TILBURG LAW SCHOOL

THE IMPACT OF THE GDPR ON THIRD-PARTY CONTRACTS IN THE CLOUD SERVICE INDUSTRY

By

Matthias Gangl

ANR 363124

Dissertation submitted in Partial Fulfillment of the Requirement for the Award of Master of Laws Degree, LLM International Business Law

(6th of June 2019)

Supervisor:

Prof. Dr. Joseph. A. McCahery

ABSTRACT

Organizations are increasingly outsourcing parts or entire business processes to third-party service providers, who collect data as part of their services. In instances where third-party agreements between these parties entail the processing of EU citizens' personal data, EU data privacy laws apply. The contractual relationship between customers *(data controllers)* and service providers *(data processors or data controllers),* subject to EU data privacy laws, constitutes an essential source of mutual data privacy commitments. Under the previous Data Protection Directive 95/46/EC the data controller was solely liable for data privacy compliance, which excluded any statutory obligation of data processors imposed by law. The General Data Protection Regulation (GDPR) introduced direct statutory obligations as well as grave sanctions on data processors, which severely alters the contractual relationship with data controllers.

The purpose of this paper is to analyze the impact of newly introduced obligations under the GDPR on third-party contracts. To address this question we canvassed existing literature about the key considerations which led to the implementation of a new data protection regulation. Existing literature is further used to scrutinize the GDPR's key changes. In addition, we conducted an empirical survey of data processing agreements/addendums from 17 well-known cloud service providers ('CSPs'). This survey allowed for an in depth analysis of contracting practices in the cloud service industry. We compared the survey results with the purposes of the GDPR in order to ascertain whether it supports these bilateral relationship in the context of new and disruptive technologies. Finally, we assessed whether blockchain technology might be a valid alternative to achieve GDPR compliance.

From the literature review and the empirical survey, we found that the GDPR exhibits the following shortcomings: i) It fails to address business-to-business relationships and assumes equal bargaining power among a variety of different parties, which creates increased transaction costs for data controllers; ii) Its contractual requirements are difficult to reconcile with new technologies, such as cloud computing; iii) Neither the GDPR nor the responsible advisory bodies, the Article 29 Working Party or European Data Protection Board (EDPB), provide sufficient guidance on these shortcomings; iv) In order to be compliant with the GDPR, blockchain solutions must abandon its initial purpose, the full decentralization of data silos. This ultimately eliminates the utility of blockchain on a cost/benefit analysis.

The findings suggest the need for more guidance and clarity to resolve uncertainties related to the GDPR's contractual requirements, especially in the case of new emerging technologies.

Keywords: Data Protection, GDPR, Controller, Processor, Compliance, Cloud Services.

DEDICATION

This dissertation is dedicated to my father, Mr. Dieter Gangl and my mother, Ms. Brigitte Gangl. Thank you for enabling me to pursue my goals and support me in every difficult situation.

Also, I would like to dedicate this dissertation to my grandfather, Mr. Erich Zerza, for contributing to a large extent to the person I am today.

ACKNOWLEDGMENTS

Throughout the preparation of this dissertation, I have received a great deal of support and assistance. I would first like to express my sincere appreciation and gratitude to Prof. Dr. Joe A. McCahery whose expertise was invaluable in the formulating of the research topic and methodology. I thank you for all the support and invaluable knowledge you shared with me throughout the preparation of this thesis.

I would like to extend my gratitude to Mr. Diogo Pereira Dias Nunes. Apart from being a great friend and colleague at my internship at Signify Netherlands B.V., his support was crucial in the decision-making process of the research topic.

I thank my fellow student, supporter and, most importantly, friend, Ms. Tima Otu Anwana, whose expertise, emotional support and patience were invaluable in the preparations and completion of this dissertation.

Sincere gratitude to all my family members and especially my sister, Ms. Johanna Gangl, for her love and support. Thank you for being the person I can always rely on irrespective of the circumstances.

I would like to thank Ms. Camille Bernhart for being a great friend and supporting me throughout the entire academic year. Also, I thank my friends Mr. Juan David Perez Marin, Ms. Maria Paula Farías Quintana, Mr. Martin Hren, Mr. Juan Francisco Moreno, and Ms. Maria Jose Ariza for enriching my life since the beginning of the academic year at Tilburg University.

TABLE OF CONTENTS

INDEX

FIGURES

TABLES

APPENDICES

ABBREVIATIONS

BCR	Binding Corporate Rules
CISPE	Cloud Infrastructure Services Providers in Europe
CNIL	Commission Nationale de l'informatique et des Libertés
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
DPA	Data Processing Agreement/ Data Processing Addendum
DPD	EU Data Protection Directive 95/46/EC
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECJ	European Court of Justice
EDPB	European Data Protection Board
EEA	European Economic Area
EU	European Union
FIP	Fair Information Practice
GDPR	General Data Protection Regulation (EU) 2016/679
IaaS	Infrastructure as a Service
ICO	UK Information Commissioner's Office
ISO	International Organization for Standardization
IoT	Internet of Things
NIST	National Institute for Standards and Technology
OECD	Organisation for Economic Co-operation and Development
PaaS	Platform as a Service
RFID	Radio Frequency Identification
SaaS	Software as a Service
SCC	Standard Contractual Clauses
SME	Small and Medium sized Enterprises

CHAPTER ONE: CONTEXT OF STUDY

1.1. Introduction

Third-party agreements between data controllers and data processors[1] constitute one of the main sources of data breach vulnerability.[2] Despite this risk, uncertainties remain about the ideal contractual framework. Third-party contracts are agreements between an organization (*data controller*) and a third-party service provider *(controller or processor)*, which guarantee services, such as information management and data storage. The newly-introduced General Data Protection Regulation (GDPR)[3] applies to these agreements when they cover the processing of EU citizens' personal data. Under the previous Data Protection Directive 95/46/EC[4] (DPD) the data controller was the only party liable for data privacy compliance.[5] In contrast, the GDPR introduced direct statutory obligations as well as grave penalties and fines on data processors.[6] As such, these changes substantially altered the contractual and non-contractual relationship between data controllers and data processors.[7]

Prior to implementation GDPR, researchers examined whether the GDPR would provide sufficient guidance in terms of contracts, accountability and liability in the context of emerging technologies.[8] The focus was on the contractual requirements, such as detailed processing instructions by the controller, highlighted accountability, and assistance requirements of processors, such as the right to conduct audits. This research predicted that the GDPR's provisions would result in a range of

[1] Appendix A provides a non-exhaustive list of terms and definitions, which should provide a necessary tool kit to facilitate the understanding of this paper.

[2] Verizon Enterprise. (2019). 2019 Data Breach Investigations Report. [online] Available at: https://enterprise.verizon.com/resources/reports/dbir/ [Accessed 31 May 2019].

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

[4] 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

[5] See for example DPD Art. 23.

[6] EU GDPR Art. 82. and Art. 83.

[7] Grant, H., Lambert, A. and Pickering, K. (2016). *Data Protection Day—data processors and the GDPR - Fieldfisher*. [online] Fieldfisher.com. Available at: https://www.fieldfisher.com/publications/2016/02/data-protection-day-data-processors-and-the-gdpr#sthash.eCrAKFYy.dpbs [Accessed 19 May 2019].

[8] Lindqvist, J. (2017). New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?. 26th ed. Springer, pp.45–63, Reedsmith.com. (n.d.). *GDPR series: Outsourcing contracts — all changed, changed utterly | Perspectives | Reed Smith LLP*. [online] Available at: https://www.reedsmith.com/en/perspectives/2018/03/gdpr-series-outsourcing-contracts--all-changed-changed-utterly [Accessed 20 Apr. 2019], Pantlin, N., Wiseman, C. and Everett, M. (2018). Supply chain arrangements: The ABC to GDPR compliance —A spotlight on emerging market practice in supplier contracts in light of the GDPR. *Computer Law & Security Review*, [online] 34(4), pp.881-885. Available at: https://www.sciencedirect.com/science/article/pii/S0267364918302516 [Accessed 20 Apr. 2019].

uncertainties, increased compliance burdens and heavy negotiations for the conclusion of processing agreements. Furthermore, scholars believed that further guidance by the Article 29 Working Party[9] would be necessary to support data controller and data processor compliance with the GDPR.

Despite these limitations, the contributions identified two salient concerns regarding the application of the GDPR to contractual relationships in a technology-driven world. First, the GDPR may not provide an equal playing field between data controllers and data processors due to unequal bargaining power. Second, the GDPR may not be technology-neutral, which means that it might be difficult to apply its provisions to new disruptive technologies, such as IoT or cloud computing.

This paper complements the scarce body of existing literature by conducting an in-depth analysis of publicly available data processing agreements/ addendums (DPAs), service agreements and terms of use. While prior studies focused solely on the legal text of GDPR, we scrutinize the implications of the legal text on the contracting practices of companies. This analysis allows us to look beyond scholars' prior predictions and identify whether the GDPR provides an equal playing field for data controllers and data processors in the context of contract negotiations. This paper argues that the GDPR, and especially Article 28, entails a range of ambiguous provisions applicable to their contractual relationship. Moreover, the paper will clarify that if data controllers have a say in contract negotiations, as indicated by the GDPR,[10] then data processors would not be capable of imposing predetermined onerous terms on them.

