universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

„European Privacy Legislation:

A Legal and Economic Analysis"

verfasst von / submitted by

Mag. Iur. Wolfram Vitus Grosser

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Advanced International Studies (M.A.I.S.)

Wien 2020 / Vienna 2020

Studienkennzahl lt. Studienblatt: Postgraduate programme code as it appears on the student record sheet:	A 992 940
Universitätslehrgang lt. Studienblatt Postgraduate programme as it appears on the student record sheet:	Internationale Studien / International Studies
Betreut von / Supervisor:	Prof. Dr. Werner Neudeck

diplomatische akademie wien
Vienna School of International Studies
École des Hautes Études Internationales de Vienne

Pledge of Honesty

On my honour as a student of the Diplomatische Akademie Wien, I submit this work in good faith and pledge that I have neither given nor received unauthorized assistance on it.

(signature of student)

Abstract

As of July 2020, the General Data Protection Regulation 2016/679 (GDPR) has been in force for more than two years. Together with the e-Privacy Directive 2002/58/EC, it applies to millions of European businesses across all sectors. Both pieces of legislation have been challenging to implement for industry stakeholders; A review of their reports serves as the basis of a qualitative legal analysis of the GDPR, the E-Privacy Directive and the draft of the coming E-Privacy Regulation that seeks to identify which provisions have turned out to be most difficult for European Businesses to implement. This legal dissection will be accompanied by a quantitative assessment of the administrative fines that have been issued by data protection authorities throughout the Union. The aim is to locate problems within the legislature and to provide recommendations for how to solve them.

Die Datenschutz -Grundverordnung 2016/679 (DSGVO) ist im Juli 2020 seit mehr als zwei Jahren in Kraft. Gemeinsam mit der E-Privacy Richtlinie 2002/58/EG ist sie auf Millionen von Europäischen Unternehmen direkt anwendbar. Die Umsetzung beider Rechtsakte hat eine Herausforderung für die betroffenen Industrien dargestellt. Die Auseinandersetzung mit den Erfahrungsberichten von Interessenvertretern dient als Grundlage für eine qualitative rechtliche Analyse der DSGVO, der e-Privacy-RL und des Entwurfs der kommenden E-Privacy-VO mit dem Ziel, jene Bestimmungen zu identifizieren, die am schwierigsten in europäischen Unternehmen umzusetzen waren. Dieser rechtliche Querschnitt wird begleitet von einer quantitativen Aufbereitung der Geldbußen, die von europäischen Aufsichtsbehörden verhängt wurden.

Table of Contents

1. Introduction

The General Data Protection Regulation is the most significant piece of privacy regulation in Europe and – arguably - in the world. As of mid-2020, it has been in force for a full two years. While the GDPR provides the general framework for how Personal Data is to be processed within the Union, it is corroborated and particularised by the older e-Privacy Directive from 2002, regulating the processing of data in the context of electronic Communications. This directive is soon to be replaced with the coming e-Privacy Regulation that is currently still being formed in the ordinary legislation procedure of the European Council. These three pieces of legislation will serve as the basis for the interdisciplinary analysis performed in this Thesis. The aim is to assess which parts of the above-mentioned legal acts have proven to be most difficult or problematic to implement for European Businesses. These notions can be condensed in the following **research question:**

Which provisions of the European Data Protection Framework as defined by the GDPR, the e-Privacy Directive and the coming e-Privacy Regulation have in practice turned out to be most problematic for individual businesses?

In the first part (Chapters 2.1. to 2.3.), a qualitative legal analysis of the GDPR, the e-Privacy directive and the current draft of the e-Privacy Regulation will identify which provisions were most contentious from the point of view of the industry stakeholders. Their reports will also serve as a basis for which of the provisions will be examined more closely These provisions will be scrutinized from a legal perspective in order to understand why some of them worked well and others did not; In an effort to keep all findings palpable for readers unfamiliar with data protection law, some basic principles and definitions adorned with recent findings in the relevant judicature will also be provided in the first part. In the second part, a qualitative dimension of the research question will be explored by analysing datasets of the administrative fines issued by Data Protection Authorities throughout Europe. These statistics not only shed a light on some of the economic burden associated with the GDPR and other data protection legislation, but they also serve to confirm which provisions have been violated by European Businesses failing to meet the mandated protection requirements.

2. European Data Protection Law: Analysis and Reception

Assessing the legal status quo in the following chapter will reveal potential challenges to the European economy posed by the EU's data protection legislation. The legal sources in question are the General Data Protection Regulation (henceforth GDPR)[1], the e-Privacy Directive 2002/58/EC (henceforth ePD)[2] and the coming e-Privacy Regulation (henceforth ePR) in its current drafted version[3]. This compendium of legal acts is in no way an exhaustive list of all data protection legislation on the European level, but rather a representative cross section to fit the frame of this Thesis. The aim is not to explain the legal framework in scholastic detail, but rather to identify the parts of it that have proven most contentious for European businesses. Brief definitions of the basic principles and terms will make these provisions understandable to readers with no legal background. Reports from industry stakeholders as well as from the EU itself will serve to identify what can be considered the provisions with the highest economic impact. Each of these problems will be analysed as to what part of the legislation has caused them and how they could be ameliorated.

2.1. General Data Protection Regulation (GDPR)

2.1.1. Inception and Reception

The GDPR is the main source of data protection legislation in Europe. Due to its nature of a European Regulation, it is directly applicable in all member states and shapes the citizen's rights and obligations with direct effect. That means that most of its provisions are not dependant on any implementation in member state law; instead, they are directly applicable to European Citizens and businesses. It is a piece of legislation of considerable extent that covers everything from the general processing of personal data down to the details of accrediting certification bodies and codes of conduct. After a lengthy legislation process, it came into effect on May 25, 2018, directly applicable to millions of businesses in all of Europe. Before the GDPR entered into force, it was mostly dreaded by economic actors not only in Europe, but throughout the

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119/1

[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201

[3] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC

world; Several predictive papers and articles anticipated that it would have negative effects on European GDP, terms of trade, and investment rates (See Chapter 2.4.1.). The EU itself deemed the GDPR's adoption necessary for several reasons, as stated in its official impact assessment for the then-called "proposed Data protection Regulation" from 2012[4].

For one, the Commission mentioned the legal fragmentation caused by the GDPR's predecessor, the Data Protection Directive from 1995[5], as one of its most costly issues, as it caused an estimated several billions of Euros in administrative red tape due to crucial provisions such as the rules on consent and sensitive data varying across member states.[6] This administrative burden on the internal market is an argument that is commonly used by the EU to replace directives with regulations and thereby increasing its supranational influence. The same rationale lies behind the transition from the e-Privacy Directive to a regulation and will be discussed in more detail in section 1.3. In the light of this development, it might seem surprising that parts of the criticism that the GDPR was met with was based on harmonisation issues: The GPR is considered a legal hybrid of a Regulation with elements of a Directive – more vividly called a "limping Regulation"[7] - designed to be implemented into the member states legal system by means of national laws that particularize the general instructions.. By giving the member states too much leeway in certain areas, the EU has compromised some of the economic benefits that were expected of the harmonisation of data protection law.[8,9]. While this significant relaxation of the supranational nature of the GDPR could be considered a respectful product of the principles of subsidiarity and proportionality enshrined in the TEU[10], it certainly had unpleasant side effects for businesses hoping for completely harmonised pan-European data processing rules. A

---

[4] European Commission, *Commission Staff Working Paper: Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, XXX SEC 72/2 Brussels, 2012 (Hereafter "*GDPR Impact assessment*")

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281

[6] *GDPR Impact Assessment*, p13

[7] Ines Härtel, *Handbuch Europäische Rechtsetzung*, Springer, Germany, 2016, p 175

[8] Digital Europe, *Two years of GDPR: A report from the digital industry*, Brussels, 2020, p 12 (Hereafter „*Digital Europe"*)

[9] Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679, *Report – Contribution from the Multistakeholder Expert Group to the Stock-taking exercise of June 2019 on one year of GDPR application*, 2019, p. 22 (Hereafter "*Stakeholder Report*")

[10] Jürgen Kühling, Mario Martini et al, *Die DSGVO und das nationale Recht*, MV-Verlag, Germany, 2016, p 4

more detailed account of the opening and implementation clauses in question follows in chapter 2.1.4.

Furthermore, the Commission based its arguments for a regulation on statistics demonstrating an apparent lack of awareness and an underestimation of privacy risks on the part of businesses and a loss of control and trust on the part of the consumers.[11] This is based on Eurobarometer surveys from 2011 that asked a wide range of questions on user behaviour online as well as on attitudes to data protection.[12] These arguments have not aged particularly well, as the same Eurobarometer surveys the Commission relied on to justify new legislation have not changed for the better in the first year after the GDPR's entry into force. A GDPR-specific survey from 2019 shows that the answers to the very same question used in the initial impact assessment have gotten more negative over the course of 8 years, with more people feeling not in control of their personal data than before. It is hard to determine why this ongoing disengagement of users with their legal control of personal data online seems to grow proportionally to the legislative efforts to combat it; Besides solely blaming the growing industry and the ruthlessness of internet service providers, it seems fair to say that overcompensation in parts of the legislation has contributed to a certain numbness of the userbase when it comes to handling their personal data. The well known issues of information and consent fatigue (See chapters 2.1.3. and 2.2, respectively) are in part caused by insufficiencies in the legal texts.

The GDPR's drawn-out adoption process over 9 Council presidencies, similar to what we see happening currently to the draft of the e-Privacy Regulation, took some of the initial fortitude of the Commission's plans. But overall, the GDPR entered into force with no unexpected troubles, at least initially. Two years later, both sides have taken stock and have drawn different conclusions. The reports from both the Commission itself and the industry stakeholders will give an indication which GDPR provisions haven proven to be most contentious, and why. In its official document[13], the EU is not exactly accommodating to any criticism of the GDPR. The industry reports, on the other hand, seem a bit more balanced, in that they convey a picture of businesses accepting the importance of the new rules, but struggling to keep up with the

[11] *GDPR Impact Assessment*, p 25

[12] European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, Brussels, 2011, (Hereafter „*Eurobarometer 2011"*) p 125

[13] European Commission, *Communication from the Commission to the European Parliament and the Council: Data protection rules as a trust-enabler in the EU and beyond – Taking Stock*, Brussels, 2019 (Hereafter „*Taking Stock*")

sometimes exceedingly high demands and lack of scaling within the legislation. The following topics have proven themselves problematic in practice:

- Regarding the general Framework of the GDPR, there has been widespread confusion with the legal bases for processing and the general lack of scaling – i.e., the obligations not taking into account differences in economic size of the processors – has been addressed.
- Both the Commission and the industry stakeholders address the exercise of data subjects' rights, the modalities and the GDPR's information obligations.
- The work of the Data Protection Authorities (DPAs) throughout Europe, especially in connection with the fines they issue, has been evaluated
- The already mentioned harmonisation issues stemming from the GDPR's opening and specification clauses are another recurring theme.

2.1.2. The General Framework and the principles of data processing

What follows is a brief description of what it means for a specific economic actor if the GDPR is applicable to them. The intent is to convey an overview of the GDPR's main obligations in order to be able to understand their potential ramifications and the controversies that come with them. All article mentions refer to the GDPR, unless specified otherwise. A set of legal definitions necessary to understand any provision of the GDPR will provide the basis for further explorations. Any other definitions will be given in tandem with the subject matter. They will be followed by a brief delimination of the GDPR'S scope of application and an overview of the most prominent obligations for Controllers.

Personal data (Art 4 no.1)

refers to any kind of information relating to an at least identifiable natural person, which is rather analytically called the "data subject". This includes a wide range of data than say, the American concept of *Personally Identifiable Information*[14], which requires the piece of data in question to be related to an identified person on its own, with no relation to other pieces of data. For the

[14] Erika McCallister, Tim Grance, Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, National Institute of Standards and Technology, USA, 2010, p 13

European definition of personal data, the mere possibility to relate a piece of data to a person on its own or in **combination with other data**[15] are enough to trigger the legal effects, In this context, it must be stressed that pseudonymised data is also still personal if it can be put into relation with a specific data subject (Recital 26 GDPR)[16]. What counts is the Controller's and anyone else's ability to potentially link the data to a natural person, considering any means reasonably likely to be used for this purpose. This opens up a rather vast definitional crevice for all kinds of data to pass through, which is mirrored in ample **national judicature** on the subject (as the concept of personal data has been around since Directive 95/46/EC, the question of what the definition entails has seldom reached the echelons of the ECJ since the entry into force of the GDPR). Besides obvious personal information such as age and gender or a handwritten signature[17], data protection authorities (see explanation below) across Europe have found the definition to encompass less obvious items such as – rather timely in early 2020 - body temperature[18] (given the right context), the reviews and ratings of a doctor's services on an internet platform[19] and even credit information of a company that could be directly linked to the finances of the owner[20]. Data of legal persons is not included, unlike with the ePD and the ePR. The natural person whose data are being processed in any given situation is called the "*Data Subject*"; Note that the terms "(end)-user" and "consumer" are synonymously used to describe the Data Subject in the sense of the GDPR, depending on the context.

