whether the Data Retention Directive violated Art. 5(4) TFEU requiring proportionality as well as the right to privacy, the right to protection of personal data, and the right to freedom of expression, established by 7, 8, and 11 of the Charter of Fundamental Rights respectively.

The CJEU concluded that the EU legislature exceeded the limits on it imposed by the principle of proportionality in light of Arts. 7, 8, and 52(1) of the Charter.[38] According to the CJEU, the obligation to retain data relating to a person's private life constituted an interference with the right to privacy guaranteed by Art.7 of the Charter. Moreover, the processing of personal data constitutes an interference with the rights under Art. 8 of the Charter. As noted earlier, Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality. The Data Retention Directive covered all people using electronic communications without exception. It applied to individuals for whom there is no evidence capable of suggesting that their conduct may have a link with a serious crime.[39] While the retention of data allowed authorities to have access pursued a genuine objective of general interest, it was disproportionate. Where interferences with fundamental rights were at stake, the EU legislature's discretion may be limited, depending on a number of factors, including the area concerned, the nature of the right at issue, the nature and seriousness of the interference and the object pursued by the interference.[40]

CJEU concluded that the protection of personal data and the respect of private life were so significant that the EU legislature's discretion had been reduced, and any interference to rights contained under Article 7 and Article 8 of the Charter had to be limited to what is strictly necessary.[41] Subsequent to this case, the Data Retention Directive was annulled.

Article 8 of the Charter distinguishes data protection from the right to privacy and lays down some specific guarantees such as that personal data must be processed fairly for specified purposes and on the basis of consent. Under Article 8 of the Charter, the right to data protection is identified as a distinct right to the right to privacy. This is very significant and very specific to the EU legal order, as data protection is not included in other international human rights documents such as the ICCPR,[42] a multilateral Treaty adopted by the United Nations General Assembly Resolution 2200A (XXI) which entered into force on 23 March 1976, and it is legally binding all Member States who ratify it. This Treaty makes reference to a variety of important civil and political rights such as the right to life, right to privacy, freedom of religion, freedom of speech, freedom of assembly, electoral rights and rights to due process and a fair trial. Nevertheless, it does not make any reference to data protection.

In the same vein, there is no corresponding provision in the ECHR that deals specifically with the protection of personal data. However, the ECtHR frequently applies, Article 8 of the ECHR that concerns the right to privacy, to give rise to data protection as well.[43]

As discussed above, the ECtHR stated in S. and Marper v the United Kingdom that the gathering and holding of personal data, even if it is not used, constitutes violation of the ECHR Article 8.[44] In other words, the lack of a specific provision pertaining to data protection in the ECHR does not mean that data protection is not an important concern for the ECHR system. It is merely covered by Article 8 of the ECHR.

The most prominent view in academic literature is that data protection is a facet of the right to privacy.[45] In other words, privacy law is capable of encompassing aspects of data protection. Accordingly, it could be argued that data protection is the most recent evolution of the right to privacy.[46] Solove argues that privacy evolved in this way because of the proliferation of digital dossiers that created new informational privacy problems.[47] In our digitally connected era, vast amounts of information are collected, stored and analysed. This has created data centric business models, in which companies collect data and use this data for targeted advertising. On a daily basis companies such as Google, Amazon, Facebook collects an unprecedented amount of data from their users, which may have adverse implications on their userś privacy. For instance, Amazon knows not only about our shopping habits but also has sensitive data on us such as our health and sexual preferences, based on the products we purchase. If this data is hacked or passed on to third parties such as one's employer without the consent of the user, this can have grave consequences.

Some scholars do not concur with the above-mentioned prominent view and suggest that data protection is a separate right in itself as it serves a number of purposes that privacy does not and vice versa.[48] According to these scholars, data protection overlaps with the right to privacy, as they both ensure informational data privacy, but it is important to note that broader privacy concepts cannot be used to explain data protection principles such as purpose limitation, data minimisation, data quality and data security.

Despite the academic debate in relation to whether the right to data protection and privacy and whether they are separate rights, the overlap and common grounds between data protection and privacy are irrefutable. More importantly, the jurisprudence of the ECtHR and the CJEU demonstrates that the right to privacy is a very important element of personal data protection and vice versa.[49] In this respect, it can be deduced that strong data protection laws such as the GDPR are significant instruments to protect informational privacy.

The following section will discuss the General Data Protection and the ePrivacy Regulation with a view to analyse important aspects of therein.

4. The GDPR and the ePrivacy Regulation

4.1. The GDPR

25 January 2012, the European Commission proposed a reform of the EU's data protection rules by drafting the General Data Protection Regulation (GDPR)[50] in order to strengthen online data protection rights and boost Europe's digital economy. It was also done to adapt to technological advancements that had taken place in the previous decade, following the introduction of the Data Protection Directive.[51] The reactions to the GDPR have been mixed. Some scholars[52] saw it as a welcome development as it introduces stringent set of rules in terms of safeguarding the rights of data subjects and aims to empower

individuals against the misuse of their personal data. On the other hand, some scholars were more sceptical of the GDPR, as it might lead to red tape, extra costs for data controllers/ data processors as well being incompatible with the fast-paced nature of technology markets.[53]

The GDPR was published in the Official Journal of the EU on 4 May 2016. It came into force 25 May 2018. It replaced the EU Data Protection Directive 95/46/EC.[54] There are several key differences between the Directive 95/46 and the GDPR. First, the GDPR adopts a much wider definition of personal data as it reflects the changes in technology and the way organisations collect data about people. Under Directive 95/46/ EC, Article 2, personal data was defined as any information relating to an identified or identifiable natural person ('data subject'); directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. In other words, according to the Directive personal data included names, photos, email addresses, phone numbers, addresses, and personal identification numbers. Under the GDPR 4(1) personal data is defined as any information that could be used, on its own or in conjunction with other data, to identify an individual 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. Under the GDPR, personal data includes IP address, geo location data and biometric data such as fingerprint scans, and retina scans, which is much wider than envisaged in the Directive. Second, the GDPR places a significant emphasis on consent. The GDPR requires explicit opt- in for the processing of any personal data. This gives more control to users as to how their data is used. Pursuant to Article 7(2) of the GDPR, if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. In other words, the GDPR aims to put an end to long-drawn user agreements with complex language that users hardly read. Any description of data in user agreements use must be short and to the point. A third key difference between the Directive and the GDPR is that under the GDPR both data controllers and processors will be jointly responsible for complying with the data protection rules, meaning if an organisation outsources data entry or analysis to another organisation, both parties will be liable for GDPR violations. Finally, the GDPR introduces some new data subject rights, such as the right to data portability, which did not exist under the Directive. Data subject rights under the GDPR will be analysed below.