This paper will analyze the GDPR's ability to accommodate new technologies, looking specifically at contracts in the cloud service industry. Recital 15 of the GDPR states that "in order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used".[11] Prior studies have been conducted regarding GDPR's technological neutrality, in the context of IoT. These studies identified uncertainties about data controllers' and processors' mutual obligations. To illustrate, this paper studies the extent to which the existing literature explains the cloud service industry and assesses the applicability of the GDPR's contractual requirements to new technologies. This will allow us to consider inapplicable provisions

[9] The "Article 29 Working Party" is an advisory body, comprising representatives from the DPA of each EU Member State, the European Data Protection Supervisor and the Commission. Since the GDPR came into force on 25 May 2018, it was replaced by the European Data Protection Board (EDPB).
[10] See for example EU GDPR Art. 28(a).
[11] EU GDPR Recital 15.

of agreements and determine whether the GDPR has adapted to disruptive technologies that may impede the fostering of innovation within the EU.[12] In this context, the paper further answers whether the Article 29 Working Party or the EDPB provide sufficient guidance to support contract negotiations.

Finally, this paper examines whether blockchain technology constitutes a promising alternative approach to achieve GDPR compliance. Based on the analysis of the data protection authorities,[13] the EU Blockchain Forum[14] and a range of scholars,[15] the paper assesses which version of blockchain architecture is best suited to support compliance. While prior research supports the notion of blockchain technology as solution to support data privacy, this paper will examine the usefulness of blockchain solutions based on a cost/benefit analysis. These results will allow us to look beyond the enthusiasm related to blockchain technology and objectively assess its utility under the scope of the GDPR.

1.2. Purpose of the Study and Research Questions

The focus of this paper is to assess the implications of the GDPR's newly introduced obligations to the contractual relationship between data controllers and data processors, especially in the context of cloud services. This study recognizes the rapid pace of technological developments, their legal challenges and the DPD's inability to address them.

Therefore, this paper will answer the following four questions:

1. Does the GDPR provide an equal playing field for data processors and data controllers in the context of contract negotiations?
2. Is the GDPR capable of accommodating technological innovation?

[12] Under Article 173 TFEU the EU and Member state must "foster better exploitation of the industrial potential of policies of innovation, research and technological development," and the EU's "Innovation Union" initiative aims to "remove obstacles to innovation" by 2020, Available at: https://ec.europa.eu/info/research-and-innovation/strategy/goals-research-and-innovation-policy/innovation-union_en [Accessed 29 May 2019]

[13] Cnil.fr. (2018). *Solutions for a responsible use of the blockchain in the context of personal data*. [online] Available at: https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf [Accessed 20 May 2019].

[14] Eublockchainforum.eu. (2018). *Blockchain and the GDPR*. [online] Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf [Accessed 20 May 2019].

[15] Ibáñez, L., O'Hara, K. and Simperl, E. (2018). On Blockchains and the General Data Protection Regulation. [online] Eprints.soton.ac.uk. Available at: https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf [Accessed 21 May 2019], describes the technique, using hashes as proof of existing data, as "hashing out", Enigma.co. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. [online] Available at: https://enigma.co/ZNP15.pdf [Accessed 20 May 2019], Finck, M. (2017). *Blockchains and Data Protection in the European Union*. [online] SSRN. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3080322 [Accessed 16 May 2019].

3. Do the GDPR and advisory bodies, such as the WP29 or EDPB, provide helpful guidance on this matter?
4. Can blockchain technology serve as a valid alternative solution to achieve GDPR compliance?

1.3. Methodology and Limitations

This paper will outline the fundamental objectives of the GDPR as compared with the DPD. Using a literature review, this paper will focus on the evolution of the GDPR, focusing on the contractual relationship between data controllers and data processors, and the effects of the potential uncertainties.

Subsequently, this paper seeks to apply the findings to the service agreements in the cloud service industry. To this end, we focus on the contractual framework between CSPs (data processors) and their customers (data controllers). Next, this paper will present the results of an empirical survey of publicly available DPAs, service agreements and terms of use of 17 selected CSPs.[16] The results will help us understand the common contracting practices of CSPs and identify implications relevant to customers. Finally, this paper will canvass existing literature to identify alternative solutions, focusing on blockchain technology. This paper then explores the possibilities of blockchain technology as a solution to existing ambiguities regarding GDPR compliance.

Having identified the objectives of this paper, we consider some of the limitations to the conduct of the study. This paper acknowledges that contracts between customers (data controllers) and CSPs (data processors) will frequently be negotiated on a case-by-case basis in practice. The analysis of the contractual framework between these parties will be limited to the publicly available agreements. Notwithstanding the limitations, this paper will provide a range of insights and analyses of CSPs common practice regarding data protection and their collaboration with customers.

The subsequent chapters are organized as follows: Chapter II provides a comprehensive analysis of the GDPR, its preceding considerations and its main implications on third-party contracts. Chapter III will analyze how CSPs address these implications in their contracts with customers. In Chapter IV we assess if blockchain technology constitutes a valid alternative to achieve GDPR compliance, and in Chapter V we conclude the paper.

[16] See Appendix D.

CHAPTER TWO: GDPR ANALYSIS

2.1. Introduction

The GDPR is a highly complex regulation, which relies on the same underlying fundamental data protection principles as the DPD. The seven key principles are the collection limitation, data quality, purpose specification, use limitation, security safeguards, transparency, individual participation and accountability principle. These principles were derived from the OECD's "recommendations concerning and guidelines governing the protection of privacy and transborder flows of personal data".[17] This chapter will provide background information about the development of data protection laws in the EU, which culminated in the implementation of the contemporary approach; i.e. the GDPR. Further, this chapter will examine the impact of the changes, introduced by the GDPR, to the contractual relationship between organizations and their service providers.

EU data protection laws predominantly grant data subjects[18] the right to transparency and the right to request access, correction or the erasure of personal data.[19] The purpose of data protection laws is to protect data subjects from organizations using and transferring their personal data without any restrictions. It is well known that organizations are responsible for the collection and usage of data at first hand are data controllers.[20] Data processor, on the other hand "process personal data on behalf of the data controller". However, the identification of a data controller or data processor, has become increasingly difficult over time especially in complex commercial scenarios involving novel technologies. The Article 29 Working Party states that "being a controller is primarily the consequence of the factual circumstance that an entity has chosen to process personal data for its purposes".[21] The application of this clarification may cause problems in the context of new technologies. Service providers, might still be able to determine the "purpose and means" of processing personal data by

[17] OECD recommendations of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data. (1980). Available at: https://www.kantei.go.jp/jp/it/privacy/houseika/dai11/11siryou5.html [Accessed 17 Apr. 2019]

[18] Appendix A provides a non-exhaustive list of terms and definitions, which should provide a necessary tool kit to facilitate the understanding of this paper.

[19] Mahieu, R., van Hoboken, J. and Asghari, H. (2019). Responsibility for Data Protection in a Networked World – On the Question of the Controller, 'Effective and Complete Protection' and Its Application to Data Access Rights in Europe. [online] SSRN. Available at: https://dx.doi.org/10.2139/ssrn.3256743 [Accessed 6 Mar. 2019].

[20]Ico.org.uk. (2018). Some basic concepts. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/ [Accessed 6 Mar. 2019].

[21] Article 29 Data Protection Working Party, "Opinion 1/2010 on the concepts of 'controller' and 'processor'" (WP 169), adopted on 16 February 2010, at 8.

determining the technical and organizational details.[22] In this case, the service provider might qualify as a data controller, which results in an elevated set of obligations.[23]

The definitions of controller and processor under the GDPR have remained mostly the same, but it imposed new legal obligations and the responsibility for personal data breaches on both parties.[24] Therefore, the clarification of the rights and obligations of an organization and its service providers remains both a crucial and challenging task. The outsourcing business processes of these organizations to service providers requires an explicit allocation of responsibilities in their contractual relationship to comply with the GDPR and clarify accountability for personal data breaches. Figure 2.1[25] outlines a simplified scenario of an organization, outsourcing services via a CSP under the constant supervision of the national supervisory authority. The illustration of potential data flow shows that the contractual agreement between data controllers and processors (or a joint controller) requires an adequate degree of responsibility allocation.