---

[15] Elle Pyle, Laia Bertran Manyé et al, *Decoding GDPR*, Judicature Vol 102 No 1, Bolch Judicial Institute, 2018, p 61

[16] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, Brussels, 2007, p 18

[17] Slovenian Information Commissioner, Decision 07121-1/2020/1043, https://www.ip-rs.si/vop/?tx_jzgdprdecisions_pi1%5BshowUid%5D=1718 (Accessed 12. June 2020)

[18] French Conseil d'État, Decision N° 441065 https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-26-juin-2020-cameras-thermiques-a-lisses (Accessed June 12, 2020)

[19] Austrian Datenschutzbehörde, Decision DSB-D123.527/0004-DSB/2018 https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=45ed119b-7615-4a59-ab4c-a3aae2208c60&Position=1&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=28.02.2019&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=ZweiWochen&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20190115_DSB_D123_527_0004_DSB_2018_00 (Accessed June 12, 2020)

[20] Norwegian Datatilsynet, Decision 20/02220-1 (19/01582)/OMM

https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/varsel-om-overtredelsesgebyr-til-odin-flissenter-as/ (Accessed June 12, 2020)

Processing (Art 4 no.2)

The GDPR considers any handling of personal data – be it storage, use, transfer or erasure - the *processing* of data. It does not matter whether the processing is automated – i.e., done on any computer – or manual.

Controller: (Art 4 no.7)

A *controller* means the natural or legal person, public authority, agency or other body which determines the purposes and means of the processing of any personal data (other than their own). In the economic sense, the controller is the opponent of the individual consumer: They are drawing commercial or infrastructural benefits out of someone else's data, be it directories of clients and employees or the direct sale of personal data to generate ad revenue. The Controller is the main addressee of the GDPR, as all of its obligations apply to almost all processors.

Processor (Art 4 no. 8)

is a natural or legal person or any type of entity which processes personal data on behalf of the controller. That means that they do not decide over the purposes or means of the processing activity. They act as a service provider to the controller, who tells them what to do with the personal data. The role of the processor is economically attractive in a different way than that of the controller, as the processor cannot decide what to do with the data, but at the same time has to fulfil fewer obligations than the controller (although the processor's role has been rendered more challenging compared to the former regime, with more obligations to fulfil[21]).

Supervisory Authority or data protection authority (henceforth DPA, Art 4 no.21)

means an independent public authority which is established by the Member States on the basis of articles 51 to 59. Article 51 entails an implementing provision, mandating the member states to set up a DPA in a structure of their liking (Para 3 explicitly allows for DPAs with substructures). This has led to rather colourful arrangement of DPAs around Europe, from the German BfDI (*Bundesbeauftragter für Datenschutz*) with 16 substructures for each *Bundesland*[22], to agencies

[21] Lukas Feiler, Nikolaus Forgó, *EU-Datenschutz-Grundverordnung*, Verlag Österreich, Austria, 2017, (Hereafter „*Feiler/Forgó*"), p 5

[22] https://www.bfdi.bund.de/DE/Home/home_node.html, accessed June 12, 2020

led by a deciding committee such as the French CNIL[23], to smaller monocratic agencies like the Austrian DSB (*Datenschutzbehörde*)[24]. The DPAs fulfil their **tasks** found in article 57– mainly the monitoring and enforcement of the GDPR and its implementation – by virtue of the **powers** they are given by article 58, which include not only the notorious fines, but also data protection audits, the issue of warnings and recommendations or to order bans of processing in specific cases.

The GDPR's **scope of application** is rather vast, as article 2 para 1 declares it applicable to "*the processing of personal data wholly or partly by automated means*", or non-automated means if the data form part of a filing system. In other words, one would have to store their personal data stock and files in a disjointed pile of paper, as their organization via alphabetical order or date would already constitute a filing system.[25,26]. This broad material scope in combination with the equally broad definitions of personal data and processing make the GDPR affect virtually any business within the EU. The GDPR's reach even extends beyond the borders of the Union to any controller not established in the EU if their processing activities relate to the offering of goods or services to data subjects in the Union; or the monitoring of their behaviour within the EU (article 3 para 2).

With these basics out of the way, it can be clarified what it means that the GDPR is applicable to a specific controller or processor The second chapter lays the foundations for the **principles of legal data processing**, which constitute the heart of the GDPR and European Data Protection Law in General. All other chapters serve to either define them or to ensure their enforcement, as both the exercise of the data subjects' rights as well as the provisions on fines, certificates, DPAs etc. are tied to infringements or the safeguard of the processing principles. There are no less than nine principles enshrined in article 5; In an effort to keep things concise and relevant to the economic aspects, only two principles will be elaborated in detail: The principles of lawfulness and purpose limitation.

---

[23] https://www.cnil.fr/, accessed June 12, 2020

[24] https://www.dsb.gv.at/, accessed June 12, 2020

[25] Elisabeth Hödl in Rainer Knyrim (edtr), *Der DatKomm. Praxiskommentar zum Datenschutzrecht, DSGVO und DSG.*, Manz, Austria, 2018 (Hereafter "*Datkomm*"), p 96 paras 72, 73

[26] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en, accessed June 12, 2020

The principle of lawfulness in article 6 is a core provision of the GDPR. In principle, all processing of personal data that does not belong to the controller is prohibited, unless it is based on one of the 6 legal bases enumerated in Art 6 para 1. They include:

- the data subject has given consent

- The processing is necessary for the performance of a contract to which the data subject is party

- The processing is necessary for compliance with a legal obligation to which the controller is subject;

- The processing is necessary in order to protect the vital interests of the data subject or of another natural person;

- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

-The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except if they are outweighed by the interests or fundamental rights and freedoms of the data subject.

As these provisions are almost identical to their predecessors in article 7 of Directive 95/46/EC, one would assume that they should not cause problems within the new framework; And yet, rich controversy surrounded the one legal basis that did see a slight bit of change compared to the old regime, namely the basis of **the data subject's consent.** The GDPR's rules on consent in terms of data processing and what makes it valid are spread out in various articles, but are rather clearly formulated. Combining Articles 4/11, 7 and 6/1/a, one finds that consent means any clear affirmative action performed by the informed data subject to signify their freely given agreement to a specific processing activity of the controller. Not all details of this definition need to be explained in this context, as the concept of consent was already introduced by the Directive 95/46/EC and has been thoroughly dissected in the last 20 years. What was interesting in relation to the new GDPR framework was the seeming overreliance of most controllers on the legal basis of consent, which led to some unrest among businesses in the first year of the GDPR. The threat of multimillion Euro fines looming large, many businesses swarmed E-mail inboxes all over Europe with mails asking for consent for all kinds of processing activities, mostly for marketing purposes. It is unclear what caused this notion that consent was the most important (or even a particularly useful) legal basis, considering the other possibilities granted by article 6. For one,

consent must be given granularly[27], that is for each specific purpose and processing activity (recitals 32, 43). This means that the data subject must consent to each processing activity – using their name in a client registry, using their address to ship a product, taking photos at an event, contacting them by e-mail – separately. This makes the process rather cumbersome for the data subject and precarious for the controller to keep track of. Paired with the fact that consent can be revoked at any time and for no specified reason (Article 7/3), it is quite easy for the Data Subject to pull the rug from underneath the Controller's feet and to force them to stop any ongoing processing activities. These reasons alone make consent a rather wobbly basis for any kind of substantial data processing and more of a last resort to use when none of the other bases can be applied. [28,29] As mentioned, it is unclear what caused the initial confusion over-emphasis on consent as a legal basis. Two years later, most guides have caught onto the fact that the other legal bases, especially the fulfilling of a contract and the legitimate interests of the controller, are usually a much more stable foundation for habitual data processing.[30] Especially litera f allowing processing for their legitimate interests gives the Controllers an extensive legal toolbox to work with that even explicitly covers direct marketing purposes (recital 47). The Commission blames "*campaigns from consultancies seeking to provide paid-for advice, by the spread of incorrect information, for instance on the need to systematically obtain consent from individuals*"[31], unfortunately without substantiating this claim further or providing examples The industry reports simply speak of miscommunication[32], leaving it unclear where that miscommunication came from. When examining official EU documents such as the opinions of the Article 29 Data Protection Working Party (Hereafter "*WP29"*) on the subject, they don't exactly convey the notion that consent towers over the other legal bases. Compared to the old regime of Directive 95/46/EC, the new consent rules of the GDPR were not considered a large step forward that would have necessitated the panic that ensued; they were rather seen as the overdue codification of existing judicature and good practice[33] and raised the bar only slightly with elements such as

[27] Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*, Brussels, 2017, p 10

[28] *Stakeholder Report*, p 9

[29] Markus Kastelitz in *Datkomm*, p 206 para 1

[30] *Digital Europe*, p 18

[31] *Taking Stock*, p 10

[32] *Stakeholder Report*, p 9

[33] WP29, *Guidelines on consent under Regulation 2016/679*, p 3

active consent[34] (see also recital 171 on "old" consent declarations being still valid if they meet the GDPR's requirements[35]). The new obligation of being able to demonstrate that consent was given (Article 7 para 1) combined with the principle of accountability in art 5 para 2 combined with the volatile nature of consent declarations is certainly enough to explain the paranoid behaviour exhibited and consulting firms. But on the part of businesses, the weird attraction to this legal basis might stem from the fact that it is only bound by the principle of purpose limitation, and almost any processing could be justified by using the Data Subject's consent. It would be possible, for example, to ask the Data Subject for consent to track their location every single minute of the day – which is exactly what *Google* does when its location history feature is activated [36] - , providing precious and rather sensitive information to the controller. No other legal basis would be suitable for this, as no conventional contract would require such processing to be fulfilled and it would be impossible to argue that the legitimate interest of the controller outweigh the fundamental rights and freedoms of the data subject (lit f). Regarding the problems with consent to cookies in an online environment, see chapter 1.2. about the ePD.

While the principle of lawfulness gives the controller a sound reason to process the data at all, the **principle of purpose limitation** tells them what the data may be used for. The principle is comprised of two main elements: Personal Data may only be processed for legitimate, specific purposes, and further processing may only take place if it is compatible with the original purpose. While this firm restriction can be rather challenging to implement into transparency obligations and internal records such as the record of processing activities, the principle of purpose limitation has not been negatively addressed in GDPR practice. In relation with the e-Privacy directive, however, an even stricter version of the principle of purpose limitation has caused an unlevel playing field for functionally equivalent economic actors (see chapter 2.2.).

Another problem within the general framework was found within a **lack of economic scaling** in some of the obligations[37]. Especially for small and medium sized enterprises – SMEs – the principle of accountability in art 6 para 2 has proven challenging to implement, as they have to adhere to the same standards of data protection as larger enterprises, but with much less human

---

[34] WP29, *Guidelines on consent under Regulation 2016/679*, p 30

[35] Kastelitz in *Datkomm*, p 215 para 40

[36] https://support.google.com/accounts/answer/3118687?p=privpol_lochistory&hl=en&visit_id=637301124642313647-3530353734&rd=1 accessed June 20, 2020

[37] *Stakeholder Report*, p 14

resources. The GDPR makes only one provision directly dependant on the size of the Controller, which is art 30 para 5 regarding the necessity of keeping a record of processing activities. It says:

The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10."

At first glance, one might assume that this means that the rules regarding the records of processing activities barely touch any of the SMEs, given their small size. But the **size privilege** only applies in combination with one of the other three alternative conditions. Especially the second alternative - that the processing may not be occasional – renders any size distinction somewhat moot. The WP29 states in a short position paper:

"[…] a small organisation is likely to regularly process data regarding its employees. As a result, such processing cannot be considered "occasional" and must therefore be included in the record of processing activities.[38]

This again makes it difficult to think of a situation where an enterprise employing at least 10 people would not occasionally process personal data in a GDPR- relevant fashion. Additionally, the record of processing activities plays heavily into other, more basic provisions: The rights of the data subject to access their personal data or have it erased, for example, applies to every controller and in order to be able to grant the data subjects these rights, something akin to the record mentioned in article 30 must be kept in any case. This applies to the basic rules too, as the controller must make sure to have a legal basis for each processing activity and must be able to account for it (art 5 para 2). These factors combined make it unlikely that any business complying with the GDPR will not have a record of processing activities, revealing art 30 as a rather half-hearted attempt at meeting SMEs halfway.

2.1.3. Data Subjects' Rights

In articles 12 to 25, the GDPR confers a series of individual rights to the data subjects in order for them to be able to assert control over the personal data. The addressee is yet again the

[38] Article 29 Data Protection Working Party, *Position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*

controller handling their personal data. These rights can be exercised with no particular form and free of charge (art 12 para 5). Only when the requests are manifestly unfounded or excessive in quantity may the controllers charge a reasonable fee or refuse to comply, albeit with the burden of proof on them. With this relative ease of exercising the rights, it is no surprise that many data subjects have made use of them in the course of two years. This has drawn a rather clear picture which rights have proven especially useful to consumers, and which of them may not have turned out quite as handy.