In contrast to Directive 95/46/EC, the GDPR applies directly in all Member States. It is supplemented by the national legislation of EU member states. In other words, countries within Europe were given the ability to make their own changes to suit their own needs such as introducing new laws.[55]

Article 5 of the GDPR comprises seven key principles, which has been introduced to guide how personal data can be handled. These seven principles are: (1) lawfulness, (2) fairness, (3) transparency, (4) purpose limitation, (5) integrity, (6) security and (7) accountability.

The GDPR strengthens the rights of individuals with regard to the protection of their personal data and imposes stringent obligations on those processing personal data. It also introduces hefty fines of up to €20 million or 4 per cent of global turnover for those who do not comply .The GDPR is extraterritorial in its scope, which means that it will apply to data processors even when they are not based in the EU, as long as they offer goods and services to individuals and/or monitor the behaviour of individuals such as collecting personal data in the EU. This includes large US digital platforms such as Google, Facebook, Amazon that process the personal data of EU citizens. This is significant as it demonstrates that the GDPR is a key legal instrument not only for the EU but also for the whole world.

Article 4 of the GDPR provides the key definitions. Under Article 4(1) of the GDPR personal data is defined broadly to encompass 'any information relating to an identified or an identifiable person'. This means that even where the data does not directly identify a specific person, if the identity of the person can be deduced from the data; it is still considered personal data. According to the GDPR 4(1) the data subject is the identified or identifiable person whose data is being collected, stored and used. As defined under Article 4 of the GDPR, the data controller is the person or company that decides why and how personal data will be processed. The data processor is an individual or company that processes personal data on behalf of the data controller and can be same as the data controller. Under GDPR data processing is defined broadly to include any activity such as collecting, storing, using and sharing data.

Article 4 (11) of the GDRP provides the definition of consent, which is one of the requirements for processing data legally. Accordingly, 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.

Under Article 6 of the GDPR, companies must ask for consent before collecting or using a data subject's data. Under Art. 6(1) (a) of the GDPR the request for consent must be clearly distinguishable, in an intelligible and easily accessible form, and use clear and plain language.

Another important concept included in the GDPR is privacy by design. Privacy by design is an approach to systems engineering developed by Ann Cavouikan and formalised in a joint report in 1995.[56] As mentioned by Romanou, privacy by design can be articulated as the implementation of several privacy principles in the process of designing technological systems, in a way that privacy rules will be engrained in the operation and management of the processing of the data.[57] The principle is incorporated under Recital 78 and Article 25 of the GDPR. Article 25(1) and Article 25(2) of the GDPR provides that:

(1) 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 rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to

integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

(2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data is not made accessible without the individual's intervention to an indefinite number of natural persons.

Although privacy by design is a well-known concept, the GDPR does something novel by converting a well-known theoretical concept into a legal obligation for all controllers.[58] This crucially means privacy by design is now a legal requirement rather than an optional consideration. As such this is a big step in terms of making data controllers take privacy by design seriously. Privacy by design comprises two key concepts; data protection by design and data protection by default. Data protection by design will entail efforts such as the use pseudonymisation (replacing personally identifiable material with artificial identifiers) and encryption. Data protection by default necessitates providers to have at the onset the most privacy friendly settings. For example, social media platforms like Facebook should be encouraged to set users' profile settings in the most privacy-friendly setting by, for example, by limiting from the start the accessibility of the users' profile so that the users accounts are not accessible by default to everyone. Privacy by design is crucial to ensure that data controllers and companies design their ecosystems with privacy in mind at the onset rather than thinking privacy and data protection when things go wrong. In this respect, the successful enforcement of this provision is crucial for ensuring informational privacy in the online sphere.

Chapter 3 of the GDPR lays out the data privacy rights and principles that all 'natural persons' are guaranteed under EU law.

The articles that concern the right of data subjects are encompassed in articles 12, 13, 14, 15, 16, 17, 18, 19 and 20 of the GDPR.

Under Article 12 of the GDPR data processors need to explain how they process data process data in 'a concise, transparent, intelligible and easily accessible form, using clear and plain language'.

Under Articles 13 & 14 of the GDPR, when collecting personal data, the data processor needs to communicate specific information to data subjects. This entails:

i the identity and the contact details of the controller and, where applicable, of the controller's representative;
ii the contact details of the data protection officer in an organisation;
iii the purpose of the data processing;
iv the categories of personal data concerned;
v the recipients or categories of recipients of the personal data, if any;
vi Finally, if the personal data is transferred to a third country or international organisation, the existence or absence of an adequacy decision by the Commission, or any appropriate or suitable safeguards and the means as to how to obtain a copy of this information.

Article 15 of the GDPR articulates the right of access. Accordingly, data subjects have the right to know certain information about the processing activities of a data controller. This information includes the source of their personal data, the purpose of processing, and the length of time the data will be held, among other items. Most importantly, data subjects have a right to be provided with the personal data of theirs that a data processor is processing. Accordingly, a data subject can ask a data processor what data they hold of them.

Article 16 of the GDPR concerns accuracy. Data processors need to ensure that the data they hold is accurate and complete and according to this principle data subjects have a right to correct inaccurate or incomplete personal data.

Article 17 of the GDRP is about the right to erasure. This right is often referred to as the right to be forgotten. As noted by Rosen[59] in theory this right addresses an important problem in the digital age, as every photo, status update and tweet an individual post stays online for an unlimited time and it becomes very difficult to escape one's past. Perhaps this is the most renowned data subject right, as there have been several legal cases pertaining to this right, and it has generated a lot of media attention. Two cases will be discussed below.

According to Article 17 of the GDPR, data subjects may ask data processors to delete any information about them that a processor may have. There are certain exemptions to this right, which is included in the GDPR. The right to erasure, or right to be forgotten was first affirmed by the CJEU prior to the GDPR in Google v Spain.[60] In 2010, Mario Costeja González filed a complaint with the Agencia Española de Protección de Datos (AEDP), the Spanish Data Protection Agency, against a local newspaper and Google Spain for claims relating to auction notices, showing that Gonzalez failed to pay his social security debts in 1998. Gonzalez argued that the proceedings against him had been resolved and the reference to them was not relevant. He asked the local newspaper, La Vanguardia, to remove the pages or alter them so his personal information was no longer displayed. He also sought for Google Inc. to remove the links to the articles in question so that information pertaining to him did not appear in Google's search results.