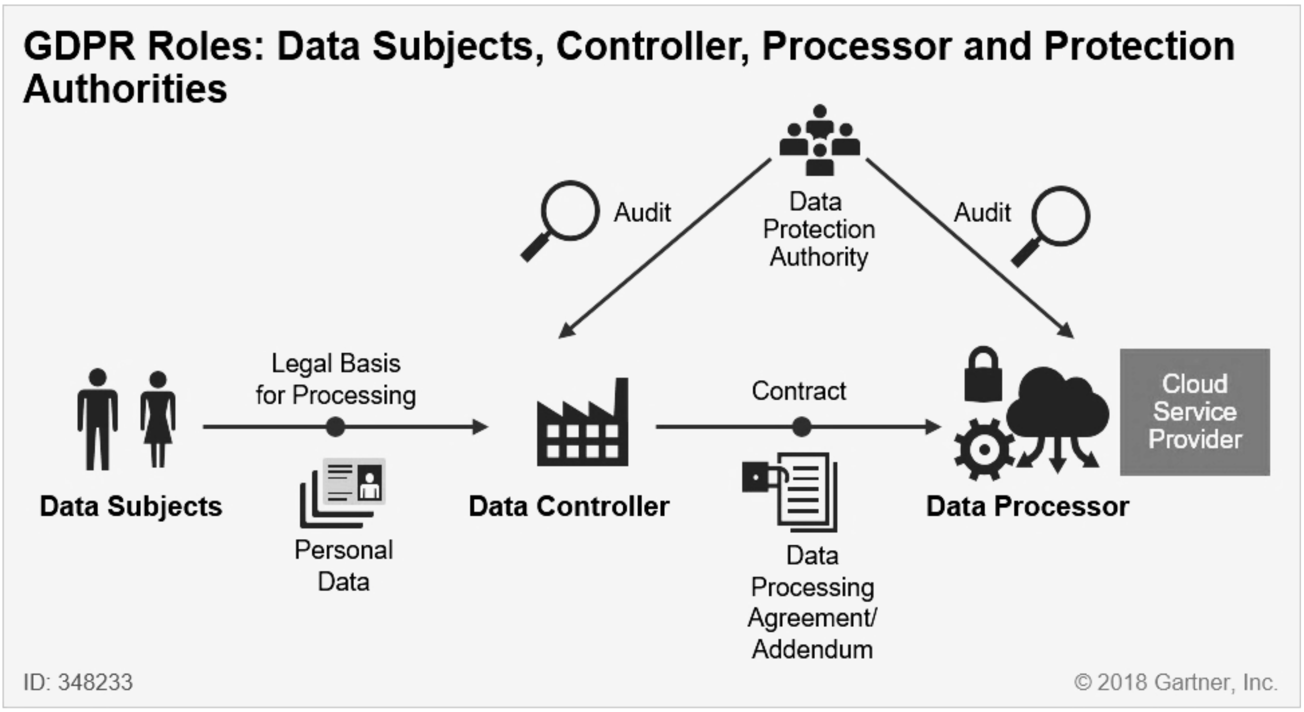
[22] Hintze, M. (2018). Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR. [online] SSRN. Available at: https://ssrn.com/abstract=3192721 [Accessed 19 Apr. 2019].

[23] See Chapter 2.4.6.

[24] See Appendix B.

[25] Figure 2.1 shows the relationship between data subjects, an organization acting as data controllers, cloud service providers acting as data processors and supervisory authorities monitoring the data security. The relationship between data subjects and data controllers grants data privacy rights to data subjects and imposes legal obligations on data controllers to store, process and transfer the personal data adequately. A data controller, which outsources cloud services, must enter into a data processing agreement with the data processor, which allocates obligations and accountability in the event of data breaches for instance. The supervisory authority of the responsible Member State monitors both the relationship of data subjects with data controllers and data controllers with data processors.

Figure 2.1 GDPR roles


GDPR Roles: Data Subjects, Controller, Processor and Protection Authorities
Data Protection Authority
Audit
Audit
Legal Basis for Processing
Contract
Data Subjects
Personal Data
Data Controller
Data Processing Agreement/ Addendum
Data Processor
Cloud Service Provider
ID: 348233
© 2018 Gartner, Inc.

Source: Gartner (2018), Stop Agonizing Over GDPR Opt-In Emails and Start Thinking about How Your Use of Cloud Impacts GDPR Compliance, https://blogs.gartner.com/richard-watson/stop-agonising-gdrp-opt-emails-start-thinking-cloud-providers/

In this chapter, Section 2.2 will outline the transformation of EU data protection laws culminating in the implementation of the GDPR. Section 2.3 will explain the key considerations and procedure preceding the GDPR. Section 2.4 will list the key changes applicable to contractual relationships between service providers (data processors) with private or public entities (data controllers) and Section 2.5 will examine the impacts on these third party contracts.

2.2. Background

In contrast to US law,[26] which characterizes 'privacy' or 'information privacy' predominantly as one unified concept, the European Union has separated the right of respect for private and family life[27]

[26] US data privacy laws intend to protect the private life of individuals in general, and do not consider data protection as separate right. However, many ideas of the GDPR can be found in US privacy laws and FTC case law; e.g. communications laws cover the storage, use and sale of user data, credit rating provider have to provide data subject access, the videotape privacy protection act imposes deletion obligations. U.S. privacy laws, which are fragmented into federal and state laws, might lack a unified overarching data privacy legislation, such as the GDPR, and regulate specific sectors and types of information; e.g. financial and health. Critics argue that this patchwork approach causes an insufficient set of data protection rights for individuals.

[27] The Charter of Fundamental Rights of the European Union includes a separate "Article 7 – Respect for private and family life: Everyone has the right to respect for his or her private and family life, home and communications."

from the right of data protection.[28] The latter refers to fair and diligent usage of personal data,[29] indicating the specific focus on the protection of personal data within the EU. By establishing a separate fundamental right of data protection, the expectations of privacy in the EU are considered to be extremely high; arguably higher than in the U.S..[30]

The legislative development towards increased data protection originated when the EU used and expanded the scope of the *Fair Information Practices (FIPs)*,[31] established by the US in the 1970s. The FPIs focused primarily on data protection in 'vertical relationships' between the government and citizens,[32] and secondarily on the credit reporting sector.[33] The EU extended the application to 'horizontal relationships' between businesses and citizens in general, which can be seen as a key element of the European approach towards data protection. This approach enshrines that every data subject shall be entitled to privacy as fundamental right.[34]

Due to the increasing fragmentation between Member States national data protection laws in 1990, which posed a threat to the internal market, the EU Commission proposed a Data Protection Directive.[35] As a result, the DPD was adopted in 1995 and had to be implemented by each Member States within three years from the date of its adoption. The objective of the DPD was to harmonize the national data protection laws of EU Member States in order to create increased protection for data subjects and free data flows throughout the EU, however the application of the DPD exposed some weaknesses, as outlined in Table 2.1. The DPD had to be implemented into national law and hence provided some latitude for national regulators thus hindering the creation of the desired harmonization of national data protection laws. For example, Member States took part in a regulatory competition

[28] The right of Protection of personal data under the Charter of Fundamental Rights of the European Union Article 8 - since the ratification of the first version of the Charta of Fundamental Rights on 7 December 2000, Most Member States' constitutions also provide data privacy protection. See on the protection of national constitutions: Koops, B., Newell, B., Timan, T., Škorvánek, I., Chokrevski, T. and Galič, M. (2019). *A Typology of Privacy*. [online] Penn Law: Legal Scholarship Repository. Available at: https://scholarship.law.upenn.edu/jil/vol38/iss2/4 [Accessed 16 Apr. 2019]

[29] González Fuster, G. (2014). Emergence of personal data protection as a fundamental right of the EU. Springer.

[30] Lee, P. (2019). *How do EU and US privacy regimes compare? - Privacy, Security and Information Law Fieldfisher*. [online] Privacylawblog.fieldfisher.com. Available at: https://privacylawblog.fieldfisher.com/2014/how-do-eu-and-us-privacy-regimes-compare [Accessed 16 Apr. 2019]

[31] See Gellman, R. (2019). *Fair Information Practices: A Basic History*. [online] SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020 [Accessed 16 Apr. 2019].

[32] Privacy Act of 1974 5 USC 552a.

[33] Fair Credit Reporting Act of 1970 15 USC §1681.

[34] Fn. 40 explained that there is no overall expectation of privacy in the U.S. and that the entitlement of individuals to privacy depends on the sector and type of information, which is caused by a fragmentation into federal and state laws

[35] Commission of the European Communities on the protection of Individuals In relation to the processing of personal data In the Community and Information security, COM 90 (314) final (September 1990).

and opportunistic behavior creating so-called data protection 'loopholes',[36] which enabled forum shopping; i.e. businesses establishing themselves in the Member State with the most favorable data protection legislation.[37] The data protection loopholes aimed to abuse the discretion in implementing the DPD and, combined with other legislative benefits,[38] to attract big tech companies. Moreover, the enforcement of the DPD did not pose a major threat, imposing marginal fines. Big tech companies appeared unimpressed facing small penalties, such as Facebook's fine of about 150.000 Euro in 2017.[39] The imposition of this fine created an external image of the EU as a rule-bound watchdog, lacking necessary enforcement tools.[40]

Finally, the rapid development of novel technologies and business structures has potentially created the most significant challenge for the European regulators.[41] The amount of data publicly provided by individuals consciously and unconsciously expanded and as a result private and public authorities processed an increased scale of data conducting their activities. Thus, the rapid pace of digitization and globalization impaired the DPD's capability to provide proper data protection within the EU.