The **Right of Access** (Art 15) has proven to be rather popular, with 18% of data subjects making use of it according to a Eurobarometer survey from 2019[39] (All following percentages are drawn from this survey). This is mirrored in the fact that most procedures regarding consumer rights before DPAs involve the right of access, as can be seen on aggregating sites such as gdprhub.eu[40] and also when examining the decision patterns of a single DPA such as the Austrian DSB. Out of 31 procedures involving the data subjects' rights, 12 were about the right of access, whereas 15 involved the right to erasure (which also scored 12 % in the survey and 26 procedures in the European aggregate). Due to the contentious nature of the Right to Erasure, it is no surprise that it seemed to have caused the most procedures. Conversely, the right to correct wrong data and the right to Data Portability have also been exercised by 16% and 13 % of users, respectively, but have caused much fewer DPA procedures. These numbers seem to be confirmed by the stakeholder reports, stating that requests for access and erasure spiked in 2018 after the entry into force of the GDPR[41], while other rights such as the ones concerning automated decision making and data portability saw little increase or no requests at all. Especially in the case of the latter, that is an unfortunate development, as the right to data portability was one of the few GDPR provisions that was actually expected to stimulate economic endeavours rather than to hamper them as it would foster a more competitive market environment[42], driving the development of new services. This would lead to more

[39] European Commission, *Special Eurobarometer 487a: The General Data Protection Regulation*, Brussels, 2019, p 13

[40] https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub, accessed June 25, 2020

[41] *Stakeholder Report*, p 7

[42] Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, Brussels 2017, p 3

interoperability and fused services and increase engagement of the user base.[43] As it turns out, these predictions were not unfounded, as even big players took action and started collaborations such as *Google's* Data Transfer Project[44], which aims to facilitate the transfer of company specific data models onto other systems. Lastly, the right to restrict processing leads a rather vestigial existence, not even showing up in the survey and with almost no DPA procedures to speak of; The Administrative Court of Baden Wüttemberg (Germany) denied its application in the case of a civil register entry, as the German Registration Law excludes the application of Article 18. The relative infrequency of this right being invoked by users and authorities might indicate that the concerns uttered in commentary literature about the legislative quality of the provisions were indeed correct, [45][46] especially regarding para 1 lit b. This provision gives the data subject the choice to restrict the processing of unlawfully held data instead of their erasure. This forces the Controller in a weird predicament where they are obligated to process data they were not allowed to process in the first place without any control over them, essentially removing their status as Controllers. This provision constitutes the only obvious mishap in Chapter 3, but it causes no significant problem because it can evidently simply be ignored in practice.

What quite definitely cannot be ignored in practice are articles 13 and 14 regarding the information obligations. Here, the problems encroach from both sides of the spectrum. On the side of businesses, the reports mention common problems with incomplete or unclear information and general difficulties with how the information demanded by the GDPR should be presented[47]. Table 1 shows a comparison between the information demanded for the privacy notice that must be made available to every data subject before collecting any of their data, the information that must be granted upon exercising the Right of Access and the information needed for the record of processing activities. It becomes evident that art 13 demands even more categories and a more detailed account of the data being processed than is needed for the actual internal records of the controller (which of course are more extensive in quantity as they include

---

[43] Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay, Ignacio Sanchez, *The right to data portability in the GDPR: Towards user-centric interoperability of digital services*, Computer Law & Security Review, 2018, p 202

[44] https://datatransferproject.dev/, accessed June 25, 2020

[45] Viktoria Haidinger in *Datkomm*, p 413 para 18

[46] *Feiler/Forgó* p 154 para 4

[47] *Stakeholder Report*, p 6

all processing activities). In principle, it is laudable that this sort of information must be made known to any data subject; But it becomes more and more and more obvious that the GDPR, mandating the presentation this dense package of information in a clear, understandable and simple manner, demands a squaring of the proverbial circle. The EU's recommendations in form of working party documents and within the GDPR itself have not made these information duties particularly easier. While the WP29-guidelines are extensive and quite useful, they are not of help especially for small controllers struggling to present their data policies because off their strictness and insistence on thoroughness. They include recommendations like the following: "*WP29's position is that, as well as providing the prescribed information under Articles 13 and 14 […] controllers should also separately spell out in unambiguous language what the most important consequences of the processing will be."*[48] The working party therefore asks for even more information to be included. At the same time, the GDPR itself insists on the use of icons to convey transparency. Throughout several recitals (60, 166) and even in the main text itself, the GDPR strongly suggests that the use of icons may be good idea. As of mid-2020, these symbols have not yet caught on as a general practice and the Commission has not made use of the implementation clause found in article 12 para 8. This lack of action on the part of legislators has also been noted at the Privacy Icon's Forum in Berlin in January of 2020[49] The research that is currently being done on the topic seems to be leaning more in the direction of risk-based assessments, e.g. where data subjects are informed about the possible risks of a processing activity or a potential lack of encryption via bright red warning symbols.[50] This research is definitely welcome and has yielded useful results such as the DAPIS project with its first set of useable icons for GDPR transparency, but it is doubtful whether the information demanded in article 13 and 14 even lends itself to visual displays of this kind. The exuberance of the legislators has led to unpleasant results such as an AI-driven study finding that out of 14 privacy notices of IT Companies like Apple, Microsoft, and Steam, none fulfilled the requirements[51]. This leads to the other side of the coin, which is comprised of the users seemingly not

---

[48] Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679* , Brussels, 2018, p 7

[49] https://privacyiconsforum.eu/gdpr-data-protection-icons-and-transparency-where-do-we-stand-panel-at-the-cpdp-2020/, accessed June 30, 2020

[50] Zohar Efroni, Jakob Metzger, Lena Mischau, Marie Schirmbeck, *Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing*, EDPL 3/2019, p 365

[51] Giuseppe Contissa, Francesca,Lagioia, Przemyslaw Palka et al, *Claudette Meets GDPR: Automating the Evaluation of Privacy Policies Using Artificial Intelligence*, SSRN Electronic Journal, 2018

understanding the overly complex information that is presented to them. Comparing the Eurobarometer surveys from 2011 and 2019, the answers to the question "*Thinking about privacy statements on the internet, which of the following sentences describes what you usually do*?" have not changed to the better: in 2011, more than half of the users (58%) read the statements completely; In 2019, this number dropped to 13 %. Furthermore, 37% have not at all read the privacy notes they encounter in 2019, with the number 1 reason for that being that the users found them too long to read.[52]

What to make of all this? Overall, it seems that the rights of data subjects have caused no significant problems among European Businesses, with the rights being rather intuitive for the data subjects and comparatively easy to respond to for controllers In regard to the transparency obligations, practice has shown that the information demanded cannot be presented in a manner that is concise enough for data subjects to actually be informed by it. The legislators have made the mistake of assuming that maximum transparency on the part of the users would be achieved by obliging the controllers to turn their internal processing records to the outside and to dump massive amounts of information on the user, all the while grimly demanding clarity and simplicity without considering whether these qualities are even possible when providing all the information. The equation of more information = more transparency does not hold, because consumers do not think in this analytical manner. The legislators saw this coming and added the lukewarm call for icons, but these icons presumably do not work with the demanded information. This is an area of the GDPR where a change in the text itself would alleviate unnecessary economic burden by making it easier for controllers to present the required information and for users to actually understand it in order to avoid **information fatigue**. In practical terms, it would be advisable to simply move parts of article 13 into article 15 and thereby expand the Right of Access. Especially Article 12 para 1 literae e (recipients of personal data), f (intention of international transfer), and para 2 literae a (Period of storage) as well as the seemingly crucial information of the legal basis in para 1 lit c. This might seem extreme, but for the average, rather uncritical data subject, the information on what *purposes* the data are used for is much more important than the legal basis, which presents itself as a technicality that the legal layman wouldn't know how to make use of. It seems more practical to include the basic information of what data is used to which purposes, and that the data subject has the right to

[52] *Eurobarometer 2019*, p 21

demand the full information on their case of processing at any time and free of charge. This would leverage the fact that at present, businesses are still somewhat swarmed with access requests that mainly cause internal costs and not much benefit to the inquiring users, as much information is simply doubled by demanding it must be communicated before any processing even takes place. The value of both the information obligations and the Right of Access would increase at the same time, as the former becomes more concise and effective and the latter less redundant.

Information given in Privacy Notice (art 12)	**Information granted by Right of Access (art 15)**	**Information in record of processing activities (art 30)**
Identity and contact details of the controller/DPO		Identify and contact details of the controller/DPO
Purposes of processing Legal basis of processing (including legitimate interests in case of art 6/1/f	Purposes of processing	Purposes of processing
Recipients of personal data	Recipients or categories of recipients of personal data	categories of recipients of Personal Data
Period of storage	Period of storage	Period of storage
transfers of personal data to a third country	Information about the appropriate safeguards of the transfer to a third Country	Transfers of personal data to a third country
Mention of all the data subjects' rights including withdrawal of consent	Mention of all the data subjects' rights to erasure, rectification, restriction and objection	

Whether the provision of the data is a legal requirement		general description of the technical and organisational security measures
The existence of automated decision making	the existence of automated decision-making	
Right to file a complaint	Right to file a complaint	

Table 1: Comparison of Information Obligations in articles 12, 15, and 30

2.1.4. DPAs and Harmonisation Issues

As mentioned before, the GDPR is known as a limping Regulation with many opening and implementation clauses. While the former require the member states to take legal action themselves in order to give the broader GDPR guidelines a concrete shape in national law (such as articles 51 to 54 establishing DPAs), the latter give the member state some leeway by letting national laws diverge from the standard GDPR Provision. The difference between the two is usually indicated by the modal verb used to introduce them: Where it says "The member States *shall*…", an implementation clause will follow, and where the member states "*may*", a facultative opening clause will follow. An example for the latter would be Article 8, allowing differing ages of consent for minors. Some have warned beforehand to not make too much use of these facultative opening clauses, prescient of the fragmentation they can bring.[53]. For economic actors, the difference between the two types of provisions does not matter, as both will lead to the same result: disharmonisation. This has been a frustrating issue for industry stakeholders, as one of the main promises of the GDPR for the European economy was that the new rules, strict as they are, would greatly reduce all costs associated with differing national laws. Not all opening and implementation clauses have been problematic, but a handful of them keeps being mentioned in the context of economic activity.

Firstly, differences between DPA structure and practice are very noticeable in practice and have proven problematic in some regards. As was mentioned above, the member states are more or

[53] Lukas Feiler, *Datenschutz-Grundverordnung ante portas*, jusIT 2016/93, Heft 5, p210

less free to organize their DPAs in any way they see fit; The 16 different provincial DPAs in Germany have turned out to be a special nuisance for industry stakeholders[54]. Generally, the DPAs are lauded for their cooperative attitude and their reliance on other tools than the dreaded fines, which is also reflected in some legislation such as the Austrian DSG (data protection law) stating in §11 that the local DPA will make sure to particularly issue warnings in cases of first-time offenders (as opposed to resorting to fines directly). But due to their granularity, provisions such as Article 35 paras 4 and 5 become problematic. They invoke the national DPAs to publish white- and blacklists of kinds of processing operations which require a data protection impact assessment according to para 1 leg cit. The same goes for arts 33 and 34, stating that the controller must notify the DPA or the Data Subjects, respectively, in case of a data breach, but only if the breach is "likely to result in a high risk to the rights and freedoms of a natural person". The European Data Protection Board and the wp29 would do well to heed the advice of the industry report to publish a consolidated list of processing activities regarding art 35 and well-defined criteria for arts 33 and 34. No substantial legislative power would be taken from the member states with such action, and the benefits would clearly be in line with what the GDPR is trying to achieve. Some DPAs remain critically understaffed due to the fact that most of them were simply rebranded or not changed at all when the GDPR came into force, with no changes to their infrastructure. Many DPAs reported needing critically more budget than they are currently working with: especially Mediterranean member states such as Greece (100% more Budget needed), Italy (37%), Croatia (127%), but also eastern DPAs such as the ones in Latvia (257%), Poland (53%) and Romania (97%).[55] The Irish DPC has been understandably busy, with it being the place of the main establishment of several large internationally active IT Companies, and stocked its personnel up to 140 staff members by the end of 2019. [56] (As opposed to, for example, the Austrian DPA with roughly 40 staff members). This trend of stocking up resources of DPAs will have to continue for a while in order to improve the respectability of their decisions and to facilitate the harmonised enforcement throughout the Union, especially in the above mentioned countries with underfinanced DPAs.