The AEDP dismissed González's claims against the newspaper, but allowed those against Google. Google appealed to Spain's high court, which in turn referred three questions to the ECJ:

(a) Whether EU rules apply to search engines if they have a branch or subsidiary in a Member State;
(b) Whether the Directive 95/46/EC applies to search engines; and
(c) Whether a person has the right to request that their personal data be removed from search results (i.e. the 'right to be forgotten')?

Google asserted that as a search engine it should not be regarded as a data processor. Hence it is not subject to the Directive provisions. Nevertheless, paragraph 41 of the Google judgment states that 'the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data'. Furthermore, under Paragraph 94 of the ruling the CJEU concluded that:

> following a request by the data subject […] that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages […] to be inadequate, irrelevant or no longer relevant, or excessive […] the information and links concerned in the list of results must be erased.

In other words, the Court concluded that as a data processor, Google is subject to data protection rules and it is required to remove links from search results, which consists of information, which may no longer be relevant.[61] However, the above landmark decision left some questions unanswered such as whether Google would be required to delete such data only in the EU or globally. Subsequent to this case, the right to erasure was incorporated into the GDPR.

In a case brought by Google against the French data protection authority, the CJEU was asked to clarify the geographical scope of the right to erasure.[62] The case concerned a dispute between the French data protection authority, Commission Nationale de l'informatique et des libertés (CNIL) and Google. On May, 2015, the President of the CNIL served a formal notice on Google that, when granting a request from a natural person for links to web pages to be removed from the list of search results (de-referencing request), it must apply that removal to all its search engine's domain name extensions.[63] In other words, Google was asked to remove information from its search engines not only in a specific member state but globally. Google refused to comply with this request and continued to limit removal of links only on search results conducted in the versions of its search engines in the Member States.[64] In addition, instead of complying with CNIL's order Google proposed to use geo-blocking, whereby internet users would be prevented from accessing the search results at issue from an IP (Internet Protocol) address deemed to be located in the State of residence of a data subject no matter which version of the search engine they used.[65] The CNIL regarded Google's geo blocking proposal insufficient. By an adjudication of 10 March 2016, CNIL imposed a penalty of EUR 100,000 to Google for violation of the GDPR.[66]

Google contended that CNIL only had the power to request and deal with deletion (de orders on the google.fr domain but not for other countries).

In its ruling the Court concluded that the right to erasure should be applied to all domain names from the EU, but it does not extend outside the EU.[67] The Court also noted that the right to be forgotten is not an unlimited right and may be limited by EU member states in order to protect freedom of information. This ruling is arguably problematic as it paves the way for divergent approaches across the EU. This could undermine the unifying effect of the GDPR. Furthermore, by allowing Google not to delete certain information for all domain names this judgment arguably reduces the scope of the right to erasure.

Article 18 and Article 19 of the GDPR concerns the right to restrict processing. Pursuant to this article, data subjects can request processors to temporarily change the way their data is processed. In addition, the data subject has the right to simply object to their data being processed.

Article 20 of the GDPR concerns the right to data portability. This is a novel data subject right which did not exist in the Data Protection Directive 95/46/EC. The right to data portability in the GDPR will require businesses to ensure that they can hand over the personal data provided by a data subject himself/herself in a usable and

transferable format. In other words, this right will enable users to transfer their personal information from one provider to another. For instance, this right will enable a user to transfer all their personal data from Facebook to another social network. The preamble of the GDPR demonstrates that the right to data portability is not just limited to social networking sites but will also be applicable to cloud computing, web services, smartphone systems and other automated data processing systems.[68] The right to data portability will apply to a wide range of areas such as social media, search engines, photo storage, email or online shops. It will be equally applicable to banks, pharmaceutical companies, energy providers, airlines – even small businesses like pizza shops or tailors if they are data controllers.

According to this article data processors need to store users' personal data in a format that can be easily shared with others and understood. Hence, if a data subject asks the data controller to send their data to a designated third party, the data controller is required to do this, if this is technically feasible. Arguably the notion of technical feasibility can undermine the scope of this right as data controllers may suggest that transferring data to a designated third party is not technically feasible due to lack of certain standards.[69] The notion of technical feasibility could have implications for the practical application of this right, as what is technically feasible for one controller may not be technically feasible to another, potentially making widespread controller to controller data transfer unrealistic in practice.

Article 21 of the GDPR concerns the right to object. Data subjects have the right to object to their data being processed by others. Their objection can only be overridden if there is a legitimate basis for processing their data.

The data subject rights included under the GDPR are quite significant rights which aim to give data subjects control over how their data is processed, stored, kept and used. However, other than the right to erasure and the right to access,[70] at time of writing there is limited precedence pertaining to the rights of data subjects, making it difficult to determine whether the users are aware of and are making good use of data subject rights such as the right to data portability.

4.2. The ePrivacy regulation

The ePrivacy Regulation[71] is a proposal for the regulation of several privacy-related topics, particularly in relation to electronic communications within the EU. When it comes to into force it will replace the Privacy and Electronic Communications Directive.[72] The Regulation is primarily aimed at companies operating in the digital economy such as Amazon and Facebook, and specifies additional requirements in relation to the processing of personal data. The ePrivacy Regulation was intended to come into force on 25 May 2018, at the same time as the GDPR, but due to disagreements between Member states concerning its scope it did not.

According to the EU Commission, the key features of the ePrivacy Regulation will be[73]:

i Privacy rules will apply to new players such as Facebook, Messenger and Skype so that these services ensure the same level of confidentiality as traditional telecommunication operators,

ii Stronger rules which will grant the same level of protection in relation to electronic communications for both individuals and businesses,
iii Privacy will be guaranteed for communications and metadata such as the time and the location of a call,
iv More business opportunities will be available for traditional telecommunication operators once consent is given for data,
v The rules on cookies, which has created a dramatic amount of consent requests for internet users, will be streamlined, simplified and it will be made more user-friendly,
vi The new rules will ban unsolicited electronic communications by e-mails, SMS and automated calling machines.
vii Finally, the enforcement of the confidentiality rules in the Regulation will be the responsibility of data protection authorities in the member states, which will make enforcement of these rules more effective.

Arguably, the ePrivacy Regulation is a significant contribution to the strengthening of informational privacy particularly in two ways. First, it will ensure that digital companies such as Facebook, Zoom, WhatsApp are expected to adhere to the same stringent standards as traditional telecommunication operators whilst providing their services. Second, the ePrivacy Regulation is expected to strengthen enforcement of the confidentiality rules, which means that any unlawful interception of online communications data such as listening or tapping will be subject to penalties and that these will be followed up vigorously by the relevant data protection authority in a Member State.