Prior research[42] has identified six key weaknesses of the DPD.[43] First, the DPD was accused of providing an ambiguous concept of personal data, which excluded considerations of potential harm for the data subject. This means that not all acts of personal data usage, subject to the DPD, could

[36] Albrecht, J. (2019). EUDataP: State of the Union. [online] Media.ccc.de. Available at: https://media.ccc.de/v/30C3_-_5601_-_en_-_saal_2_-_201312281400_-_eudatap_state_of_the_union_-_jan_philipp_albrecht#t=315 [Accessed 17 Apr. 2019].

[37] Article 4 Directive 95/46/EC determines that the 'establishment' of the data controller is decisive for the applicable national data protection law, even if it collects personal data from individuals of other Member States.

[38] Businesses chooses their location of establishment on more than one legal factor; e.g. the local labor laws and tax regime.

[39] Cnil.fr. (2017). FACEBOOK sanctioned for several breaches of the French Data Protection Act | CNIL. [online] Available at: https://www.cnil.fr/en/facebook-sanctioned-several-breaches-french-data-protection-act [Accessed 18 Apr. 2019].

[40] Hoofnagle, C., van der Sloot, B. and Zuiderveen Borgesius, F. (2019). *The European Union General Data Protection Regulation: What It Is And What It Means*. [online] SSRN, p. 71. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3254511 [Accessed 17 Apr. 2019].

[41] Commission Staff Working Paper, Executive summary of the impact assessment, SEC (2012) 73 Final (January 2012) at 1.

[42] Robinson, N., Graux, H., Botterman, M. and Valeri, L. (2019). *Review of the European Data Protection Directive*. [online] RAND Europe, pp.26-37. Available at: https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf [Accessed 17 Apr. 2019].

[43] See Table 2.1

cause an impact on privacy. This left open the question of whether EU data privacy laws should take the criterion of potential harm into account.[44]

Second, Article 18 of the DPD included the obligation on data controllers to notify the national supervisory authority before conducting a specific act of data processing. An exception to Article 18 existed where "the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations".[45] This notification obligation intended to establish transparency for data subjects and supervisory authorities and create awareness of the responsible data controllers. However, different implementations of the Member States caused an array of different notification obligations and exemptions, which rendered the intentions of the DPD ineffective. This could be considered as a prime example of the lack of harmonization between national data protection laws within the EU.

Third, the DPD adopted a narrowed scope of territorial applicability, which did not impose liabilities on businesses, incorporated outside the territory of an EU Member State but processed data of EU citizens.[46]

Fourth, the DPD rendered data transfers to 'third countries' cumbersome by requiring an 'adequate' level of data protection in this country[47] or Standard Contractual Clauses (SCCs)[48] or Binding Corporate Rules (BCRs).[49] A survey conducted by the ICO[50] indicated that the majority of interviewees agreed that the adequacy test was too stringent, because it only acknowledged the jurisdiction of the third countries as being adequate, if it followed the DPD strictly. SCCs seemed more promising in terms of efficiency, but the approval of these clauses varied depending on the Member State. In addition, the DPD lacked a clear framework for facilitating the approval of BCRs.

[44] Robinson, N., Graux, H., Botterman, M. and Valeri, L. (2019). *Review of the European Data Protection Directive*. [online] RAND Europe, pp.26-37. Available at: https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf [Accessed 17 Apr. 2019].
[45] DPD Art. 18.
[46] DPD Art. 4.
[47] DPD Art. 25(6) sets out that the EU Commission can adopt an adequacy decision allowing the data transfer to a third country
[48] Under DPD Art. 26(4), the EU Commission can decide, which standard contractual clauses provide for appropriate safeguard to ensure compliance with the DPD.
[49] BCRs are not codified in the DPD but were developed by the Article 29 Working Party. BCRs are internal rules within an international organization, which allow the organization to transfer personal data to third countries within the same organization.
[50] Robinson, N., Graux, H., Botterman, M. and Valeri, L. (2009). Review of the European Data Protection Directive. [online] RAND Europe, p.33. Available at: https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf [Accessed 17 Apr. 2019].

Fifth the DPD's definitions of a controller[51] and processor[52] were not flexible enough to provide clarity about which definition applies to companies in an increasingly modern economy.

Sixth, the DPD lacked the ability to enforce its provisions adequately and hold controllers accountable. Although data subjects had the right to remedies,[53] a data breach may not cause immediate damages, the damages are difficult to quantify and individual damages are mostly too minor. In addition, the Member States applied uneven and non-transparent standards of enforcement and accountability.

Table 2.1 EU Data Protection Directive's Weaknesses and Explanation

EU Data Protection Directive weaknesses	
Unclear relation of personal data with the risk of harm	The scope of personal data solely focused on the definition of 'personal' data, without considering potential harm.[54]
Inefficient notification obligations	Due to different implementations of the Directive, there were 20 different notification and registration procedures combined with a variety of exemptions.[55]
Territorial applicability	The concept of an establishment was narrowed to the territory one of the Member States where the controller established its business. Companies domiciled outside the EU but processing EU citizens' data were not subject to the DPD.[56]
Transfer of data to third countries were cumbersome	The use of adequacy decisions seemed outmoded considering business realities.

[51] DPD Art. 2(d).

[52] DPD Art. 2(e).

[53] DPD Art. 22.

[54] Sweden's implementation of the EU Data Protection Directive separates unstructured data and structured data, which is deliberately gathered to facilitate searches or compilation for data. Whereas the former does not constitute personal data pursuant ot the EU Data Protection Directive, the latter can cause data breaches only if it would involve improper intrusion on privacy. https://ec.europa.eu/justice/article-29/documentation/annual-report/files/2007/10th_annual_report_en.pdf [Accessed 6 March 2019].

[55] Robinson, N., Graux, H., Botterman, M. and Valeri, L. (2009). Review of the European Data Protection Directive. [online] RAND Europe, pp.31-32. Available at: https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf [Accessed 17 Apr. 2019].

[56] de Hert, P. and Czerniawski, M. (2016). Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. [online] Oxford Academic, pp. 230-243. Available at: https://academic.oup.com/idpl/article/6/3/230/2447252 [Accessed 17 Apr. 2019].

	The authorization of Standard Contractual clauses and Binding Corporate Rules entailed excessive approval procedures on a national level.[57]
The definition of parties involved in storing, processing and transferring data as part of their activities	Unclear definition when companies act as a processor or controller especially in an online environment.[58]
Accountability and enforcement standards were inconsistent	Unclear allocation of responsibilities due to mostly intangible damages and uneven criteria of enforcement.[59]

Source: Review of the European Data Protection Directive, Available at: https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf

The implication is that the DPD, which aimed to establish awareness of data privacy issues and the key principles of adequate data protection practice,[60] failed to provide processes that were capable of translating these aims into reality. As shown in Table 2.1, the DPD's inefficiency was caused by the fragmentation of national data protection laws of the EU Member States, and the fact that some of its provisions were outdated in an increasingly globalized world. Although the critical principles of the DPD were solid and sound, its rigid approach could not keep up with the dynamic development of globally acting companies anymore.

The range of weaknesses of the DPD, which were outlined in this chapter, could best be addressed by a contemporary legal framework. As we shall examine in the upcoming sections, these weaknesses were provisionally addressed through the GDPR. [61]

2.3. Considerations and Procedures preceding GDPR Implementation

In this section, the considerations, legislative process and implementation procedure preceding the GDPR shall be addressed. The EU Commission implemented a number of steps whereby it conducted

[57] Robinson, N., Graux, H., Botterman, M. and Valeri, L. (2009). Review of the European Data Protection Directive. [online] RAND Europe, pp.33-35. Available at: https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf [Accessed 17 Apr. 2019].
[58] Ibid p. 36.
[59] Ibid pp. 35-36.
[60] See fn. 31.
[61] See Chapter 2.4.

a substantive analysis and consulted the significantly affected stakeholders.[62] The Commission published a proposal text in 2012,[63] and the subsequent trilogue meetings[64] with the Council[65] and the EU Parliament[66] resulted in the official adoption of the GDPR in May 2016. After a two year transition period with no alterations the GDPR took effect in May 2018.[67]

The EU Commission pursued two main purposes in proposing a novel EU data protection legislation. Firstly, the reimplementation of the DPD's dual goal of protecting EU citizens' personal data and supporting the free flow of data in the internal market. Secondly, the adjustment of the DPD to the technological developments and the scale of data controlled and processed by private and public entities.