---

[54] *Stakeholder Report*, p 12

[55] European Data Protection Board, *First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities*, Brussels, 2019, p 10

[56] Irish Data Protection Commission, *Annual Report*, Ireland, 2019, p 8

Most other opening clauses have not caused hinderances, with a few exceptions. All differences stemming from Art 8/1 allowing for different ages of consent for children could easily have been avoided[5758], if the legislators had made a choice and stuck to the harmonisation principle of the regulation. That would have spared the working party having to encourage "the Member States to search for a harmonized solution in this matter."[59] This would of course not have solved the basic conundrum of how the users' age should be verified in a digital society without collecting heaps of additional data just to be able to verify the age of the consenting subject. This seems to stand in opposition of article 11, where the GDPR acknowledges that it would be counterproductive to process even more personal data for sole reason of complying with the GDPR if this additional data is not needed for the purposes of the controller. An example could be signing up for an internet forum via E-Mail and nickname, with the controller having to gather even more information to make sure the user giving consent is old enough (assuming they're dealing with personal data). If the Controller doesn't collect the data, they are at risk of unlawfully processing data. A mere checkbox where the new subscriber types in their age would be rather useless and seems like a mere formality covering up a lack of substantial compliance with the law. And yet, the working party recommends this procedure at least in "low risk situations", admitting that it might not be a "watertight solution in all cases. " While it is obvious that minors need an additional level of protection when it comes to giving consent, this basic problems often puts controllers in an uncomfortable position having to collect more data than they normally would, lest they risk the extreme disadvantages of unlawful processing. A possible approach to a compromise in this situation would be to simply take the notion of low-risk services or low risk categories of personal data, and exempt them from this rule. This might seem extreme, but it would be an objectively better situation than having minors give their consent where they are not allowed to because all they have to do is click a little box, with the controllers processing their unlawfully, but also unknowingly so. Excluding categories of low risk services such as internet forums and E-mail services from the age restriction would at least resolve the current predicament caused by the GDPR. It must be noted that this line of reasoning is seen purely from a data protection lens and is only recommended in relation to the current, unfair, situation as created by the GDPR; It does not consider the question whether children

[57] *Digital Europe,* p 7

[58] *Stakeholder Repor*t, p 10

[59] Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*, p 23

should be able to conclude the necessary private law contracts for these services (see also art 8 para 3).

Another point that has been often brought up is the possibility of class action based on the mandate of individuals[60]. The Commission laments that not more Member states have made use of the opening clause in article 80 para 2. Para 1 leg cit establishes that any data subject can have a not-for-profit organisation with statutory objectives which are in the public interest and is active in the field of protection of personal data lodge complaints to DPAs on the data subject's behalf, if the latter so chooses. The addressed opening clause in para 2 allows member states to provide within their national law that these same organisations can file complaints without the data subject's mandate. The aim was to combat passiveness on the side of consumers and a general unwillingness to engage in long, costly procedure out of which the plaintiffs stand little to gain. This aim was achieved quite swiftly, with, for example, none of your business and La Quadrature du Net filing in a complaint against google on the very same day the GDPR entered into force. This led to one of the largest fines yet issued, costing google 50 Million Euros.[61] It therefore seems that the objective of this provision has been reached regardless of whether the opening clause was used, especially since it is comparatively easy for a member off said organisation to simply file a complaint privately and then mandate their own association.

2.2. The E-Privacy Directive and the coming E-Privacy Regulation

The E-Privacy Directive from 2002 -hereafter "ePD" - was conceived long before the GDPR as a corollary piece of legislation to Directive 95/46/EC and is still in force to this day. Now it serves as a self-declared *lex specialis* to the GDPR, complementing and particularising the latter with provisions that apply to the processing of personal data for publicly available electronic communications services. A short overview of its main content, with a focus on those provisions that are likely to have additional economic effects, will help place it within the legal framework and explain its relationship to the GDPR. All article and recital mentions in the following chapter refer to the ePD unless specified otherwise.

[60] *Taking Stock*, p 8

[61] French CNIL, Decision SAN-2019-001

The E-Privacy Directive serves two main goals:

- to ensure an equivalent level of protection of fundamental rights and freedoms with respect to the processing of personal data in the electronic communication sector, and
- to ensure the free movement of such data within the single market. (Article 1, recital 2)

To those ends, the ePD defines a certain **scope of application** for the different provisions it has. This scope is rather fragmented in that different articles apply to different sets of companies or even private persons[62]. Essentially, there are two main areas of application:

1. Specific, **stricter rules for data processing** that apply to the providers of telecommunications services.

A was stated above, the GDPR requires the controller to have a legal reason for any processing of personal data. As the ePD is a much older document (given the rate of technical progress), several articles of the ePD are "consumed" by the GDPR insofar that the latter's generally applicable obligations demand the same standards as the ePD[63], which is why not all of its provisions generate noticeable legal and economic consequences for service providers; The GDPR is particularised by the ePD and data processing in the context of providing an electronic communication must meet higher standards.

Articles 6 and 9 severely hinder a service provider's ability **to process traffic and location data**: Under the ePD, they may use traffic and location data only to the purpose of providing the communication service to their subscribers, and the only possible legal reason for this processing (other than providing the service) is the user's consent. In essence, this constitutes an even stricter limitation of the legitimate purposes available to the service provider and prohibits them from engaging in any kind of advertisement-based models since they are not allowed to use the subscriber data for anything other than providing and marketing their own service.

An important detail is that in the text of the ePD these rules apply to the **providers** of electronic communication services. This means that the following types of companies **are addressed**:

- Telephone providers

---

[62] Joris van Hoboken, Frederik Zuiderveen Borgesius, *Scoping Electronic Communication Privacy Rules: Data, Services and Values*, JIPITEC 198, 2015

[63] The European Data Protection Board, *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*, 2019

- Internet providers.

  These service Providers are limited in their ability to process traffic and location data.

The following types of services/companies are **not** addressed:

- Analogue radio and television broadcasting[64]
- Providers of **Over-The-Top (OTT)** services. OTT services mean the use of existing infrastructure – mainly the internet – to convey any type of content, be it videos, music or websites, but also instant messaging, (video-)calling or e-mails.[65] Examples for services **not covered** by the ePD's main provisions: Radio Stations, *Whatsapp, Zoom, G-Mail, Netflix, Spotify*

Even though some of these services, especially messaging applications, are functionally equivalent to classic communications services such as SMS texting or calling, their providers do not have to adhere to the special provisions of the ePD- only to the general framework established by the GDPR. However, since the ePD is a **directive**, there are substantial differences in the national implementations of the material scope. While in some countries OTTs are covered by the transformed ePD, other countries have opted not do so in legislation and judicature, causing considerable confusion on the topic.[66] This fragmented state has been cemented by the ECJ, which decided in mid-2019 that *Gmail,* in its function as a webmail provider, was not covered by the EU framework directive, and in extension of that cannot be considered to be covered by the scope of the ePD.[67] The other rules established by articles 7,8,10,11 and 12 are less incisive and establish an array of opt-out rights for subscribers of ECS, e.g. opting out of subscriber databases, itemised billing and setting call identification preferences.

2. Rules regarding the storing of or gaining access to **information in the terminal equipment** of a user- in other words, rules regarding the handling of **cookies**.

---

[64] European Commission, Directorate-General of Communications Networks, Content & Technology, *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation,* Brussels, 2015, p 25

[65] Body of European Regulations for Electronic Communications, *Report on OTT services*, BoR (16) 35, 2016, p 14

[66] *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*, p 116

[67] ECJ case C-193/18, recitals 40, 41

These provisions found in article 5 para 3 ePD are what led to its endearing nickname of "*the cookie directive*"[68], because they are not limited to any kind of service provider. Instead, they apply to anyone storing cookies on any kind of terminal device, which means that this provision affects a vast array of economic actors.[69] Any business or private person that operates a website lies within the scope of article 5.3. In order to place any cookies on a terminal device beyond those strictly necessary to provide the service (e.g. those necessary for the functioning of the website), the informed consent of the user is required. User consent, therefore, is the only legal reason for this type of data processing, which means that the ePD complements the GDPR in this case by making it even stricter. In practice this mainly translates to the cookie pop up that every user readily clicks out of the way when visiting any website. Although the obligation to place these consent popups has existed since 2009, the fines threatened by the GDPR have successfully incentivised most website operators to fulfil it (although as of now, it still depends on the national implementing law how severe the fines can be). In the wake of these provisions, the problem of **consent fatigue** has often been mentioned[70]: Due to the granularity required by the law, consent must be given for each individual processing activities. This consent must be given actively, and not as a mere "opt-out" variant. Since the GDPR rules for consent apply to the ePR context as well (Article 2 lit f). This leads to users being swarmed with pop up windows asking for their consent, and has caused the perverse effect of less engagement with the lawfulness of the processing situation in spite of ever stricter legal safeguards. This situation is similar to what was stated about the effects of too detailed information obligations ins chapter 2.1.3.

Now that its objectives, scope and basic content are clear, the ePD must be placed within the **larger context** of the GDPR. How do their provisions interact? As was mentioned above, there are significant overlaps between the two texts, especially as both of them demand a data breach notification and "appropriate technical and organisational measures"[71,72,73]. It therefore seems apt

---

[68] As amended by Directive 2009/136/EC

[69] European Commission, Deloitte, *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, 2017, p 137

[70] WP29, *Guidelines on consent under Regulation 2016/679*, p 17

[71] *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities* p 15

[72] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, p 1

[73] Article 29 Data Protection Working Party, *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)*, Brussels, 2017, p 1

to imagine the ePD as protruding from under the larger veil of the GDPR in several spots. Its main additional legal consequences lie in the fact that ECS providers have limited purposes and legal reason at their disposal when processing user data, and that anyone storing cookies on any terminal device must do so with the informed consent of the device owner. Especially the latter would in part be achieved by the GDPR alone, but the ePD makes sure that user consent is required, and it applies to all forms of data, not just personal data. All of its provisions are also expressively applicable to legal persons (art 1 para 2), extending its scope beyond that of the GDPR.

Subject matter	Scope of application
Establishment of appropriate technical and organisational measures to safeguard security of its services (Art 4/1)	Only ECS Providers
Data breach notification (Art 4/2)	Only ECS Providers
Confidentiality of Communications (Art 5/1)	Unclear; Possibly wider than the above [74]
Consent for storing Cookies on any device (Art 5/2)	Any website operator
Limiting the processing of traffic and location data (Art. 6 and 9)	Only ECS Providers – not OTTs (depending on member state)
Specific technical options that must be made available for end users: Calling line identification, subscriber databases, call forwarding (Art. 7,8,10,11)	Only ECS Providers

Table 2: Scope of application of the ePD's provisions, controversial aspects highlighted

Over its lifespan, **the ePD has therefore achieved** two things: It has distorted the internal market for communication services by imposing restrictive data processing rules on ECS providers, but not on OTT providers that offer competing services that are functionally identical to the end consumer.[75] It has increased bureaucratic expenses throughout Europe due to its nature of a Directive, as it had to be transposed into national law, with variances along all 28 member states, with different authorities than the data protection authorities tasked with watching over individual articles. It has made it necessary for every website operator to obtain user consent for

[74] *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, p 99

[75] *Scoping Electronic Communication Privacy Rules: Data, Services and Values*, p 203

storing cookies. Especially the first point has induced criticism from stakeholders active within the industry and is not lost on the EU itself, which has mandated several studies on the transformation and performance of the ePD. The findings of these and other studies have led to the **conception of an E-Privacy regulation**.

The proposal for this regulation was adopted in 2017 and was originally supposed to enter into force alongside with the GDPR. It has, however, spent the last three years in the limbo that is the EU's ordinary legislation procedure, and has seen no less than 6 council presidencies pass by without reaching a unanimous decision by the council.[76] As of May 2020, the last changes were made on march 6, 2020;[77] In the past 20 revisions the text has been altered extensively compared to the first version of 2017, and has in some instances reverted to the original form, disregarding some changes made since 2017. Regardless of that, the main structural changes to the existing regime that are likely to have an impact on the internal market are already decided upon (and will be elucidated hereafter). Wherever the newest amendments alter the proposal, they do so by making it ever more detailed and incisive, meaning that any predictions made about the economic impact of the current proposal will most likely hold true for the final version. After the assessment studies mandated by the EU deemed the general existence of a separate piece of legislation to regulate the matter necessary and identified the measured increase of the protection level as the most suitable option,[78] the ePR now pursues the same objectives as the ePD and reiterates most of its content.

2.3. The E-Privacy Regulation

2.3.1. General Framework

The following chapter will analyse the ePR in its current version as of March 6, 2020, and the effects it is likely to have on businesses. All article mentions refer to this version of the ePR, unless specified otherwise. In a nutshell, the result of the extensive REFIT exercise performed by Deloitte for the EU (see footnote 70) and of other analyses was that the ePD was justified in its

[76] EUR- Lex Homepage, https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52017PC0010#2020-03-06_DIS_byCONSIL , accessed 3. May 2020

[77] Council of the European Union, Interinstitutional File: 2017/0003(COD), Brussels, 2020

[78] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, p 2

legal goals – mainly to safeguard the confidentiality of electronic communications – but ineffective and costly in reaching them, as well as outdated in its choice of legal definitions.[79] Thus, five different policy options were offered by the Commission to be tested for their potential effects on the internal market. Among those five options, the one specified as "Measured reinforcement of privacy/confidentiality and simplification" was deemed the preferred option. It seemingly struck the balance between attaining the predefined objectives and keeping the predicted admirative burden and compliance at a bearable level. Given the summary of the ePD in the previous chapter, any new piece of legislation would have had to address these points of contention:

- The discrepancy in the scope of application, covering ECS providers, but not OTT Service providers,
- The extensive burden imposed on website operators by the provisions regarding the interaction with terminal equipment and
- The administrative burden created by 28 different transformations and interpretations of the ePD Provisions
- while still keeping the confidentiality of communications intact, as this is one of the main factors for attributing so called EU-added value to both the ePD and the ePR. [80].