As noted by Voss, while the GDPR ensures the protection of personal data, the ePrivacy Regulation ensures the confidentiality of communications, which may also contain other forms of data including non-personal data (for instance friends data) and data related to a legal person, which is not protected by the GDPR.[74] ePrivacy Regulation will extend the scope of data protection as it will cover data that is currently not protected by the GDPR. Furthermore, whilst the GDPR only concerns protection of data under Article 8 of the Charter, ePrivacy Regulation is concerned about Article 7 of the Charter as it deals with the right to private life and communications. Hence, the ePrivacy Regulation is an important regulatory tool in complementing the GDPR, in particular in relation to communications data.

5. Issues pertaining to the GDPR and informational privacy

5.1. Enforcement issues and potential divergence between member states

As noted above, the GDPR introduced hefty fines for those who do not comply with its principles. As an example, if an organisation does not process an individual's data without consent, it can be fined. Also, if an organisation has a security breach and does not deal with it as required by the GDPR it can be fined.

Before the GDPR was implemented there was growing concern that some companies/organisations could be adversely impacted due to excessive fines. One of the biggest fines under the GDPR was issued against Google. On 21 January 2019, the French data

protection regulator (CNIL) fined Google €50 million for not providing enough information to users about how it uses the data that it gets from different services as well as not obtaining proper consent for processing user data.[75] The case was initiated on May 2018 as CNIL received complaints from the associations None of Your Business (NOYB) and La Quadrature du Net (LQDN). In the two complaints the associations stated that Google did not have a valid basis to process the personal data of its users of its services, particularly for advertisement personalisation purposes. CNIL carried out inspections and concluded that there were two types of breaches of the GDPR. First, CNIL observed that essential information such as data processing purposes, the data storage periods and how personal data will be used for ads personalisation was not easily accessible for users and the information provided by Google was neither clear nor comprehensive.[76] Second, CNIL observed for processing personal data for advertising personalisation, userś consent was not sufficiently informed and the collected consent neither specific nor unambiguous.[77] For instance, before creating an account, the user is asked to tick the boxes 'I agree to Google's Terms of Service' and 'I agree to the processing of my information as described above and further explained in the privacy policy' in order to create an account. Therefore, the user gives his/her consent in full, for all the processing operations carried out by Google based on this consent. This contradicts Article 4(11) of the GDPR, as consent is specific only if it is given distinctly for each purpose.

In Germany, the Federal Commissioner for Data Protection and Freedom of Information (BfDI) imposed a fine of EUR 9,550,000 on the telecommunications service provider 1&1 Telecom GmbH, as the company had not taken sufficient technical and organisational measures to prevent unauthorised persons from being able to obtain customer information.[78]

In the case of 1&1 Telecom GmbH, the BfDI was informed that anyone calling the company's customer service could obtain extensive personal customer data by providing a customer's name and date of birth.[79] The BfDI concluded that this authentication procedure was in breach of Article 32 of the GDPR and asked the company to take appropriate technical and organisational measures to protect the processing of personal data.[80]

In the UK, the Data Protection Agency, the Information Commissioner's Office (ICO) has issued a notice of intent to British Airways. Following an investigation, on July 2019, the ICO has issued a notice of its intention to fine British Airways £183.39 million for violation of the GDPR.[81] The proposed fine related to a cyber incident which involved user traffic to British Airway's website being diverted to a fraudulent website. As a result of this security breach, the personal data of 500,000 British Airways customers was compromised, it is believed to have started in June 2018.[82] The breach is held to be caused by the poor security arrangements of British Airways.

According to DLA Piper's GDPR Data Breach Survey dated January 2020, data protection authorities in the EU have imposed EUR 114 million in fines under the GDPR regime for a wide range of GDPR infringements, from the period of January 2019 to January 2020.[83] Amongst all member states France, Germany and Austria are the member states which have imposed the highest total amount of fines. France has imposed fines of just over EUR 51 million, Germany EUR 24.5 million and Austria EUR 18 million respectively.[84]

In the light of above, it may be argued that there is a need to strengthen the enforcement of the GDPR across all member states. Current cases suggest that larger member states

such as France, Germany may be more likely to enforce the GDPR than smaller member states, perhaps due to lack of resources. Also, some member states might be more lenient towards violation of the GDPR. This in the long run may lead to deviations between Member states which could be detrimental to informational privacy as it can lead to forum shopping, where data subjects can bring their case before an EU member state that is more likely to render a decision in their favour.

5.2. Ambiguity with regards to data subject rights may undermine the enforcement of the GDPR

As noted above, Chapter 3 of the GDPR contains several key data subject rights such as the right to data portability**.** Following an open public consultation that continued until the end of January 2017, on 5 April 2017, the Article 29 Working Party[85] approved a revised and substantive guidance clarifying some of the ambiguities with regards to the right to data portability.[86] In other words, due to some uncertainties surrounding the right to data portability, Article 29 Working Party issued guidance clarifying the extent and scope of the right to data portability. As of 25 May 2018, the Article 29 Working Party was replaced by the European Data Protection Board (EDPB). EDPB has also issued guidance on issues including but not limited to automated decision-making, profiling, consent and data breach notifications.

Nevertheless, the lack of case law and precedent particularly with regards to some data subject rights (with the exception of the right to erasure and the right to access) begs the question as to whether there is a need for further guidance and clarity with regards to some data subject rights. As mentioned above, the right to erasure under Article 17 of the GDPR seems to be a right which is regularly utilised by data subjects. The Google Spain case analysed above demonstrates that data subjects are utilising this right and regularly taking action to have inaccurate or out-dated information deleted from a search engine or a website. However, since the inception of the GDPR, there seems to be no other cases in relation to the rights of data subjects. Perhaps it is a bit premature to expect cases pertaining to data subject rights, 2 years after GDPR's inception. Nevertheless, it must be noted that if data subjects are better informed of their rights, they might be in a better position to take up their rights, which may lead to efficient enforcement of the GDPR and perhaps more precedent in this area. This currently this does not seem to be the case.