The three EU legislative bodies attempted to address the apparent weaknesses of the DPD, mentioned under section 2.2, by creating a regulation, which sought to comply with contemporary technological standards and impose rights directly onto EU citizens. The DPD set a minimum standard of data protection laws for national legislators, but the variety of different national implementations of the DPD caused increasing confusion especially of organizations involved in cross border trading.[68] The question of the applicable law often remained unclear, which posed an unsatisfying solution, considering the growing complexity of data privacy. EU legislative bodies concluded that a regulation, which prevailed over national data protection law and applied directly in each Member State, might pose the most suitable solution. No single government could modify its national data protection law in

[62] From 9 July to 31 December 2009, the Consultation on the legal framework for the fundamental right to the protection of personal data. The Commission received 168 responses, 127 from individuals, business organizations and associations and 12 from public authorities, Available at: http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm. [Accessed 27 March 2019]
From 4 November 2010 to 15 January 2011, the Consultation on the Commission's comprehensive approach on personal data protection in the European Union. The Commission received 305 responses, of which 54 from citizens, 31 from public authorities and 220 from private organizations, in particular business associations and nongovernmental organizations, Available at:
http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm. [Accessed 27 March 2019]

[63] Commission Proposal for a 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 (General Data Protection Regulation), COM(2012) 11 final (January 2012).

[64] Trilogue meetings are informal meeting of representatives of the Council, Parliament and Commission, which may be scheduled at any time of the EU legislative procedure.

[65] The Council of the EU represents the national governments of the 28 EU Member States. The votes of each representative are weighed in accordance with the population of the represented EU Member State;

[66] The EU Parliament, which constitutes the only parliamentary elected body of the EU, has legislative power without the ability to propose new legislation;

[67] GDPR Art. 99(2): "It shall be effective from 25 May 2018".

[68] EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide - Second Edition. (2017). IT Governance Ltd., pp.18-21.

order to facilitate compliance with the GDPR because the representatives of each EU Member State had already participated in the voting of the Council of the EU. The change of the legal character of EU data protection laws, from a directive to a regulation, hence attempted to address the lack of harmonization between differing national data protection laws of EU Member States.

In addition to the harmonization of data protection laws within EU Member States, the GDPR, which included several changes to the former DPD, had an impact on both data controllers and data processors. In the subsequent two sections we examine the fundamental changes compared with the DPD and their impact on third-party contracts between organizations and their deployed service providers.

2.4. Key Changes of the GDPR

The GDPR attempted to create a legislative act, based on the fundamental principles of the DPD, which was suitable to the rapid technological developments. The GDPR resembled the DPD's dual goal to protect EU citizens' right to the protection of personal data as well as to enhance free data flow within the internal market. In other words, the GDPR attempted to strengthen EU residents' data privacy rights by imposing specific restrictions on organizations controlling, storing and processing personal data. The GDPR, however tends to prioritize the preservation and extension of individuals' right to data protection[69] and simultaneously imposes an increased burden of compliance on both data controllers and processors. This means that the GDPR may impede the business of organizations using and storing personal data as a data controller or data processor. Table 2.2 outlines the weaknesses of the DPD and shows the relevant changes of the GDPR, which have an impact on third-party contracts. These changes, while not leading to new definitions of the data controller and processor, imposed a new set of obligations on the parties to comply with the GDPR.

Table 2.2 GDPR changes

EU Data Protection Directive weaknesses	GDPR changes
Unclear relation of personal data with the risk of harm	Extended personal data scope created a 'capture-all' application.[70]

[69] TFEU Art. 16.

[70] DLA Piper. (n.d.). EU General Data Protection Regulation - Key changes | DLA Piper Global Law Firm. [online] Available at: https://www.dlapiper.com/en/netherlands/focus/eu-data-protection-regulation/key-changes [Accessed 19 Apr. 2019].

Inefficient notification obligations	Mandatory notification by data controller and provision of certain information to the data protection authority, other data controllers and sometimes data subjects within 72 hours.[71]
Territorial applicability	Extension of the territorial scope, imposing liability on companies processing data outside the EU.[72]
Transfer of data to third countries were cumbersome	Adequacy decisions, appropriate safeguards, SCCs or BCRs, codes of conduct and certification mechanisms.[73]
The definition of parties involved in storing, processing and transferring data as part of their activities	Same definitions but new obligations imposed on data controllers and processors.[74]
Accountability and enforcement standards were inconsistent	Obligation to demonstrate compliance with the GDPR.[75] Changes strengthening the enforcement of the GDPR.[76]

Taken together, the changes of the GDPR point in the direction of an increased protection of data subjects' rights at the expense of data controllers and processors, which carry burden of compliance with new and more complex provisions.[77]

2.4.1. Extended Scope of Personal Data

As we noted earlier,[78] the DPD's concept of personal data excluded considerations of potential harm for the data subject. The GDPR does not address this issue and even broadened the scope of application

[71] Hoofnagle, p. 73.

[72] Hintze, M. (2018). Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR. [online] SSRN, p. 12. Available at: https://ssrn.com/abstract=3192721 [Accessed 19 Apr. 2019], Hoofnagle, p. 85, Rubinstein, I. and Petkova, B. (2018). *The International Impact of the General Data Protection Regulation*. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3167389 [Accessed 19 Apr. 2019].

[73] Hintze, pp. 9-10, Hoofnagle, pp. 83-85.

[74] Hintze, p. 4, Hoofnagle, p. 85.

[75] Hoofnagle, p. 73, Hintze, p. 16.

[76] Hoofnagle, pp. 92-97, Hintze, p. 2.

[77] The GDPR includes 99 detailed provisions and 173 recitals. The DPD included 34 provisions and 72 recitals.

[78] See Chapter 2.2.

by combining existing definitions of the DPD with case law of the ECJ[79] on that matter.[80] The GDPR applies to "any information relating to an identified or identifiable natural person ('data subject')".[81] The classification as an 'identifiable' data subject requires a shallow level of data transmitted to data controllers since "all the means reasonably likely to be used"[82] shall be taken into account. This means that data might be personal data even if an organization cannot identify a data subject based solely on this data. Data, qualifying as 'identifier', go beyond the name of a data subject and can also be public non-sensitive data, ID numbers, pseudonymous identifiers,[83] location data and online identifier. Recital 30 of the GDPR lists potential online identifiers, such as IP addresses, cookies and radio frequency identification (RFID) tags.[84]

In summary, a company arguably processes "personal data" under the new definition of the GDPR whenever it touches data relating to an individual, irrespective of the classification as public or non-public, directly or indirectly identifying a data subject and sensitive or non-sensitive.[85] The expansion of the regulatory perimeter of personal data imposes a much higher burden of compliance on data controllers as well as data processors, requiring them to consider appropriate compliance solutions.

There are thought to be a number of competing solutions, which should always be based on the following considerations. First, organizations should attempt to eliminate and avoid unnecessary personal data or render it anonymous. This means that the information "does not relate to an identified or identifiable natural person".[86] Second, if the usage of personal data is indispensable, organizations might use pseudonymization.[87] The use of pseudonymization does not exclude the data from the

[79] *Breyer v. Bundesrepublik Deutschland* , Case C-582/14, for example clarified that Internet protocol addresses constitute personal data.

[80] DLA Piper. (n.d.). EU General Data Protection Regulation - Key changes | DLA Piper Global Law Firm. [online] Available at: https://www.dlapiper.com/en/netherlands/focus/eu-data-protection-regulation/key-changes [Accessed 19 Apr. 2019].

[81] See Appendix A.

[82] EU GDPR Recital 26.

[83] Ibid.

[84] EU GDPR Recital 30: "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."

[85] Hoofnagle, C., van der Sloot, B. and Zuiderveen Borgesius, F. (2019). *The European Union General Data Protection Regulation: What It Is And What It Means*. [online] SSRN. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3254511 [Accessed 17 Apr. 2019].

[86] EU GDPR Recital 26

[87] EU GDPR Art 4(5), pseudonymization means "that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

GDPR's scope, but it may be useful to mitigate the risk of data breaches and reduce the likelihood of potential harm to data subjects in the event of a data breach. Data controllers and data processors should, therefore, use personal data solely if anonymization or pseudonymization would be insufficient for the specific purpose of data processing.

Overall the solutions discussed above amount to an attempt to minimize the exposure of data controllers and data processors. The GDPR's elevated bar of compliance, however, is likely to induce data controllers and processors to assume that every data they process is personal given the broadened scope of personal data. Under these circumstances, data controllers and processor are well-advised to avoid processing data whenever it is feasible or to implement adequate compliance procedures.

2.4.2. EU-wide Notification Obligation

This section focuses on the collaboration of data controllers and processors in the event of a data breach.[88] The GDPR obliges data controllers under Article 33(1) to notify data breaches to the responsible supervisory authority "without undue delay (…) within 72 hours after having become aware of it". The data breach has to result "in a risk to the rights and freedoms of natural persons" to trigger the notification obligation of a data controller. The GDPR also obligates data processor under Article 33(2) to "notify the controller without undue delay after becoming aware of a personal data breach".

EU data protection laws had not included any obligation to notify data breaches before the implementation of the GDPR. The DPD included the ineffective requirement that data controllers had to notify the responsible supervisory authority before conducting any wholly or partly automatic processing operations.[89] In addition, the fragmentation of notification standards within the EU enabled data controllers to either avoid notifications completely, because of deficient legal obligations or to accept sanctions, which were significantly lower than potential reputational damages. The GDPR attempted to increase transparency and the accountability of data controllers and processors by replacing the ex-ante approach of the DPD. The notification obligation of both the data controller and processor is linked to their awareness of the data breach, which supposedly offered some notification leeway. However, the GDPR obliges both parties to implement appropriate technical and organizational measures in combination with periodic monitoring, assessment and evaluation of these

[88] EU GDPR Art. 33.
[89] See Chapter 2.2.

measures to ensure the maintenance of an adequate security level.[90] To be sure, the burden of proof for unawareness about data breaches, therefore, seems to be unattainably high.