The ePR addresses the first point by cleaning up its scope of application, stating clearly that it applies to

- *the processing of electronic communications content data and of electronic communications metadata carried out in connection with* ***the provision and the use of electronic*** *communications services;*

- *end-users' terminal equipment information .*

- *the offering of a publicly available directory of end-users of electronic communications services;*

- *the sending of direct marketing communications to end-users.* (Article 2 para 1)

---

[79] European Commission, Deloitte, *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, p 211

[80] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, p 5

This leaves no wiggle room for providers of OTT services. [81]. Electronic communication content is defined as content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound, meaning that a wide range of services like as *Whatsapp* or video calling applications process electronic communications content in order to function. Therefore, any application processing communication content or its metadata in connection with at least the use of the internet or the phone lines is covered by the ePR. The intent of levelling the playing field for the providers of functionally equivalent services was an explicit goal in drafting this regulation[82]; and this goal will be achieved by the current version of the ePR. The same applies for any fragmentation issues, as the ePR's nature of a regulation will serve to harmonise the communication framework rules across all member states. However, The legislators have yet again opted to include a number of **opening clauses** in the Regulation; Although the ePR does not limp in the same way the GDPR does in that it is in need of national implementation to even work properly, a handful of facultative opening provisions will be likely to cause harmonisation issues, should the member states choose to utilize them. Provisions such as article 16 para 2a, for example, allow the member states to set a period of time after the sale of a product or a service in which the service provider may use the end-users contact details for direct marketing. National differences in these timeframes are programmed to cause headaches for service providers, given that most other matters are harmonised.

Moving on to the **specific rules of processing electronic communications data** , article 5 ePR makes it clear that *Any interference with electronic communications data, […], by persons anyone other than the end-users concerned, shall be prohibited*, except when permitted in the Regulation. In principle, the ePR differentiates 3 main kinds of data sets and provides individual rules for their processing (see table 3): There are **electronic communications data**, which is comprised of **electronic communications conten**t (such as pictures or a message sent over whatsapp, henceforth "*content*") and **electronic communications metadata** (such as the duration of a call, number of messages sent etc., henceforth "*metadata*"), and **terminal equipment information**.

Article 6 gives a general frame for how electronic communications data are to be processed and to which purposes. Article 6a and 6b follow up with specific rules content and metadata,

[81] Keren Shatkin, *Analyse des Entwurfs der e privacy Verordnung*, Universität Wien, Austria, 2018, p 15

[82] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, p 4

respectively, with content having the strictest processing rules as it is the most sensitive set of data. Art 6a states:

Providers of electronic communications networks and services shall be permitted to process electronic communications content only:

for the purpose of the provision of a service requested by an end-user for purely individual use if the requesting end-user has given consent, or

if all end-users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes

The general idea seems to be to limit both the possible legitimate purposes and the legal bases for data processing at the same time. This is likely to be read as a restriction of the legal basis to only the provision of the requested service with user consent. This is also implied by the following article 6b regulating the processing of metadata, stating it is only permitted if:

the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, or

it is necessary for the provision of an electronic communications service for which the end-user has concluded a contract; or

it is necessary to protect the vital interest of a natural person, in the case of emergency, in general upon request of a public authority, in accordance with Union or Member State law; or

it is necessary for the purpose of the legitimate interests pursued by the electronic communications service or network provider, except when such interest is overridden by the interests or fundamental rights and freedoms of the end-user, in particular where the end-user is a child.

This provision already mirrors article 6 GDPR much more closely, and provides a similar set of legal bases using the same formulations as the GDPR. Especially the inclusion of the legitimate interest of the service provider is a rather significant concession to the business stakeholders, allowing them to handle metadata comparatively freely. It must be stressed, however, that the legitimate interests of the service provider are explicitly considered overridden by those of the user if the service provider tries to use the metadata to create an individual profile of the end-user (art 6a para 1 lit e, second part). Therefore, the processing rules for metadata remain stricter than the general GDPR rules, albeit not as strict as those for electronic communications content.

Lastly, **terminal equipment information and cookies** are treated similarly to metadata, as article 8 ePR allows for quite extensive processing possibilities. Para 1 reads:

*The **use** of processing and storage capabilities of terminal equipment and the **collection** of information from end-users' terminal equipment other than by the end-user concerned shall be prohibited, except on the following grounds […],*

leaving it unclear whether collecting information means the same as processing it in the sense of the GDPR; Since making proper use of these data in order to be able to provide a service – say, allowing for geolocation by means of terminal equipment data – would entail extensive processing, this provision must likely be read this way. Processing terminal equipment data is generally allowed if

- user consent is given
- it is necessary carrying out the transmission of an electronic communication over an electronic communications network or for providing an information society service requested by the end-user;
- it is necessary to locate terminal equipment when an end-user makes an emergency communication either to the single European emergency number '112' or a national emergency number
- or if carried out in the legitimate interests of the processor, where again building an individual user profile is explicitly excluded from being a legitimate interest. (Article 8)

The handling of cookies – that is, information stored in and levied from the terminal equipment of the user – has become considerably more complicated and verbose in the ePR compared to its predecessor. This is no surprise, as over the last 10 years, the issues of tracking end user devices, M2M-communication and the internet of things has become much more prevalent. All of these technologies are determined by the interaction with terminal devices, and the ePR being a directly applicable regulation necessitated rather complex rules. As the main concern with the old regime was the fact that any website operator had to indiscriminately collect end user consent for any cookies that exceeded the bare technical necessities – causing noticeable cost for businesses and consent fatigue for users -, the Commission had originally opted for a so-called browser solution, as proposed by the Deloitte assessment. In the first version of the ePR proposal, Consent for interaction with terminal equipment could be given "*by using the*

appropriate technical settings of a software application enabling access to the internet" (Article 9 para 2 original ePR Proposal), meaning that consent could be expressed within the browser settings. This was supposed to both avoid over-saturation of the users caused by cookie popups on almost every website, and to free individual website operators of compliance costs, shifting them to the browser providers. This browser solution took heavy criticism from both WP 29 and industry stakeholders. The working party, adamant on maintaining high levels of data protection and not wanting to undermine the GDPR standard, pressed that the end user must be able to give their consent on a per-purpose basis, not through non-specific browser settings, so as to maintain coherence with art 7 GDPR (concerning the modalities of consent). Additionally, the obligations to provide users with sufficient information must be met, in order for the end-user to be able to give informed consent according to the GDPR[83] (not to be confused with the information obligation in articles 13 and 14 GDPR, which are more extensive than the information required to give informed consent[84],[85]). While a solution to these problems could potentially be integrated in the technical infrastructure of the browser software, criticism from the some industry stakeholders aimed to prevent precisely that, as it would essentially delegate the compliance with European data protection rules to foreign companies, as almost all browser software is US-based.[86] The legislators have since ostensibly caved in to some of the criticism and adapted the text mostly favouring economic interests. In the ePR's current version, the subject of gathering cookies is split up in two articles, art 4a and art 8. As mentioned above, the collection of terminal equipment information is regulated similar to that of electronic communications content and metadata, with explicitly enumerated purposes and legal reasons. What remains of the old browser solution is found Art 4a para 2, stating that

"*Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1*) [referring to the storing of information on terminal devices based on the owner's consent, author's note], *consent may be expressed by using the appropriate technical settings of a software application* ~~*enabling access to the internet*~~ ***placed on the market***

---

[83] Article 29 Working Party, *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)*, Brussels, 2017, p 17

[84] *Feiler/Forgó*, p76 para 25

[85] Hödl in *Datkomm*, p 102, para 121

[86] https://www.faz.net/aktuell/eprivacy-verordnung-faz-schickt-offenen-brief-an-die-eu-15037279.html, Letter from press industry stakeholders to the EU, accessed June 23, 2020

permitting electronic communications, including the retrieval and presentation of information on the internet."

(The crossed-out passages show the old formulation, the bold passages show the additions in the current version.)

Compared to the old wording, the new description of the software application has become wordier and apparently more inclusive. Where before, "enabling access to the internet" – which was a rather clumsy way to address browsing software – could more or less only refer to a browser, the new formulation would in theory also include a messaging service. It can also be assumed that it includes more than just web browsers because the legislators could have just used the definition of the "internet access service" found in Article 2 of Regulation (EU) 2015/2120. Effectively, this provision alters the base GDPR rules on consent (in art 7 GDPR) insofar as the controller no longer has to demonstrate directly that consent was given by a specific individual data subject (Art 7 para 1 GDPR), but rather that the technical protocol shows that consent was given on the terminal equipment (Art 4a para 2). If the end-user is adequately informed and the consent is actually necessary for the requested services, the other GDPR requirements for valid consent would be met. Regarding cookies, this will shift the burden of the website operator away from implementing a consent pop-up on every single website to managing their relationship with the operator of the browser software, in order to be able to demonstrate via technical protocols that the collected cookies – which can in principle be collected for any purpose, also in the sole interest of the controller – were placed with user consent. If implemented correctly, this new solution should be able to effectively tackle the issue of consent fatigue.

Types of data:	Electronic communications data (art 6)		Terminal equipment information (art 8)
	Content (Art6a)	**Metadata (Art 6b)**	
Purposes	- the provision of a service requested by an end-user for purely individual use if the requesting end-user has given consent - Other purposes if consent from all end users (needs assessment	- Any specified legitimate purpose if the end user concerned has given consent	- - Any specified legitimate purpose if the end user concerned has given consent
Legal basis	- Only user consent	- User consent - Provision of a service within a contract - Protect vital interest of person - Legitimate interests of the processor	- the end-user has given his or her consent; or - it is necessary for carrying out the transmission of an electronic communication over an electronic communications network/ it is necessary for providing an information society service requested by the end-user; or; or - (d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user

Table 3: Types of Data covered by the ePR per Legal Basis and Purpose

2.3.2. Interaction with the GDPR

Again, the same question arises as it did with ePD: How do the ePR and the GDPR interact? And, more importantly, does the ePR really elevate the level of protection and bring added value

to the data protection framework? It depends on the type of data that is being processed. As the ePR explicitly includes data of legal persons and non-personal data, it has a naturally extended scope compared to the GDPR; It is however, hard to think of a case where any type of electronic communications data (including content and metadata) would not be personal data in the hands of the processing service provider, given the extensive definition of personal data in the GDPR and in judicature. As stated in recital 26 GDPR, is enough for the natural person to be identifiable with the given piece of data alone or in combination with other data, and the service provider would in most cases be able to link any data – be it content or metadata – to a device, an identification number and therefore to a natural person.

As for **the level of protection**, it remains unclear whether the ePR in its current state would bring significant added value to the current system. The allowed purposes and legal bases for processing metadata and terminal equipment information (Arts 6b and 8 ePR) more or less mirror the GDPR with slightly stricter variants of the legal bases. It is noteworthy that the service provider can process these data also in their own interest, similar to art 6 para1 lit f GDPR; This is a big concession to the industry stakeholders and will not exactly please authorities such as the WP29 and the European Data Protection Board. Only in regard to electronic communication content, there seems to be a noticeable improvement in the level of protection, as it can only be processed for narrow purposes with the user's consent. Rules such as art 7 ePR – "*The provider of the electronic communications service shall erase electronic communications content or make that data anonymous when it is no longer necessary for the purpose of processing in accordance to article 6(1) and 6a(1)"* – are entirely superfluous, given that the exact same result could be drawn out of art 5 para 1 lit c and e (Principles of data minimisation and storage limitation).

Concerning the **enforcement of the new rules**, the ePR intends to call upon the DPAs to monitor the application (it could in theory also be a newly installed authority that meets the exact same requirements in articles 51 to 54 GDPR, see article 18 ePR); The member states may rely on other authorities with "*sufficient expertise*" for monitoring articles 12 to 16, comprised of classic telecommunication matters: Unwanted calls, phone directories, line identification and emergency communications. This means that the already existing classic communication authorities wil continue their work relating to phone land lines. It is highly doubtful that member states will create new authorities that exactly mirror the existing DPAs. This will inevitably lead to more workload coming to the already over-encumbered DPAs (see chapter 2.1.4.) and not exactly smoothen out the transition from ePD to ePR.