5.3. The GDPR does not fully address the imbalance of power between the data subjects and the data controllers and may need to supplemented by other laws

As discussed above the GDPR gives data subjects several important rights, such as the right to data portability. Nevertheless, the GDPR does not and cannot fully address the imbalance of power between data subjects and data controllers. For instance, when signing up to use the services of a company such as Google or Facebook, the users have the option of not consenting to the terms and conditions offered by that company. Nevertheless, this may result in them not being able to use the services offered by that company, which may be essential for them in order to communicate with others or receive/share information. The GDPR gives the users some power by raising the standards for acquiring consent. However, due to the significant market power of digital giants such as Google and

Facebook, data subjects often have very limited choice when it comes to giving consent. This may push them to consent to data collection practices they would not otherwise have consented to. As pointed out by Lynskey, the validity of consent can be questioned when these power and informational asymmetries exist.[87] For example, in its complaint to the Irish Data Protection Commissioner the group Europe v Facebook contended that Facebook has become a standard form of communication and the validity of consent given to a monopoly such as Facebook is questionable, as it is not an informed, unambiguous and specific consent .[88] This view was also shared by the Article 29 Working Party in its opinion WP187 [89]: 'Considering the importance that some social networks have acquired, some categories of users (such as teenagers) will accept the receipt of behavioural advertising in order to avoid the risk of being partially excluded from social interactions'.

In other words, even if the data subjects know that a company's terms and conditions are not respecting their informational privacy, in practice they do not have much bargaining power particularly when the company that provides the services has a near monopoly position. This suggests that the GDPR itself cannot tackle all the problems associated with the imbalance of power between the data subjects and the data controllers. Arguably, in the case of digital monopolies such as Google and Facebook, the imbalance of power and indirectly informational privacy issues created by unfair terms and conditions can be dealt with by the relevant competition authorities. If a competition authority finds that a dominant undertaking abuses its market power by imposing unfair terms and conditions, which harms competition or other competitors, this undertaking can be subject to proceedings under Article 102 of the Treaty on the Functioning of the European Union. Art 102 TFEU prohibits any exclusionary or exploitative abuse by one or more undertakings in a dominant position. The provision can also be used to tackle large platforms with questionable data collection practices, if there is a clear harm to consumers and to the competitive process. In this regard, it is worth mentioning the recent case against Facebook. On 6 February 2019, the Bundeskartellamt (the German Federal Cartel Office) concluded its three-year investigation into Facebook. The investigation concerned Facebook's data collection practices and the interplay between data protection and competition law. The Bundeskartellamt asserted that Facebook is dominant in the German market for social networks for private users.[90] Furthermore, according to Bundeskartellamt, Facebook made the use of its social networking service conditional upon users granting excessive permission to collect and process their personal data. It also failed to make its users aware that it collected users' personal data from third party websites and other Facebook owned platforms (such as WhatsApp and Instagram) and merged them with data gathered on its own platform, which enabled it to profile users.[91] As elaborated by Colangelo, if a third-party website has embedded Facebook products such as the 'like' button or use analytical services such as Facebook Analytics, the users' data will be transferred to Facebook via application programming interfaces (API's) when they visit that third party's website.[92] As a result, through API's, even if a user visits other website than Facebook his/ her data is collected and processed by Facebook. To summarise, according to Bundeskartellamt Facebook's terms of service, which enabled excessive data collection, was contrary to the General Data Protection Regulation. This allegedly amounted to an exploitative abuse under ARC § 19(1) (the German equivalent of Article 102 TFEU that concerns abuse of a dominant position) in violation of competition law. As a remedy, the Bundeskartellamt ordered Facebook to change its terms of service and

to refrain from collecting data from third party websites and other Facebook owned platforms.

Facebook applied for the suspension of this judgement before the Higher Regional Court of Düsseldorf (OLG). On 26 August 2019, the OLG suspended the Bundeskartellamt's decision, questioning its legal basis.[93] With regard to the alleged exploitative conduct, the OLG held that FCO did not carry out sufficient investigation into ' as if competition' (the counterfactual situation[94]) and as a result did not provide any meaningful findings on the issue of which conditions of use would have been formed under competitive conditions.[95] In other words, since the Bundeskartellamt did not assess the counterfactual and how the situation would have developed in the absence of Facebook's alleged conduct, it had no evidence to show that Facebook's terms and conditions deviated from the behaviour of a company in a competitive market.[96] The OLG stated that the Bundeskartellamt's decision failed to explain why the data collected by Facebook was excessive.[97] The OLG noted that the use of Facebook is conditional on the consent of the users to the processing of their data, however the users remained free to use or not use Facebook depending on their values and preferences.[98] According to OLG, the FCO was merely discussing a data protection issue, which is not a competition problem. OLG contended that, even if Facebook's terms and conditions were contrary to data protection rules, not every legal violation is sufficient to give rise to an abuse of a dominant position.[99] Both German law (Section 19GWB) and EU Competition law (Article 102 TFEU) require a harm to competition, which was arguably not proved in the instant case. Subsequent to this decision, the Bundeskartellamt has lodged an appeal with the Federal Court if Justice. At the time of writing, the case is pending.

This case demonstrates that in the near future more competition authorities in different member states may take action against digital companies with questionable data collection practices, if there is a clear link between dominance and abusive conduct and they can prove that there is harm to competition. Hence, issues that are not addressed by the GDPR, such as imbalance of power between data controllers and data subjects, can be resolved by competition laws and other laws such as the Consumer Protection Law and Contract Law.

5.4. It may be too early to assess the impact of the GDPR on the right to privacy

In a 2020 study, Linden et al investigated the impact of the GDPR on privacy policies. Linden et al concluded that overall, the GDPR has made a positive impact on the incorporation of privacy rights and information and indeed the GDPR had a more pronounced impact in the EU.[100] However, it must be noted that the GDPR is a relatively new instrument and it may be premature to assess its impact. Perhaps assessing its impact in the next 5–10 years perspective will be more useful in terms of getting a fuller picture. Furthermore, further research needs to be undertaken to evaluate the impact of the GDPR outside of the EU due to its extraterritorial impact.

5.5. Technological advancements may make some provisions of the GDPR redundant

The GDPR has many provisions that are drafted taking into consideration the current state of technology. For this reason, certain provisions in it might be obsolete in a few

years due to technological advancements. As an example, as mentioned under Section 2.2, Article 20(2) of the GDPR suggests that data subjects can ask their data to be transmitted directly from one controller to another where technically feasible. For the time being, certain data transfers may not be technically feasible for data controllers, nevertheless in 10 years time, particularly with the adoption of common standards in different industries, it may not be possible for a data controller to say that data transfer is not technically feasible. In other words, wording in certain provisions in the GDPR may need to adopted/amended taking in to consideration technical developments. It would be particularly useful to conduct further research as to the specific parameters of and criteria for technically feasibility within and across industries, to determine when the term 'feasible' needs to be revisited. This may be applicable to other provisions of the GDPR as well.