The GDPR provides no clear standards and no guidance as to which data breaches are notifiable and which party shall decide about the necessity to notify. According to the GDPR the notification obligation solely depends on the impact on "the rights and freedoms of natural persons", but does not clarify which party is entitled to assess the likely risk of personal data exposure. Therefore, agreements between controllers and processors may include a notification structure, designating the party responsible for assessing the likelihood of risk arising from a data breach, and a timeframe for data processors which may between 24 and 48 hours.[91] Section 3.4.5 will address the willingness of CSPs to accommodate customers and their notification obligations as data controllers.

2.4.3. Territorial Applicability

The GDPR extended the territorial applicability not only to organizations within the EU but also to organizations established outside of the EU. According to Article 3(1) of the GDPR, the qualification as an organization within or outside of the EU depends on the "establishment" of the data controller or processor. The term "establishment" is defined under Recital 22 of the GDPR and "implies the effective and real exercise of activity through stable arrangements", regardless of the legal form of these arrangements and whether the data is processed within the EU. The GDPR's definition of an establishment within the EU, therefore, applies to a broad spectrum of organizations. Recent decisions of the ECJ have proven the broad extraterritorial applicability of the GDPR by imposing provisions of the GDPR on a parent company, established outside of the EU, based on the violations of an EU based subsidiary. [92]

Under the GDPR, however, the avoidance of an "establishment" within the EU cannot be considered as a safe harbor for data controllers and processors. The GDPR also applies if the processing activities of the personal data of data subjects are related to "the offering of goods or services",[93] irrespective of

[90] EU GDPR Art. 32.

[91] Reedsmith.com. (n.d.). *GDPR series: Outsourcing contracts — all changed, changed utterly | Perspectives | Reed Smith LLP*. [online] Available at: https://www.reedsmith.com/en/perspectives/2018/03/gdpr-series-outsourcing-contracts--all-changed-changed-utterly [Accessed 20 Apr. 2019]

[92] In *Google Spain SL, Google Inc. v AEPD, Mario Costeja Gonzalez* (C-131/12) the Grand Chamber found that Google Inc was "established" within the EU, because of its Spanish subsidiary's EU based sales and advertising operations.

[93] EU GDPR Art. 3(2)(a).

required payments or the monitoring of data subjects' behavior.[94] The GDPR thereby applies to data processors, which are solely established outside of the EU but provide services to data controllers within the EU.

2.4.4. Cross-Border Data Transfers

This section considers the issue of organizations transferring data from the EEA to a service provider domiciled in a third country. Chapter V of the GDPR regulates the transfer of personal data outside of the EEA.[95] Article 44 – 49 of the GDPR, contain provisions similar to those of the DPD. These articles permit the transfer of personal data outside the EU under several different circumstances. Firstly, the EU Commission still provides a list of countries with an adequate level of personal data protection ('Adequacy decisions').[96] Secondly, if the third country does not provide an "adequate" level of data protection, data controller or processor could utilize a safeguard enumerated under Article 46, including SCCs[97] and BCRs.[98] Thirdly, the GDPR sets out derogations and exceptions under Article 49, which entitle data controller and processors to the cross-border transfer of personal data outside the EEA without "adequate" protection.

These provisions have similarities with the DPD and many organizations, consequently, already have compliance procedures in place. However, the differences between the GDPR and the DPD are noteworthy considering the significant increase of fines and penalties for non-compliance with the GDPR.

In particular, the GDPR explicitly confirms the validity of BCRs as a safeguard under Article 46. The GDPR sets out certain conditions, these BCRs have to match in order to receive an approval of a supervisory authority. This change may facilitate cross-border data transfer, especially in countries with no recent recognition of BCRs. As opposed to standard data protection clauses, BCRs are more

[94] EU GDPR Art. 3(2)(b).

[95] European Economic Area (EEA) unites the EU Member States and the three EEA EFTA States (Iceland, Liechtenstein, and Norway) into an Internal Market.

[96] EU GDPR Art 45, The number of countries with an adequate data protection level is extremely low, although the DPD already included a similar provision. These are: Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay.

[97] See fn. 48, The EU Commission can still decide, which standard contractual clauses provide for appropriate safeguard. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en [Accessed 1 April 2019].

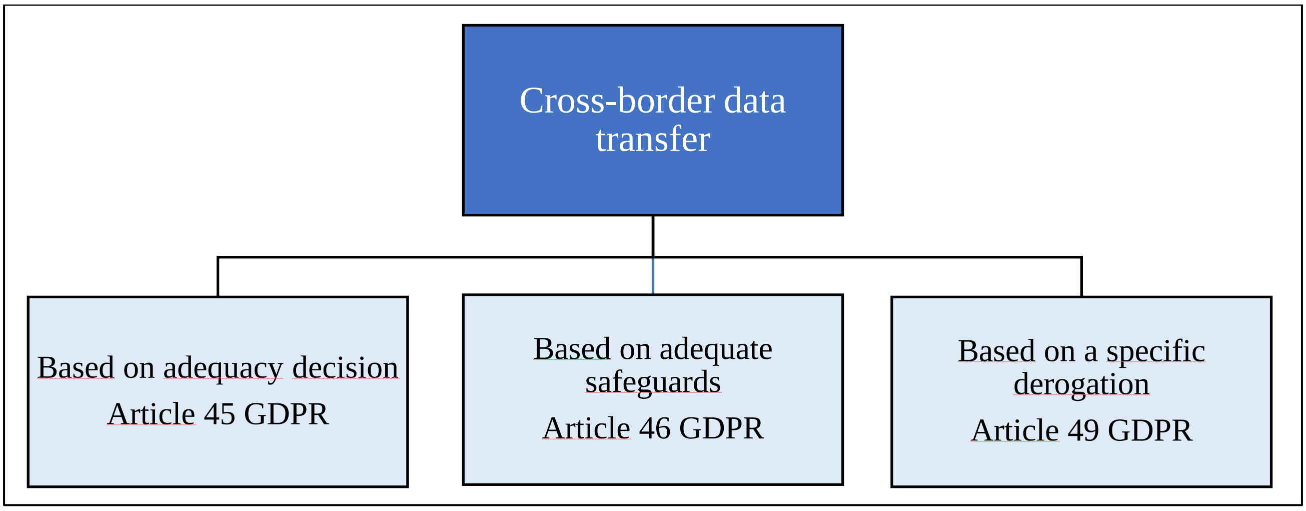
[98] See fn. 49.

business favorable due to the increased flexibility and reduced administrative burden after implementation.

In contrast to the DPD, the GDPR allows for the creation of SCCs by the EU Commission and no longer requires the approval of a national supervisory authority. The Commission has published two different versions, which apply to controller-processor[99] and controller-controller[100] relationships. Both variations have been adopted prior to the GDPR's commencement and hence may not addressed the entire range of the newly introduced obligations to data controllers and data processors.[101]

Additionally to the modification of the BCRs and SCCs, the GDPR provides two more mechanisms (also safeguards) under Article 46(2)(e) and (f). Under these provisions, data controller and processors can justify international transfers of personal data by relying on either an approved code of conduct or a certification mechanism.

Figure 2.2 Cross-Border transfer of personal data



Cross-border data transfer

Based on adequacy decision

Article 45 GDPR

Based on adequate safeguards

Article 46 GDPR

Based on a specific derogation

Article 49 GDPR

The changes implemented in the GDPR concerning the transfer of personal data outside of the EEA have to be taken into account by both data controllers and data processors. Both must assess current

[99]2010/87/: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) (Text with EEA relevance).

[100] 2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271)Text with EEA relevance.

[101] Lexology.com. (2018). *Standard contractual clauses challenged by GDPR and scrutinized by CJEU | Lexology*. [online] Available at: https://www.lexology.com/library/detail.aspx?g=d4a4a515-4868-4445-8b1c-0d358feab8fe [Accessed 1 Jun. 2019].

data flows in order to define which data is shared with third parties and which jurisdiction applies. Furthermore, existing data transfer mechanisms must be reviewed to ensure continued compliance with the GDPR. The changes may easily be addressed in practice due to the fact that the GDPR implemented minimal changes to the existing regulatory framework under the DPD.

2.4.5. Data Processor Liability

As opposed to former EU data protection laws, under the GDPR data processors incur direct statutory obligations. The previous DPD imposed obligations on the organization responsible for determining the purpose and means of the processed personal data (data controller). Service providers employed by the data controller to process data, were predominantly exempted from the same obligations.