Further analysis seems idle, given how extensively the draft has already been changed and is still changing as of May 2020. **In conclusion**, the ePR will address the most ardent issues under the old ePD regime in a way that will most likely please some of the industry stakeholders – that is, the classic service providers. They no longer have a disadvantage to OTT providers, which will have to adhere to the ePR standards in all of Europe. If the Council avoids overbearing opening clauses, this unification will likely reduce red tape, as was stated in the Deloitte report; It will, however, place an economic burden on the newly included OTT providers, as everything from dating apps (Recital 11a) to streaming platforms are now potentially affected. This means that where before, these platforms were able to rely on all the legal reasons provided by Art 6 GDPR when processing electronic communications data, they are now more restricted when processing both electronic communications data and pertaining metadata. For example, a messaging app now can now no longer use its user data to create user profiles out of both communication data and data levied from the user's terminal equipment (without the user's consent), where before this would have been possible under the GDPR. This could severely hamper the processor's ability to generate ad revenue or other forms of data-based revenue. At the same time, this would not result in a significantly higher level of protection. The GDPR has all the safeguards in place to prevent the abuse of metadata or terminal equipment data, if both users and authorities take their rights and duties seriously and act on them; When it comes to the protection of communications content – an absolutely important and sensitive issue – the ePR doesn't bring quite enough to the table to be considered a clear improvement over the status quo and to outweigh the economic disadvantages that it entails.

This relates to one of the **other options** that were evaluated by the Deloitte assessment paper: namely **to simply repeal the ePD with no replacement** and let things play out under the general umbrella of the GDPR. Obviously, this course of action would have been the most industry-friendly option to reduce red tape and compliance cost. As the Deloitte study put it quite dryly, "*The repeal of the ePD would generally have positive impacts*"[87]: Compliance cost would be reduced to zero, administrative burden for authorities greatly reduced, the differences between the service providers would be levelled and the internal market would profit. But the policy objectives – especially the safeguard of confidentiality and security of communications – would not entirely be met by the GDPR, as communications data could potentially be processed without

[87] European Commission, Deloitte, *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, p 412

consent and legal persons as well as non-personal data would not be protected. Active user rights such as hiding phone numbers on a per call basis or block unwanted calls would be absent as well. Eventually, the decision for a new piece of legislation was obvious, as the EU is not keen on reducing its supranational influence by repealing its legislation without replacement, and they are somewhat stuck between a rock and a hard place: Keeping the old regime intact would have been unfeasible both legally and economically, considering the outdated format and content of the ePD. Repealing it without replacement would leave a potential hole in the data protection framework and reduce the EU's supranational expansion in an area that it has quite firmly under control, and a new piece of legislation – as it happens, the ePR – would either betray the goal of high protection standards by being too industry friendly or antagonize service providers by choking the economy even more than before (and even with the ePR's rather lax provisions in the current version, at least OTT providers will not be happy that they will have to abide by the rules from now on). All the while, The institutions keeping vigil over data protection law in the EU such as the EDPB and the WP29 are quite exigent in their demands for a high level of protection, and will not be pleased with the way the initially stricter rules of the ePR have been watered down during its long and yet unfinished adoption process. As it stands, the ePR might not be well received for these reasons, trying to achieve everything and nothing; The Council will have to make a decision – A strict European fortress of high data protection standards cannot at the same time be a sprawling economic playground for electronic service providers.

2.4. Effects of Privacy Legislation

2.4.1. General Considerations

The economics of privacy have been examined quite closely since the **"first wave"** of data processing, starting in the early 1980s[88]. Early critics of privacy regulation argued that any kind of legal restriction or protection of personal data will lead to inefficiencies in the market. *Posner*, for example, used rather basic arguments and thought experiments to convey this point: A potential employee has every reason to hide certain deficiencies like medical problems from his potential employer, who in turn wants to know as much as possible about the people he seeks to hire. Helping the employee to conceal this information via privacy protection will lead to a suboptimal allocation of employees to employers, as the information asymmetry impedes the

[88] Acquisti,. Taylor, Wagman, *The Economics of Privacy*, Journal of Economic Literature, 2016, p 450

employer's ability to make an informed decision[89]. In a similar vein, *Stigler* concluded that Privacy regulation increases the cost of achieving a given level of information. If a certain data set – e.g. the criminal record of an employee – cannot be obtained directly, the employer has to retrieve the information in a different, more costly fashion, for example by keeping the employee under close surveillance for a certain period. The difference in cost between the suppressed direct method and the workaround must lead to inefficiencies that could have been avoided[90]. Arguments to the contrary can also be made: For example, *Gottlieb* and *Smetters* observed the disclosure of MBA graduates' grades to potential employers, concluding that in some situations, non-disclosure of grades leads to pareto improvements[91].

This research on the economics of privacy is quite extensive, but it is also very general – discussing universal effects on theoretical market situations – or very Anglocentric, given that the Chicago school was a main driver of the field. As the decades passed and technology advanced, the academic focus shifted and dispersed together with the sprawling market. While the first papers considered the collection of data more as conceptual utility cost, there now exists a large market for personal data where data records are directly purchased from data brokers by companies seeking to use the records for customer identification, advertising and price discrimination., The new European Privacy Regime as determined by the GDPR is only two years old (as of 2020), and its **potential economic ramifications** have been contemplated, but not yet empirically studied. Assessments made by the European Commission itself were understandably eager to present the GDPR's effects in the best light possible, while industry stakeholders reported notable problems in the implementations of both the GDPR and the ePD, as was discussed in the previous chapters.

On the scholastic side, most *ex ante* assessments of the GDPR were made in the years from 2012 to 2018, following the predications made by the EU itself in its assessment paper[92]. This assessment followed a similar structure as the assessment of the effects of the ePD (except that it was of course purely prospective, not respective). The literature produced in this period is

---

[89] Richard Posner, *The Economics of Privacy*, The American Economic Review, Vol. 71, No. 2, American Economic Association, 1981, pp. 405-409,

[90] George J. Stigler, *An Introduction to Privacy in Economics and Politics*, The Journal of Legal Studies, Vol. 9, No. 4, The Law and Economics of Privacy, pp. 623-644, The University of Chicago Press, Chicago, 1980

[91] Daniel Gottlieb, Kent Smetters, *Grade Non-Disclosure***,** National Bureau of Economic Research, Cambridge, 2011

[92] European Commission, *Commission Staff Working paper SEC(2012) 72/2 Impact Assessment Accompanying the GDPR*, Brussels, 2012

notably diverse and includes many different approaches to measure the GDPR's economic effects[93]..Each paper or article studied an individual effect that the GDPR might have on a different level of the economy. This augural literature mainly boiled down to two different angles to predict the economic effects of the GDPR and other privacy legislation, namely Macroeconomic effects: (Effect on trade, GDP of European Countries) and effects on the Business Level (One-time cost of implementation and running expenses of compliance, administrative burden including fines issued by authorities, effect on innovation).

Since almost every active business is affected by European data protections laws (especially by the GDPR), it was expected to have noticeable macroeconomic impacts. The European Commission does not mention the possibility of an **impact on the European aggregate gross domestic product**, neither in its *ex ante* assessment from 2012 nor in its first review from 2019. Conversely, the European Centre for International Political Economy (ECIPE), mandated by the U-S- Chamber of commerce, seemed quite eager to find economic downsides of privacy legislation in general and especially the GDPR in studies conducted in 2013 and 2014 [94,95]. These studies assumed different possible scenarios regarding the eventual implementation of the new laws in practice. All of the legal concepts ECIPE found most concerning have eventually been adopted and are being lived in legal practice today. While the first paper from 2013 predicted no effect on GDP, the 2014 paper predicted a "GDP loss" of 0.4 Percent within the EU-28. Similar predictions were made regarding the effect on trade via a reduction of services exported to the union, as the legislation serves as a non-tariff barrier that keeps especially US exporters from offering their services here. While these predictions were substantial in their numbers, any actual effects on these variables can hardly be detected as privacy legislation is entangled with each business in a way that makes it impossible to single out its effect on national accounts. A different approach lies in trying to quantize compliance cost of privacy legislation for individual businesses, as was done in the Deloitte study regarding the efficacy of the ePD (see chapter 2.2). These cost analyses, however, are largely based on very broad assumptions of

[93] Stéphane Ciriani, *The Economic Impact of the European Reform of Data Protection*, Digiworld Economic Journal, no. 97, 2015

[94] Matthias Bauer, Fredrik Erixon, Michal Krol, Hosuk Lee-Makiyama, *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, European Centre for International Political Economy (ECIPE), Brussels, 2013

[95] Bauer, Matthias; Lee-Makiyama, Hosuk; Van der Marel, Erik; Verschelde, Bert, *The costs of data localisation: Friendly fire on economic recovery*, ECIPE Occasional Paper, No. 3/2014, Brussels, 2014

how much a single given obligation might cost based on the average salary of an employee in the EU times the time it takes to implement that obligation[96]. Given the enormous scope of the GDPR (and combining it with the scope of the ePD), these assumption-based calculations would be of little value in determining the true compliance cost of privacy legislation.

But two years after the entry into force of the current framework, **an analysis of the fines** issued by the DPAs around Europe makes it possible to identify not only one dimension of the cost of privacy – which is the amount of Euro paid in fines -, but also to quantitatively asses which provisions have caused the most problems for Controllers, as opposed to the qualitative assessment of the first chapters. What follows is an analysis of the fines issued by all European DPAs per time, country and provisions based on the enforcement tracking dataset maintained by CMS Law Tax.[97]

2.4.2. GDPR Fines

As was discussed in chapter 2.1.4., the work of the DPAs was generally well received by businesses and industry stakeholders. The GDPR penalties were a source of particular dread for companies active in data processing, as they were significantly higher than under the old regime and often heralded as "draconic"[98]. But the authorities were lauded for their cooperative attitude towards Controllers and for making use of all the powers at their disposal without immediately resorting to fines. Nonetheless, over the first 2 years of the GDPR in action, a substantial number of fines has accumulated and reveals some interesting developments in the attitude of DPAs towards administering them. Article 83 GDPR sorts the fines into two tiers of penalty, depending on how sensitive the violated provisions are. Para 4 lists the following Articles:

(a), the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43,

(b), the obligations of the certification body pursuant to Articles 42 and 43;

(c), the obligations of the monitoring body pursuant to Article 41(4)

---

[96] European Commission, Deloitte, *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector: Annexes of the Final Report,* p 18

[97] https://www.enforcementtracker.com/#

[98] Rainer Knyrim, *Die neuen Pflichten nach der EU-Datenschutz-Grundverordnung im Überblick (Teil V),* Dako 2016/6 Heft 1 / 2016, Manz, Austria, 2016, p11

and threatens fines of up to 10 Million € or 2% of the annual worldwide turnover for these violations. Especially literae (b) and (c) are of minor importance and have not caused any procedures involving the violation of the articles mentioned therein. Para 5 leg cit contains the higher second tier penalties of administrative fines up to 20 Million €, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover. This provision in particular is responsible for the vast sums of penalties that had to be paid by some large companies over the course of 2019 (see below). the following provisions are protected by this penalty:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b)the data subjects' rights pursuant to Articles 12 to 22;

(c)the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d)any obligations pursuant to Member State law adopted under Chapter IX;

(e)non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1)

Quite evidently, the provisions mentioned in this paragraph form the heart of the GDPR and are thus protected by higher penalties. What follows is an overview of all procedures where fines where issued sorted by the violated provisions (Table 4):

Tier 1 Penalties (art 83 para 4, up to 10 Million €/ 2% of total annual turnover)	
Type of Provision	**Number of DPA decisions mentioning this Provision**
Art 8 (Consent of Children)	12
Art 28 (Processor/Controller Relationship)	4
Art 29 (Processor/Controller Relationship)	1
Art 31 (Cooperation with the supervisory authority)	7
Art 32 (Security of processing / appropriate technical and organisational measures)	82
Art 33 (Notification of a personal data breach to the supervisory authority)	13
Art 34 (Communication of a personal data breach to the data subject)	5
Art 35 (Data protection impact assessment)	4
Art 36 (Prior consultation with DPA)	1
Art 37 (Designation of the data protection officer)	5
Art 58 (Powers of the DPA)	14
Tier 2 Penalties (Art 83 para 5 up to 20 Million €/ 4% of total annual turnover)	
Art 5 (Principles of Processing)	183
Art 6 (Lawfulness of Processing)	137
Art 7 (Rules on Consent)	7
Art 9 (special categories of personal data / "*Sensitive Data*")	11
Art 12 (Modalities of exercising Data Subjects' rights)	15
Art 13 (Information Obligations)	32
Art 14 (Information Obligations)	14
Art 15 (Right of Access)	26
Art 17 (Right to Erasure)	12
Art 18 (Restriction of processing)	2
Art 21 (Right to Object)	13

Table 4: GDPR Provisions per tier of penalty and Number of DPA procedures mentioning the provision

Note that a single DPA decision usually finds several provisions to be violated, which is why the sum of the right column amounts to more than the total sum of fines issued (which is 344). It is obvious that articles 5 and 6 sport the highest numbers, as they constitute the heart of the GDPR (see chapter 2.1.2.) and every violation of one the obligations can in some way or other be construed a violation of article 5. This betrays a **potential systemic flaw** within the layered system of penalties in article 83. This flaw lies in the combination of violations of article 32 and the underlying principles of processing. Art 32 is a rather general provision, mandating the controller and the processor to implement appropriate technical and organisational measures for the protection of personal data, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data

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

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

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

A violation of this article is normally covered by art 83 para 4 – the lower penalty tier. But a failure of the Controller to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems might just as well be subsumed under a violation of article 5 para 1 lit f (Principle of **Confidentiality and Integrity**). In fact, the Spanish AEPD did just that in a recent decision concerning the reallocation of a user phone number that caused the new holder of the number to be able to access the old former holder's account data[99]. As article 32 is by far the provision with the most violations in the first tier of penalties (82), this lapse in properly layering the penalties artificially potentially might drive up the Euro amounts being paid, which might not be an undesired effect on the part of the EU or the member states, but is certainly problematic form the point of view of the individual business. As any violation of article 32 could potentially involve the principles of processing, the Controllers are less able to profit from the layered system of penalties.