5.6. Even the strongest data protection laws are not sufficient to resolve all privacy issues

As pointed out by Bruschi, even the strongest data protection laws such as the GDPR will not suffice to protect users and companies from cyber-attacks and security breaches, and ultimately there will always be data breaches undermining individuaĺs privacy.[101] Although the GDPR introduces strong data protection measures, hackers and computer attacks will remain a constant threat to useŕs informational privacy as evidenced in the recent Facebook Cambridge Analytica scandal. The scandal came to surface in 2018, when it became evident that Cambridge Analytica gained access to the personal data of 87 million Facebook users without their consent and used this data for political advertising and for manipulating voters both in the US elections and for the Brexit referendum in the UK.[102] Hence, data protection laws are indeed welcome instruments in protecting privacy in the online sphere, but they cannot be sufficient on their own without vigilant and well-informed consumers as well as companies/organisations who are constantly reviewing and improving the security of user data.[103]

5.7. Privacy by design is still far from unfolding its full potential

As noted above, Article 25 GDPR and Recital 78 of the GDPR incorporates the privacy by design principle which is a significant step for enhancing informational privacy. However, as noted by the European Data Protection Supervisor (EDPS), Gioavanni Butarelli, in 2018, privacy by design is far from unfolding its full potential.[104] In its report the EDPS made some useful recommendations to the European Institutions. According to the EDPS, in order to make privacy by design achieve its desired impact, the EU needs to;

i ensure strong privacy protection, including privacy by design, in the on-going legislative process for the ePrivacy Regulation,
ii support privacy when adapting or creating legal frameworks which influence the
iii design of technology, by increasing incentives and substantiating obligations including liability rules,
iv foster the roll-out and adoption of privacy by design approaches and Privacy enhancing technologies in the EU and at the Member State level through appropriate implementing measures and policy initiatives;

v ensure continuous availability of competence and resources for research and analysis on privacy engineering and privacy enhancing technologies at EU level,
vi support the development of new practices and business models through the research and technology development instruments of the EU, with a special focus on emerging technologies such as artificial intelligence, machine learning and blockchain;
vii support policy initiatives for EU institutions and national public administrations to lead by example and to integrate appropriate privacy by design requirements in public procurement,
viii support an inventory and observatory of the 'state of the art' of privacy engineering and Privacy Enhancing Technologies (PETs) and their advancement to raise awareness on the subject.[105]

In general, all the above-mentioned measures will contribute to the adoption of privacy friendly technologies and ensure that privacy is considered at the design phase, rather than at the end.

In the light of above, it can be said that there are quite a few efforts that the EU needs to undertake to ensure that privacy by design becomes a reality rather than a theoretical obligation drafted under the GDPR. First, the ePrivacy Regulation should come into force as soon as possible. Second, all EU institutions should instigate dialogue with key stakeholders such as IT companies to ensure that privacy is taken into consideration at the time of planning a processing system. Finally, the EU should incentivise privacy by design by developing policy initiatives and by rewarding efforts of industry players who are working towards solutions that respect and enforce informational privacy. This could take the form of financial incentives such as grants or tax reliefs, or leveraging the power of the public sector through solution requirements in public tenders.

6. Conclusion

Data protection regulation such as GDPR is one piece of a larger puzzle. GDPR has been a significant step in the right direction to protect the right to privacy particularly in the online sphere. Nevertheless, it must be noted that the GDPR is not a complete revolution as it builds on existing EU law on data protection and the right to data privacy such as Directive 95/46/EC. A very important aspect of the GDPR is to empower data subjects against exploitation and potential misuse of their data and in this respect, it is a crucial instrument for informational privacy. Having said that GDPR merely as a legal instrument is not sufficient to strengthen data protection and enforce informational privacy in the online sphere. As discussed above even the strongest privacy laws cannot such as the GDPR cannot stop data breaches which are caused by poor online security and evolving online attacks.

In the light of above, it must be noted that GDPR is a right step in direction in terms of protecting informational privacy but there is still a long way to go in terms of achieving informational privacy.

The following observations can be made to ensure that the GDPR has teeth and achieves its full potential.

First, the enforcement of the GDPR needs to be vigorous, companies and all relevant stakeholders including public and private actors that exploit and misuse personal data need to be subjected to strong penalties.

Second, the EDPB should monitor divergent practices in Member States. If the EDPB finds that some member states issue less fines and there has been relatively less enforcement activity in a particular member state, the underlying reasons behind these needs to be thoroughly investigated to ensure consistent implementation of the GDPR in all Member states.

Third, as noted above in order to take full advantage of data subject rights under Chapter 3 of the GDPR, data subjects and data processors who are faced with data subject requests need to better informed. As noted above, the Article 29 Working Party and the now the EDPB has issued various guidance with the aim of clarifying certain ambiguities in the GDPR. The efforts of the EDPB is invaluable, however Member states should also take active steps to ensure that the public and data processors are aware of the content and limitation of these rights. As noted above, the lack of case law post GDPR particularly pertaining to data subject rights is concerning as it may indicate that there is still a level of ambiguity surrounding these rights.

Fourth, as discussed above GDPR does not fully address the power imbalance between data controllers and data subjects. This power imbalance can be rectified by other laws such as competition law, when there is a clear harm to competition and consumers. In this respect data protection authorities in member states should develop good working relations with other regulatory bodies and collaborate on issues pertaining to informational privacy.

Fifth, as mentioned under Section 3.7, the GDPR Article 25 incorporates privacy by design, which is very significant step for enhancing informational privacy. Nevertheless, as pointed out by the EDPS, privacy by design is still far from unfolding its full potential.[106] In this respect, the EDPB should continue to promote privacy by design alongside with other European data protection authorities and provide guidance to controllers on the appropriate implementation of the principle. As noted earlier, there is a pressing need to ensure that the ePrivacy Regulation comes into force as soon as possible, as it will be very useful in complementing the GDPR particularly in relation to the protection of online personal communications. Furthermore, European policymakers should implement, encourage and develop frameworks and facilitate dialogue with key stakeholders such as engineering companies, to make privacy by design a reality rather than a theoretical legal provision.

Ultimately, it must be noted that the GDPR is not an end in itself to protect and promote informational privacy; it is just the start of a journey with perhaps no end destination. As noted under Section 3.5, the use of certain terminology and provisions in the GDPR must be revisited due to the pace of technological advancement to ensure provisions do not become obsolete. Protecting informational privacy is neither a simple task that can be left to the EU alone, nor to a single piece of legislation such as the GDPR. Hence, not only the EU, but all developed/developing countries and international organisations including the European Council and the United Nations should work towards policy aimed at establishing common ground rules for protecting privacy in the online sphere.