The GDPR imposes a number of specific obligations on data processors. This includes the obligation to maintain the documentation of processing activities,[102]implement appropriate security measures,[103] assist data controllers in implementing a data protection impact assessment (DPIA),[104] appoint a data protection officer,[105] collaborate with the responsible supervisory authority and comply with the obligations on international data transfers.[106] Furthermore, a data processor must enter into a data process agreement with a data controller fulfilling the obligations of Article 28. A breach of one of these obligations may trigger direct liability in the form of sanctions[107] or private party claims.[108]

The new documentation obligations, force data processors to assume responsibility for their data privacy compliance due to the potential threat of revenue based fines and private claims. Service providers must examine and revise each of their contracts in order to comply. In addition, service providers must decide for each contractual relationship whether the data will be processed as a data processor or as a data controller. Service providers may opt to act as data processors as this constitutes lower levels of responsibilities as compared with a data controller.

In contrast, service provides acting as data controllers bear the main responsibilities as they are faced with the application of stricter GDPR obligations. Customers of service providers, acting as data

[102] EU GDPR Art. 30(2), See Appendix C, “Documentation Requirements”.
[103] EU GDPR Art. 32.
[104] EU GDPR Art. 28(3)(f), Art 35.
[105] EU GDPR Art. 37.
[106] EU GDPR Chapter V, See Chapter 2.5.5.
[107] EU GDPR Art. 83.
[108] EU GDPR Art. 79.

controller, encounter similar difficulties, but the GDPR imposes more obligations on them. The GDPR requires controllers namely to secure the personal data it processes itself and every data processed down the supply chain. Therefore, the procurement department of data controllers must examine each contract with service providers accurately and renegotiate them in order to comply with the GDPR.

This demands that the contract between a data controller, who outsources services to a service provider must be extensively negotiated. The GDPR includes binding requirements, for controller – processor relationships, which have to be included in the mandatory DPA.[109] As we shall see below,[110] some of these requirements lack specificity, which causes arbitrage between the negotiating parties. A variety of authors[111] have discussed this as being one of the key issues identified with the provisions of the GDPR. This is due to the fact that a party with greater expertise in the field of data privacy may be capable of receiving concessions from uninformed counterparties, which may result in financial, operational and reputational costs.

2.4.6. Increased Burden of Accountability

The GDPR further imposed increased accountability requirements on organizations processing personal data. In particular, the data controller bears the primary responsibility to demonstrate compliance with the “principles relating to processing of personal data”.[112] This underlying obligation to prove compliance was achieved through the implementation of some specific governance obligations, such as the documentation and data retention obligations.[113]

Data controllers accordingly must keep “records of processing activities”.[114] This obligation requires date controllers to keep comprehensive internal records of their data processing activities placed at the disposal of the responsible supervisory authority. Likewise, this obligation applies to data

[109] EU GDPR Art. 28.

[110] See Chapter 2.5.

[111] Reedsmith.com. (n.d.). *GDPR series: Outsourcing contracts — all changed, changed utterly | Perspectives | Reed Smith LLP*. [online] Available at: https://www.reedsmith.com/en/perspectives/2018/03/gdpr-series-outsourcing-contracts--all-changed-changed-utterly [Accessed 20 Apr. 2019], Brook, D. (2018). GDPR puts vendor contracts in the security spotlight. *Computer Fraud & Security*, [online] 2018(4), pp.5-7. Available at: https://www.sciencedirect.com/science/article/pii/S1361372318300319?via%3Dihub [Accessed 20 Apr. 2019], Pantlin, N., Wiseman, C. and Everett, M. (2018). Supply chain arrangements: The ABC to GDPR compliance —A spotlight on emerging market practice in supplier contracts in light of the GDPR. *Computer Law & Security Review*, [online] 34(4), pp.881-885. Available at: https://www.sciencedirect.com/science/article/pii/S0267364918302516 [Accessed 20 Apr. 2019].

[112] EU GDPR Art. 5(2).

[113] See Appendix C, “Documentation requirements”.

[114] EU GDPR Art. 30.

processors,[115] which means that they must maintain up-to-date records of its data processing as well. The documentation requirements placed on data processors, however, seem less extensive than those imposed on data controllers. The data processors' documentation requirements are less extensive under Article 30 GDPR but, must be specified in the DPA with data controllers, as required under Article 28 GDPR. The extent of data processors' documentation obligation, therefore, depends on the contract with the data controller.

Additional documentation obligations are determined under Article 35. Article 35 obliges data controllers to perform a DPIA[116] in case of "high risk to the rights and freedoms of natural persons" and the consultation of a data protection officer (DPO) or a supervisory authority.[117] The DPIA includes an impact assessment before the processing of high-risk data.[118] Data processors do not share the obligation of an ex-ante DPIA but must assist the data controller in preparing the DPIA if necessary and upon request.[119]

Also, the data controller is obliged to provide "data protection by design and by default".[120] "Data protection by design" means that the controller of personal data must assess the potential impact of processing certain personal data throughout the designing process of the provided service or product. In particular, the data controller must integrate "appropriate technical and organizational measures" upfront to comply with the GDPR and to protect data subjects' rights. "Data protection by default" means that the data controller is obliged to collect and process solely data that will be used for the "specific purpose of processing".[121] The controller of the data thus has to ensure by default that the processing of data for a specific purpose is limited to the necessary data amount, period of data storage and accessibility needed for each purpose.

[115] EU GDPR Art. 30(2).

[116] Data privacy impact assessment.

[117] EU GDPR Art. 36 and Art 58.

[118] High-risk data processing comprises of "automated processing, including profiling, which produce legal effects concerning the natural person or similarly significantly affect the natural person", processing of special categories of personal data[118] and long-term "systematic monitoring of a publicly accessible area".

[119] GDPR Art. 28(3)(f) determines that the contract between data controller and processor must specify that the processor "assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor."

[120] EU GDPR Art. 25.

[121] EU GDPR Art 25(2)

If the data controller uses the services of a data processor, a DPA between those parties shall set out the period of processing and ensure that the data controller complies with its obligation to protect personal data by default.[122]

2.5. The Impact on Third-Party Contracts

This section addresses the impact of the GDPR's new obligations on third-party agreements between data controllers and their service providers. As mentioned above, the GDPR expanded its scope of application on the supply chain, which sets out a new risk assessment foundation for both data controllers and service providers, acting as data processors. The third party-contracts between an organization and its service providers constitute a significant source of risk, which requires mutual data protection commitment by allocating responsibilities and obligations between the parties.[123] The subsequent sections will explain the necessary considerations of data controllers due diligence before selecting a service provider and the negotiable contractual terms of a GDPR compliant agreement.

Sub-processors

Article 28(2) allows the engagement of sub-processor only with prior 'general authorization' of the controller. In addition, the controller is granted the opportunity to object to changes in sub-processing or give 'specific authorization'. Service providers, however might be reluctant to constantly inform their customers about changing sub-contractors and refer to a public list of sub-contractors, which is kept up-to-date.[124] This solution may not be used to substitute the obligations under Article 28(2), because it would undermine the controller's right of objection by putting him in a more retrospective role.

Additionally, Article 28(4) obliges the processors to impose the same obligations on every engaging sub-contractor in the supply chain. Service providers, especially those outside of the EU, might claim

[122] GDPR Article 28(3) and 28(3)(g), defines that the data controller, "at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data", See also GDPR Recital 81.
[123] There are three types of risks, which emerge in this context, including financial exposure through administrative fines and compensation of data subjects, and reputational and operational ramifications.
[124] Ibid.

that it is difficult to harmonize the complex set of contracts with different parties. Moreover, the GDPR does not specify which terms must be completely identical in the controller-processor contract.[125]

2.5.1 Due Diligence

The GDPR obliges a data controller to “use only processors providing sufficient guarantees to implement appropriate technical and organizational measures, in such a manner that processing will meet the requirements of [the GDPR], and ensure the protection of the rights of the data subject”.[126] Appropriate compliance with this provision can only be achieved by conducting comprehensive due diligence before selecting a service provider.

The due diligence should address the following key issues. First, the controller should scrutinize the transparency of the provider regarding the ways in which it collects, uses and protects data. The level of transparency is ascertained by reviewing published privacy statements, white papers and other relevant materials.

Second, the provider could be qualified as data controller or processor based on the information in its published statements. As set out above,[127] the extent of legal obligations under the GDPR strongly depends on the classification of the service provider as a data controller or processor.

Third, information regarding the extent of the provider’s data security commitment may be identified through its reputation, data privacy history and transparency about its security measures.

Fourth, the controller must examine the length of time which the service provider retains personal data. This is because if the provider is a processor, the DPA with the controller shall determine that the processor retains personal data no longer than necessary for its services. The controller may prefer service providers, who provide clear information about data retention.

Fifth, a service provider outside the EEA has to be domiciled in a country subject to an adequacy decision, alternatively the service provider must agree to SCCs in the contract.

[125] Pantlin, N., Wiseman, C. and Everett, M. (2018). Supply chain arrangements: The ABC to GDPR compliance —A spotlight on emerging market practice in supplier contracts in light of the GDPR. *Computer Law & Security Review*, [online] 34(4), pp.881-885. Available at: https://www.sciencedirect.com/science/article/pii/S0267364918302516 [Accessed 20 Apr. 2019].
[126] EU GDPR Art. 28(1).
[127] See Chapter 2.5.