[99] AEPD Decision, PS/00104/2020

Concerning the other violations, articles 5 and 6 naturally count the highest numbers of violations due to being at the heart of the GDPR. Accounting for this, it seems that the provisions mentioned in the stakeholder reports as problematic are also responsible many of the issued fines. Especially in the second, higher tier of article 83 para 5, violations of the information obligations were mentioned 64 times. The right of access, the right to erasure and the right to objection were cited the most of all the Data Subjects' rights, which mirrors the Eurobarometer survey on their frequency of exercise. The right to objection is likely included quite often because of Article 21 para 2, allowing the data subject to object to their data being processed for direct marketing purposes (which can be done in the legitimate interest of the controller, without consent of the Data Subject). This creates an opt-out situation – as opposed to the usual opt-in concept on consent-based processing – where users have to exercise this right quite frequently.

Moving away from the individual provisions, a **time-based analysis** shows the development of the total amount penalties paid per month since the GDPR's entry into force (Figure 1).

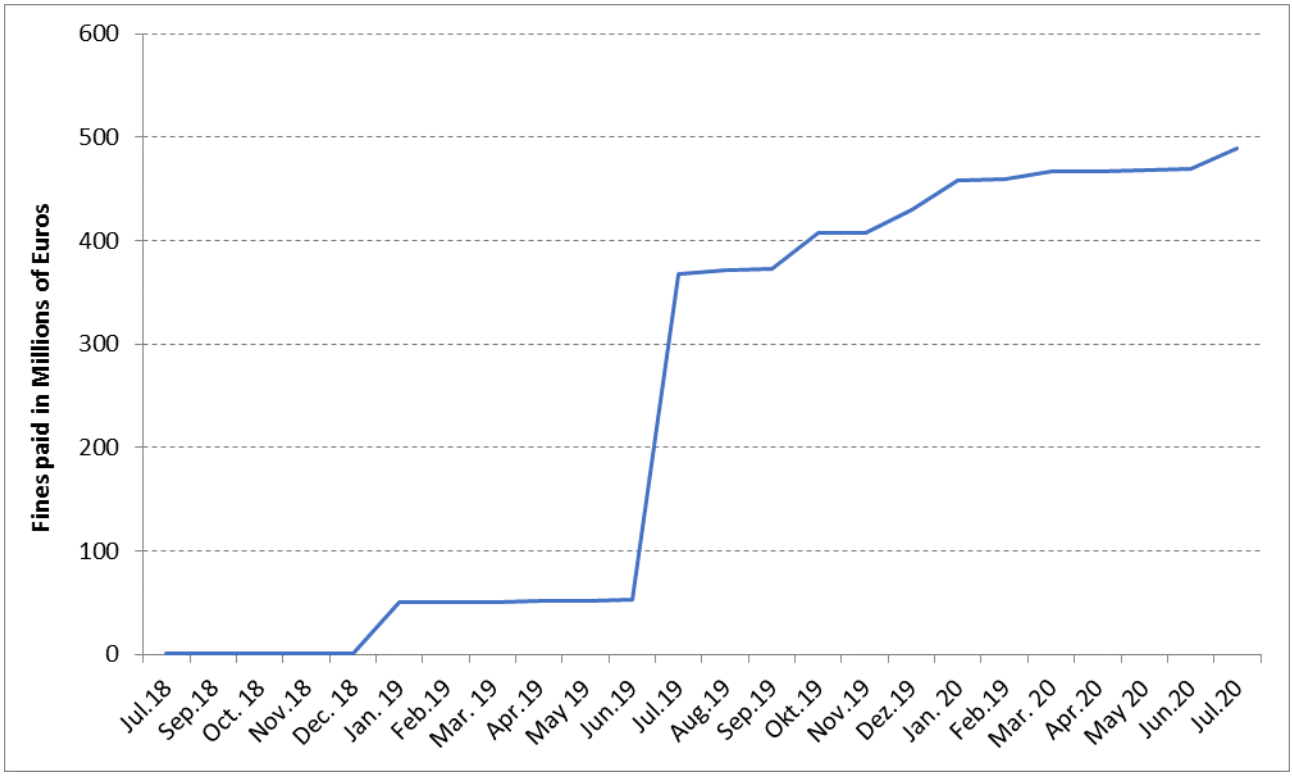

Figure 1: Fines issued in Millions of Euros over time

One notes the initial reluctance of DPAs to make use of the fines, until the Portuguese Comissão Nacional de Protecção de Dados (CNPD) kicked things off by dishing out a rather substantial

fine of 400.000 € to a Public Hospital for violating the principle of data minimization in article 5 para 1 lit c GDPR (and other infringements)[100]. After that, smaller fines accumulated until January 2019, when the French issued fine for *Google* hit like a bombshell and drove the total sum of fines into the tens of millions (see chapter 2.1.4.). The British Information Commissioner followed up in July with the two largest fines issued to date: 110. Million and 204 Million for Mariott International[101] and British airways[102], respectively, for data breaches in each company (These fines are not yet legally binding and have not been paid). After setting this example, the spell seemed broken for most DPAs and the fines started to accumulate gradually until July 2020. The overall picture is of course quite distorted by both the French *Google* case and the two UK-issued fines, but removing them from the overall picture reveals a rather steady increase in the total amount of money paid in fines. Because of the extreme divergence in numbers of the Euro amounts, the number of procedures (Figure 2) per month draws a clearer picture of how the DPAs grew more and more confident in issuing penalties.

[100] Portuguese CNPD, Decision 984/2018

[101] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/, accessed July 5, 2020

[102] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/, accessed July 5, 2020

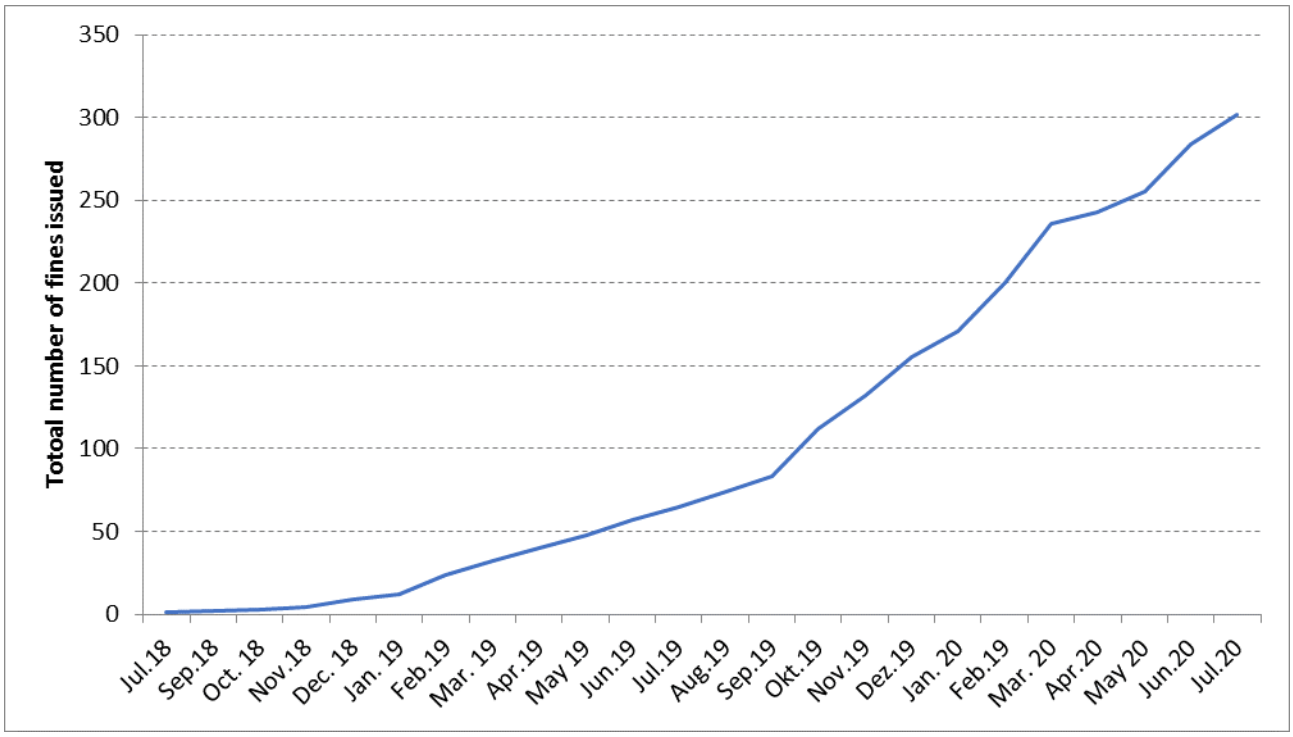

Figure 2: Total number of fines issued over time

A per country analysis shows differing behaviour of national DPAs. Most notable is the fact the UK as the country that has issued the highest amount of Euro to be paid has done so with only 3 procedures involving large players (Mainly British airways, Marriott International), while the country that has issued the highest total number of fines – Spain with 104 procedures – has only amounted to roughly 3 Million Euros worth of penalties. This is the reason why the UK is excluded from Figure 3, as the distortion effect becomes too large otherwise. Accumulated in the "*others*" category are the following countries: Estonia, Malta, Isle of Man, Czech Republic, Iceland Lithuania, Slovenia, Ireland, Cyprus, Belgium, Latvia, Finland, Portugal, Hungary, Romania, Poland and Greece,

which all issued less than a Million Euro worth of fines each. Countries like Hungary and Romania were also quite trigger-happy and issued 26 and 30 penalties, respectively. The second highest total Euro amount was surprisingly paid in Italy, at 56 Million €, mostly based on a penalty of almost 30 Mio € for a telecommunications operator.

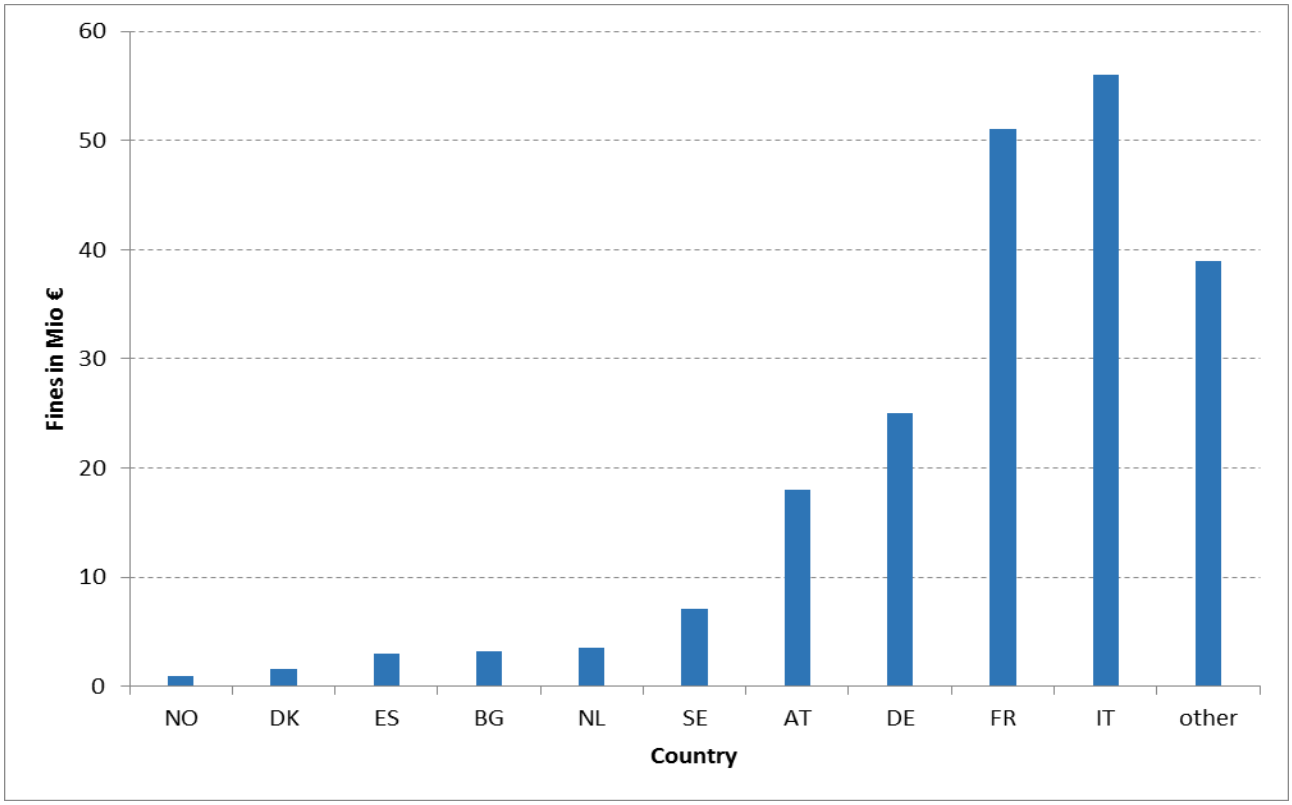

Figure 3: Fines in Millions of Euros per Country

France follows with 51 Million - almost entirely comprised of the *Google* decision – and Germany comes in forth at 26 Million. Austria scored surprisingly high due to the 18 Million € fine that was imposed on the Postal Service for collecting personal data on the political affiliation of Data Subjects [103] (The official document is not yet available as the decision is not yet final, similar to the British cases). **Overall**, the fines amount to roughly half a billion (489 Million) Euros after two years of the GDPR in action. If corrected for the two extreme outliers that are the British fines for Marriott and British Airways, the trend seems to indicate that the fines will become more frequent in number, but not necessarily higher. Considering that well more than half of the total amount consists of only two fines of 314 Million €, the remaining 175 Million Euros seem rather tame. It must be stressed that the GDPR applies to nearly every Business active in the Union, and there are no exceptions made when it comes to the DPAs' power to issue fines. Every Business can be fined for violations of the GDPR, and it lies entirely