Notes

1. This article will concentrate on informational privacy. In this article, the term 'informational privacy' is used to describe the relationship between the collection and dissemination of data, technology, the public expectation of privacy, legal and political issues surrounding them.
2. Özgür H. Çinar, 'The Right to Privacy in International Human Rights Law', *Journal of Information Systems & Operations Management* 13, no. 1 (2019): 33.
3. International Covenant on Civil and Political Rights adopted 16 December 1966 entered into force 23 March 1976 999 UNTS 171, Art 17.
4. Robert C. Post, 'Three Concepts of Privacy', *The Georgetown Law Journal* 89, no. 6 (2001): 2087–98.
5. See for instance, Post, 'Three Concepts of Privacy', 2087–98; Samuel Warren and Louis Brandeis, ' Right to Privacy', *Harvard Law Review* 4, no. 5 (1890): 193–220.
6. Samuel Warren and Louis Brandeis, ' Right to Privacy', *Harvard Law Review* 4, no. 5 (1890): 193–220.
7. Anna Jonsson Cornel, 'Right to Privacy' *Oxford Constitutional Law* (2015), https://oxcon.ouplaw.com/view/10.1093/law:mpeccol/law-mpeccol-e156?print=pdf (accessed June 15, 2020).
8. J. Solove, 'Understanding Privacy', *Harvard University Press GWU Legal Studies Research Paper* GWU Law School Public Law Research Paper, no. 420 (2008), https://ssrn.com/abstract=1127888 (accessed June 15, 2020).
9. See for instance; Case T-194/04 the Bavarian Lager Co Ltd v Commission [2007] ECR II-04523, where the General Court expressly makes reference to ECHR Article 8.
10. Opinion 2/313 pursuant to Article 218(11) TFEU 18 December 2014 ECLI: EU: C: 2014:2454.
11. Ibid.
12. Ibid.
13. European Parliament Briefing ' EU Accession to the European Convention on Human Rights (2017) https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/607298/EPRS_BRI(2017)607298_EN.pdf (accessed June 15, 2020).
14. Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012 :391–407.
15. Hielke Hijmans, and Alfonso Scirocco, 'Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help?' *Common Market Law Review* 46 (2009): 1485–525.
16. Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford: Oxford University Press, 2015), 106.
17. *Gaskin v United Kingdom* (1989) 12 EHRR 36.
18. *Perry v United Kingdom* (2004) 39 EHHR 3.
19. *Copland v United Kingdom* (2007) 45 EHRR 37.
20. *Leander v Sweden* (1987) 9 EHRR 433.
21. *S. and Marper v. the United Kingdom* (2009) 48 EHRR 50 para 121.
22. *Perry v United Kingdom* (2004) 39 EHRR 3, para 42.
23. *Bohlen v Germany* [2015] ECHR 194.
24. For example, see *Von Hannover v Germany (59320/00) [2004]* E.M.L.R. 21*; (2005) 40* E.H.R.R. 1 *and Editions Plon v France (58148/00) (2006)* 42 E.H.R.R. 36.
25. European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence (2019) para 115, https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf (accessed June 15, 2020).
26. Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR', *International Data Privacy Law* 3, no. 4 (2013): 222.
27. See for instance; Case C-62/90 *Commission v Germany* [1992] ECR I-2575, para 23.
28. Case C-139/01 *Oesterreicher Rundfunk and Others* [2003] ECR I- 4989.
29. Case T-194/04 the Bavarian Lager Co Ltd v Commission [2007] ECR II-04523.

30. Ibid., para 15–17.
31. Ibid., para 23–36.
32. Ibid., para 123.
33. Ibid., para 124.
34. Ibid., para 125.
35. Ibid., para 63.
36. Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR* (C-92/09) and *Hartmut Eifert (C-93/09) v Land Hesse*n [2010] ECR I-11063.
37. Joined Cases C-293/12 and C- 594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014].
38. Ibid., para 69.
39. Ibid, para 64 and 65.
40. Joined Cases C-293/12 and C- 594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] para 47.
41. Ibid., para 52.
42. International Covenant on Civil and Political Rights adopted 16 December 1966 entered into force 23 March 1976 999 UNTS 171 (ICCPR).
43. See, e.g., *Amann v Switzerland*, no 27798/95, ECHR 2000-II, para 65 and *Rotaru v Romania* [GC] App no 28341/95, ECHR 200-V, para 43.
44. *S. and Marper v. the United Kingdom* (2009) 48 EHRR 50.
45. For example Westin describes privacy as ' the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is shared with others' Alan Westin, *Privacy and Freedom* (Athenaeum, 1967), 158; Daniel Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York : New York University Press, 2004); Yves Poullet, ' Data Protection Legislation: What is at Stake for our Society and Democracy) *Computer Law and Security Review* 25, no. 3 (2009): 211–26.
46. For instance in the American context Solove argues that ' the right to information privacy has emerged in the courts as a spin-off of the regular constitutional right to privacy'. Daniel Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York : New York University Press, 2004), 75.
47. Solove, *The Digital Person*, 8.
48. See e.g.; Juliane Kokott and Christoph Sobotta ' The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR', *International Data Privacy Law* 3, no. 4 (2013): 223; Maria Tzanou, 'Data Protection as Fundamental Right Next to Privacy? " Reconstructing" a Not So New Right', *International Data Privacy Law* 3 (2013): 88; Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford: Oxford University Press, 2015), 104.
49. Kokott and Sobotta, 223.
50. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1.
51. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to processing of personal data and on the free movement of such data [1995] OJ L 281/31.
52. For example see; Amy Kristin Sanders, 'The GDPR One Year Later: Protecting Privacy or Preventing Access to Information', *Tulane Law Review* 93, no. 5 (May 2019): 1229–54; Simon Davies, 'The Data Protection Regulation: A Triumph of Pragmatism over Principle', *European Data Protection Law Review* 2, no. 3 (2016): 290–6.
53. See for instance, Tal Z. Zarsky, 'Incompatible: The GDPR in the Age of Big Data', *Seton Hall Law Review* 47, no. 4 (2017): 995–1020; Eduardo Ustaran, 'EU General Data Protection Regulation: Things You Should Know', *Privacy and Data Protection Journal* 16, no. 3 (2016): 3; and see also Francoise Gilbert, 'European Data Protection 2.0: New Compliance

Requirements in Sight – What the Proposed EU Data Protection Regulation Means for U.S. Companies', 28 *Santa Clara Computer & High Tech. Law Journa*l 815 (2012): 848–49.

54. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to processing of personal data and on the free movement of such data [1995] OJ L 281/31.
55. It is worth noting that different member states have different legal traditions, which has an influence on their data protection law. For instance, German data protection law is anchored to the notion of human dignity; French data protection prioritises the concept of individual liberty; whilst Belgian data protection law places emphasis on privacy. On this see Evelien Brouwer, *Digital Border and Real Rights: Effective Remedies for Their Country Nationals in the Schengen Information System* (The Hague: Martinius Nijhoff Publishers, 2008), 198.
56. Ronald Hes and John Borking 'Privacy-Enhancing Technologies: The Path to Anonymity Volume 1 (1995), https://collections.ola.org/mon/10000/184530.pdf (accessed June 15, 2020).
57. Anna Romanou, 'The Necessity of the Implementation of Privacy by Design in Sectors Where Data Protection Concerns Arise', Computer Law & Security Review 34 (2018): 99–110.
58. Ibid.
59. Jeffrey Rosen, 'The Right to Be Forgotten' Stanford Law Review 64 (2012) https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/ (accessed June 15, 2020).
60. *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C- 131/12,* ECLI: EU: C:2014:317, ILEC 060 (CJEU 2014) 13,05.2014.
61. Ibid.
62. Case C-507/17 Judgment of the Court (Grand Chamber) of 24 September 2019. Google LLC, successor in law to Google Inc. v Commission Nationale De L'informatique Et Des Libertés (CNIL) ECLI: EU: C: 2019: 772
63. Ibid, para 30.
64. Ibid, para 31.
65. Ibid, para 32.
66. Ibid, para 33.
67. Ibid, para 6 and 65.
68. Gabriela Zanfir, 'The Right to Data Portability in the Context of Data Protection Reform', *International Data Privacy Law* 2, no. 3 (2012): 149.
69. For a comprehensive discussion of the right to data portability see Aysem Diker Vanberg and Mehmet Bilal Ünver, 'The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo? *European Journal of Law and Technology* 8, no. 1 (2017), http://ejlt.org/article/view/546/727 (accessed June 15, 2020).
70. It is worth noting that there have been several cases prior to the GDPR that concerns the right to access such as the Bavarian Lager C-28-08P and Egan& Hackett v Parliament T-190/10. Bavarian Lager case has been discussed in this article.
71. Regulation of The European Parliament and of the Council concerning the Respect for Private Life and for the Protection of Personal Data in Electronic Communications within the European Union.
72. Directive 2002/58/EC e European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47.
73. European Commission, Proposal for an Eprivacy Regulation, https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation (accessed June 15,2020).
74. W Gregory Voss, 'First the GDPR Now the Proposed ePrivacy Regulation', *Journal of Internet Law* 21, no. 1 (2017): 3–11.

75. The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (accessed June 15, 2020).
76. Ibid.
77. Ibid.
78. European Data Protection Board 'BfDI imposes fines on telecommunications service providers' (20, https://edpb.europa.eu/news/national-news/2019/bfdi-imposes-fines-telecommunications-service-providers_en (accessed June 15, 2020).
79. Ibid.
80. Ibid.
81. Information Commissioner's Office, 'Intention to fine British Airways £183.39m under GDPR for data breach' (2019) https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/ (accessed May 2, 2020).
82. Ibid.
83. DLA Piper Data Breach Survey, January 2020, https://sweden.dlapiper.com/sites/default/files/node/field_download/DLA%20Piper_Data%20Breach%20Report%202020.pdf (accessed June 15, 2020).
84. Ibid.
85. It should be noted that as of 25 May 2018, the Article 29 Working Party ceased to exist and it has been replaced by the European Data Protection Board (EDPB).
86. Guidelines on the right to data portability, Article 29 Working Party, [2017] 16/EN WP 242 rev. 01 adopted on April 5, 2017.
87. Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford: Oxford University Press, 2015), 189.
88. Europe v Facebook, ' Response to the Audit' by the Irish Office of Data Protection Commissioner on "Facebook Ireland Ltd"', Vienna, 4 December 2012, 42: < http://www.europe-v-facebook.org/report.pdf> (accessed June 15, 2020).
89. Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent 01197/11/EN WP187 adopted on 13 July 2011 available < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> (accessed June 15, 2020).
90. Case summary, "Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing" 2019, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=3> p. 5, 2019 (accessed June 15, 2020).
91. Ibid.
92. Guiseppe Colangelo, ' Facebook and the Bundeskartellamt's; Winter of Discontent' (2019) https://www.competitionpolicyinternational.com/facebook-and-bundeskartellamts-winter-of-discontent/ (accessed June 10, 2020).
93. OLG Düsseldorf, August 26, 2019, Case VI-Kart 1/19 (V).
94. Counterfactuals in competition law analysis can be used to assess the effects of an event and how the situation would have developed in the absence of that event.
95. OLG Düsseldorf, para 27 and 47.
96. Colangelo, supra note 92.
97. OLG Düsseldorf, para 32.
98. Ibid, para 71, 76 and 77.
99. Ibid, para 44, 46 and 71.
100. Thomas Linden et al., 'The Privacy Policy Landscape after the GDPR, Proceedings on Privacy Enhancing Technologies', *Proceedings on Privacy Enhancing Technologies* 1 (2020): 47–64.
101. Danilo Bruschi, 'Information Privacy: Not just GDPR', in *Computer Ethics - Philosophical Enquiry (CEPE) Proceedings*, ed. D. Wittkower (2019), 9 https://digitalcommons.odu.edu/cepe_proceedings/vol2019/iss1/9 (accessed June 15, 2020).
102. Jim Isaak and Mina J. Hanna, 'User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection', *Computer* 51, no. 8 (2018): 56–9.

103. John Thornhill, 'GDPR is a Start but not Enough to Protect Privacy on its Own', *Financial Times* https://www.ft.com/content/624f813e-5f5e-11e8-9334-2218e7146b04 (accessed June 15, 2020).
104. Opinion 5/2018 Preliminary Opinion on Privacy by Design by European Data Protection Supervisor, para 22, p. 5 https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (accessed June 15, 2020).
105. Ibid., p. 21.
106. Ibid., p. 5.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Aysem Diker Vanberg is a Senior Lecturer at the School of Law & Criminology at the University of Greenwich specialising in EU Competition Law and IT Law. Prior to joining the University of Greenwich, she worked at Anglia Ruskin University as a Senior Lecturer and at the University of Essex as an Associate Lecturer and as a research associate. Before moving to the UK, she qualified as a lawyer in Turkey and worked as a lead In-House Counsel for multinational companies including MAN Nutzfahzeuge AG and Cimpor Cimentos de Portugal.

ORCID

Aysem Diker Vanberg http://orcid.org/0000-0002-0614-1707