[103] https://wien.orf.at/stories/3019396/, accessed July 7, 2020

in the discretion of DPAs how high the penalty should be and whether they want to resort to other means, such as warnings or restrictions of processing until any inadequacies are rectified. Especially compared to other economic sectors such as cartel law, the GDPR fines seem more than moderate: Fines imposed for the violation of EU Cartel law (Art 101 TFEU) within the same two years for which the GDDPR has been in force have amounted to 2,546,068,000 (2,5 Billion) €, with 1,5 Billion coming in in 2019 alone[104]. In the larger context, the fines imposed based on the GDPR have proven strenuous for a very small handful of large companies, but harmless for the economy at large.

[104] European Commission, *Cartel Statistics*, Brussels, 2020

3. Conclusion

Combining the findings of the previous chapters allows for a tentative conclusion of how the GDPR and the e-Privacy Directive have been received, whether the coming e-Privacy Regulation will stick the landing and how European Data Protection law as a whole might develop in the coming years.

The ePD as the main piece of legislation on data protection in the context of **electronic communication** has not aged particularly well in the 18 years since its creation. It has created and uneven playing field for functionally equivalent service providers, not covering services that are mainly based on the exchange of electronic communications due to its outdated provisions, and it imposes rather impactful restrictions on electronic service providers. Due to its nature of a European Directive in need of transformation into national law, its harmonisation issues are abundant. **The ePR**, still caught in the ordinary legislation procedure, aims to rectify some of its predecessor's problems, but might fail in its effort to please the industry stakeholders with quite liberal processing possibilities while at the same time including a much broader array of services in its scope of application. If the new Regulation does not manage to create significant added value to the system of the GDPR, it will be ill-received by businesses and data protection advocates alike.

The GDPR as the largest and most important piece of the puzzle has generally been received more favourably than expected; The stakeholder reports express a genuine understanding for the importance of the issue of Data Protection and a willingness to comply on the part of the industry stakeholders. This willingness to cooperate is somewhat impeded, however, by legislative shortcomings in the system of the GDPR. The initial confusion and overreliance on the legal basis of consent was not necessarily caused by the text of the GDPR itself - or by official EU Communication, for that matter – but rather by the somewhat illusory usefulness of this legal processing basis; the GDPR's information obligations, however, have proven to be strenuous for businesses to implement and overly complicated for consumers to understand because of overregulated transparency requirements and redundant provisions that demanded Controllers to keep and share the same records over and over. When it comes to problems of scaling withing the legislation – i.e., allowing laxer provisions for SMEs or micro enterprises – the GDPR offers

very few remedies. But an extensive layered system different provision for different size classes of Controllers would entirely undermine the policy objectives of the Data Protection framework, which is the reason why an extensive scaling system based on economic capacity is neither advisable nor likely to be implemented. Lastly, it is unfortunate that the GDPR is still haunted by harmonisation issues and national differences because of the numerous opening and implementation clauses it is riddled with. Although the long legislation clearly demanded compromises on the part of the Union, the legislators would have done well to double down on the harmonising force of the Regulation, as this was the strongest economic argument for the GDPR.

These findings were corroborated by the data on the **administrative fines** that have been issued by the DPAs in the first two years of the GDPR's application. The same provisions that the industry stakeholders identified as problematic to implement were the ones that caused much of the penalties. It must be noted, though, that the work of DPAs across Europe has been generally been lauded as cooperative and business friendly, in that DPAs made use of all the powers administered to them by the GDPR without immediately resorting to fines. The overall sum of fines was also not out of the ordinary; In fact, it turned out to be quite tame (except for the two extreme British outliers that are still not finally binding), especially when compared to other pan-European penalties, and when comparing it to the dystopian premonitions that were uttered before the GDPR entered into force. The trend does seem to indicate a steady incline in the total number of fines issued, though, and the following years will tell whether the GDPR fines – which will come into play within the scope of application of the coming e -Privacy Regulation – will become an actual threat to European businesses.

4. List of Abbreviations

Art	Article
e.g.	exempli gratia
ECJ	European Court of Justice
ECR	European Court Reports
edn	edition
EDPB	European Data Protection Board
eds	editors
EP	European Parliament
ePD	E-Privacy Directive
ePR	E-Privacy Regulation
EU	European Union
GDPR	General Data Protection Regulation
Lit	Litera/literae
OJ	Official Journal of the European Union
p/pp	page/pages
para/paras	Paragraph/Paragraphs
SMEs	Small- and medium-sized enterprises
WP29	Article 29 Data Protection Working Party

5. Bibliography

EU Documents

Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, Brussels 2017

Article 29 Data Protection Working Party, *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)*, Brussels, 2017

Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, Brussels, 2007

Article 29 Data Protection Working Party, *Position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*

Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*, Brussels, 2017

Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, Brussels, 2018

Body of European Regulations for Electronic Communications, *Report on OTT services*, BoR (16) 35, 2016

European Commission, *Cartel Statistics, Brussels*, 2020

European Commission, *Commission Staff Working paper SEC(2012) 72/2 Impact Assessment Accompanying the GDPR*, Brussels, 2012

European Commission, *Communication from the Commission to the European Parliament and the Council: Data protection rules as a trust-enabler in the EU and beyond – taking stock*, Brussels, 2019

European Commission, *Digital Economy and Society Index Report 2019*, Brussels, 2019

European Commission, Directorate-General of Communications Networks, Content & Technology, *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*, Brussels, 2015

European Commission, *Special Eurobarometer 359*: *Attitudes on Data Protection and Electronic Identity in the European Union*, Brussels, 2011

European Commission, *Special Eurobarometer 487a: The General Data Protection Regulation*, Brussels, 2019

European Data Protection Board, *First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities*, Brussels, 2019

Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679, *Report – Contribution from the Multistakeholder Expert Group to the Stock-taking exercise of June 2019 on one year of GDPR application,* 2019

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC

The European Data Protection Board, *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*, 2019

Papers, Articles and Reports

Acquisti,. Taylor , Wagman, *The Economics of Privacy*, Journal of Economic Literature (2016)

Alessandro Acquisti, Leslie K. John, and George Loewenstein, *What Is Privacy Worth?*, The Journal of Legal Studies, Vol. 42, No. 2, pp. 249-274, The University of Chicago Press, Chicago, 2013

Bauer, Matthias; Lee-Makiyama, Hosuk; Van der Marel, Erik; Verschelde, Bert, *The costs of data localisation: Friendly fire on economic recovery*, ECIPE Occasional Paper, No. 3/2014, Brussels, 2014

Daniel Gottlieb, Kent Smetters, *Grade Non-Disclosure***,** National Bureau of Economic Research, Cambridge, 2011

Digital Europe, *Two years of GDPR: A report from the digital industry*, Brussels, 2020

Elle Pyle, Laia Bertran Manyé et al, *Decoding GDPR*, Judicature Vol 102 No 1, Bolch Judicial Institute, 2018

Erika McCallister, Tim Grance, Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, National Institute of Standards and Technology, USA, 2010

George J. Stigler, *An Introduction to Privacy in Economics and Politics*, The Journal of Legal Studies, Vol. 9, No. 4, The Law and Economics of Privacy, pp. 623-644, The University of Chicago Press, Chicago, 1980

Giuseppe Contissa, Francesca,Lagioia, Przemyslaw Palka et al, *Claudette Meets GDPR: Automating the Evaluation of Privacy Policies Using Artificial Intelligence*, SSRN Electronic Journal, 2018

Irish Data Protection Commission, *Annual Report*, Ireland, 2019

Joris van Hoboken, Frederik Zuiderveen Borgesius, *Scoping Electronic Communication Privacy Rules: Data, Services and Values*, JIPITEC 198, 2015

Keren Shatkin, *Analyse des Entwurfs der e privacy Verordnung*, Universität Wien, Austria, 2018

Lukas Feiler, *Datenschutz-Grundverordnung ante portas*, jusIT 2016/93, Heft 5

Matthias Bauer, Fredrik Erixon, Michal Krol, Hosuk Lee-Makiyama, *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, European Centre for International Political Economy (ECIPE), Brussels, 2013

Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay, Ignacio Sanchez, *The right to data portability in the GDPR: Towards user-centric interoperability of digital services*, Computer Law & Security Review, 2018

Posner, Richard, *The Economics of Privacy*, The American Economic Review, Vol. 71, No. 2, American Economic Association, 1981

Rainer Knyrim, *Die neuen Pflichten nach der EU-Datenschutz-Grundverordnung im Überblick (Teil V)*, Dako 2016/6 Heft 1 / 2016, Manz, Austria, 2016

Stéphane Ciriani, *The Economic Impact of the European Reform of Data Protection*, Digiworld Economic Journal, no. 97, 2015

Zohar Efroni, Jakob Metzger, Lena Mischau, Marie Schirmbeck, *Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing*, EDPL 3/2019

Books

Ines Härtel, *Handbuch Europäische Rechtsetzung*, Springer, Germany, 2016

Jürgen Kühling, Mario Martini et al, *Die DSGVO und das nationale Recht*, MV-Verlag, Germany, 2016

Lukas Feiler, Nikolaus Forgó, *EU-Datenschutz-Grundverordnung*, Verlag Österreich, Austria, 2017

Rainer Knyrim (edtr), *Der DatKomm. Praxiskommentar zum Datenschutzrecht*, *DSGVO und DSG*., Manz, Austria, 2018

Judicature

Slovenian Information Commissioner, Decision 07121-1/2020/1043,

French Conseil d'État, Decision N° 441065

Austrian DSB, Decision DSB-D123.527/0004-DSB/2018

French CNIL, Decision SAN-2019-001

ECJ case C-193/18

AEPD Decision, PS/00104/2020

Portuguese CNPD, Decision 984/2018

Websites:

European Commission Website, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en, accessed June 12, 2020

EUR-Lex Homepage, https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52017PC0010#2020-03-06_DIS_byCONSIL , accessed May 3, 2020

Germand DPA Website
https://www.bfdi.bund.de/DE/Home/home_node.html, accessed June 12, 2020

French DPA Website
https://www.cnil.fr/, accessed June 12, 2020

Austrian DPA Website
https://www.dsb.gv.at/, accessed June 12, 2020

Google Support Website
https://support.google.com/accounts/answer/3118687?p=privpol_lochistory&hl=en&visit_id=637301124642313647-3530353734&rd=1 accessed June 20, 2020

GDPRHUB Website
https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub, accessed June 25, 2020

Data Transfer Project Website,
https://datatransferproject.dev/, accessed June 25, 2020

Privacy Icons Forum Website,
https://privacyiconsforum.eu/gdpr-data-protection-icons-and-transparency-where-do-we-stand-panel-at-the-cpdp-2020/, accessed June 30, 2020

Letter from press industry stakeholders to the EU
https://www.faz.net/aktuell/eprivacy-verordnung-faz-schickt-offenen-brief-an-die-eu-15037279.html, accessed June 23, 2020

British Information Commissioner Website,
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/, accessed July 5, 2020
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/, accessed July 5, 2020

Austrian News Website,
https://wien.orf.at/stories/3019396/, accessed July 7, 2020

Databases

CMS Law Tax GDPR enforcement Database, https://www.enforcementtracker.com/#