Sixth, the contractual framework and its essential elements must be clear. Although the GDPR only obliges controllers to contract with processors, it may also want to have contractual assurances by a service provider, acting as controller.

The due diligence shall serve as a primary selection between different service providers and as preparation for negotiations of the agreement.

2.5.2. Contractual Requirements

As mentioned above, the due diligence conducted by service users (controllers) shall cover considerations about the contractual arrangements with the service provider. These considerations also depend on the service provider's classification as controller or processor.

If the service provider acts as a data processor,[128] the contract (DPA) with the data controller must comply with the requirements under Article 28 and specific additional requirements set out by the GDPR.[129] Under Article 28 the contract between data controller and processor must include the subject matter, duration, nature and purpose of the processing, the type of personal data, the categories of data subjects, as well as the obligations and rights of the controller.

Additionally, Article 28(3) contains a list of specific elements, which must form a part of a contract with a data processor. In particular, Article 28 sets out the mandatory contractual elements of a DPA. These contractual elements include the processors obligation to process data only on documented instructions of the data controller,[130] to implement appropriate security measures,[131] to engage a sub-processor only after prior authorization of the controller and to pass all legal obligations under the contract with the controller to the sub-processor.[132] In addition DPAs shall obligate a data processor to assist the controller comply with it data breach notification obligations,[133] and to delete or return the personal data, depending on the controller's choice, to the controller after finishing the provided

[128] The designation as a 'processor' or 'controller' in a contract must reflect the reality, which means that "even though the designation of a party as data controller or processor in a contract may reveal relevant information regarding the legal status of this party, such contractual designation is nonetheless not decisive in determining its actual status, which must be based on concrete circumstances." Article 29 Data Protection Working Party, "Opinion 1/2010 on the concepts of 'controller' and 'processor' ". Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf [Accessed 3 Apr. 2019]

[129] See Chapter 2.5.4.

[130] EU GDPR Art. 28(a).

[131] EU GDPR Art. 28(c) and Art 32.

[132] EU GDPR Art. 28(d).

[133] EU GDPR Art. 28(f).

service.[134] Finally, the data processor should provide the controller with all necessary information in order to comply with the obligations under Article 28 and allow audits conducted by the controller or a mandated auditor.[135]

Audits

A number of these mandatory contractual elements may be subject to extensive negotiations between the parties. For example, Article 28(3)(h) contains an extension of the accountability principle. This Article imposes an obligation on processors to make available all necessary information and allow audits (including inspections). Service providers might be hesitant to grant a third party access to its system. Alternatively, instead of granting permitting audits, service provider may provide certificates of internationally accredited programs, such as the ISO 27001, or shared results of former conducted audits.[136] It's in the discretion of a data controller to accept or reject these alternatives. In the instance where the processor permits audits the parties may specify the respective clause in the DPA. The clause should adequately specified, addressing the frequency, scope and burden of bearing the costs.

Security measures

The GDPR obliges both data processors and controllers to implement "appropriate technical and organizational measures", [137] but only sets out a non-exhaustive enumeration including pseudonymization and encryption of data without being prescriptive. It remains unclear which security measures are most suitable in regards to this obligation. As we shall see later, new technologies, such as blockchain technology might be the solution to this problem.[138]

Data breach notifications

Under Article 33(2), the data processor is required to notify the data controller in case of a data breach. In contrast, Article 28(f) the contract (DPA) should solely oblige the data processor to assist the

[134] EU GDPR Art. 28(g).
[135] EU GDPR Art. 28(h).
[136] Reedsmith.com. (n.d.). *GDPR series: Outsourcing contracts — all changed, changed utterly | Perspectives | Reed Smith LLP*. [online] Available at: https://www.reedsmith.com/en/perspectives/2018/03/gdpr-series-outsourcing-contracts--all-changed-changed-utterly [Accessed 20 Apr. 2019].
[137] EU GDPR Art. 28(3)(c) and Art. 32.
[138] See Chapter 4.

controller in notifying data breaches. The GDPR includes no specific duty to include a notification obligation in the contract with data processors, which leaves space for negotiations.

Where the service provider acts as a data controller, the GDPR does not require the organization which deploys the services, to enter into a contract. Organizations acting from inside the EEA could agree to the controller-to-controller SCCs,[139] with a service provider processing its data from outside the EEA. Organizations should ensure that service providers acting as data controllers are bound to similar contractual obligations as set out under Article 28, obliging them to transfer, use and store the personal data appropriately.[140]

In cases where the organization and the service provider act as joint controllers, the parties must enter into an agreement aimed at clarifying each party's respective responsibilities and obligations. This is especially important for the nomination of the controller, who is responsible for the notice to data subjects. The controller acts as a contact point when data subjects request to exercise their rights.[141]

Irrespective of the service provider's classification, data controllers, may favor clear contractual commitments about the notification structure and which party shall decide about the necessity to notify.

2.5.3. Liability and Costs

This section addresses the allocation of liabilities and costs in third party contracts under the GDPR's changed liability structure. Under the GDPR liabilities can arise through direct sanctions of a supervisory authority,[142] claims of individuals[143] or contractual commitments.

Both data controllers and processors can be subject to a fine imposed by a supervisory authority. The fines can amount to €20 million or 4% of the worldwide turnover, whichever is higher, for specific data protection breaches, such as the infringement of a data subject's right.[144] Alternatively the fine

[139] 2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271)Text with EEA relevance.

[140] Hintze, M. (2018). Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR. [online] SSRN, Available at: https://ssrn.com/abstract=3192721 [Accessed 19 Apr. 2019].

[141] EU GDPR Art. 26.

[142] EU GDPR Art. 83.

[143] EU GDPR Art 82.

[144] EU GDPR Art. 83(5)(b) and Art. 12-22.

can amount to 10 million or 2% of the worldwide annual turnover, for other breaches, such as data protection by design and default.[145]

Individual claims by data subjects can be brought against controllers and processors without the need to prove financial losses. The proof of distress, anxiety or reputational damage could be sufficient to institute a claim.[146] As we will see below, the parties may limit the exposure by including indemnification rights in the contractual agreements.[147]

The contractual requirements between controllers and processors under Article 28, however, exclude a mandatory allocation of liability, which means that the parties must negotiate contractual liability internally. There may be conflicting interests depending on the way in which the parties are classified. This is because under the GDPR, data controllers bear greater responsibilities than data processors. The conflict of interests is further increased by the respective bargaining power of the parties.

Data processors may prefer to cap their liability due to the direct liability imposed on them by the GDPR. Considering the financial exposure a controller faces in the event of joint liability, a capped service provider liability would shift the financial risk to the controller. For example, a controller would have to bear administrative fines[148] and investigation costs issued by the supervisory authority, compensations accrued by claims of individuals[149] and cost to mitigate reputational damages. Therefore, data controllers may favor to implement their own liability cap. In particular, controllers might want to carve out data protection breaches from the general liability caps and implement a separate cap in line with the increased penalties of the GDPR.[150]

In addition the insurance coverage, especially related to cybersecurity, of each party will be a decisive factor for the allocation of liabilities between the parties.[151] The parties might review if their existing insurance protects against both personal data and regulatory breaches and matches the contractual liabilities.

[145] EU GDPR Art. 25.

[146] EU GDPR Art. 82 allows for claims based on non-material damages.

[147] See Chapter 3.4.6.

[148] EU GDPR Art. 83.

[149] EU GDPR Art. 82.

[150] Pantlin, N., Wiseman, C. and Everett, M. (2018). Supply chain arrangements: The ABC to GDPR compliance —A spotlight on emerging market practice in supplier contracts in light of the GDPR. *Computer Law & Security Review*, [online] 34(4), pp.881-885. Available at: https://www.sciencedirect.com/science/article/pii/S0267364918302516 [Accessed 20 Apr. 2019].

[151] Ibid.

The allocation of costs arising from compliance, such as costs of audits under Article 28(3)(h), must be seen separated from liability issues. The GDPR also does not address this issue and hence leaves the allocation of costs up to the contracting controller and processor, which must decide on a case-by-case basis.[152]

The resolution of the conflicting interests concerning liability and allocation of costs will depend on the bargaining strength of the respective party. As mentioned above, the GDPR leaves space for negotiations between the parties, which might benefit parties with more knowledge and expertise, such as big CSPs. Therefore, data controllers should negotiate carefully in order to avoid financial, operational and reputational damages.

2.6. Summary

In this section, we addressed four questions: i) what data protection laws preceded the GDPR; ii) what considerations led to a revision of the previous data protection laws; namely the DPD; iii) what main changes of the GDPR apply to the contractual relationships between service providers (data processors) with private or public entities (data controllers) and iv) what are the impacts of the changes on these contracts.

We explained that EU data protection laws aim to protect data privacy as a separate fundamental right. As opposed to U.S. Law, EU data protection laws intention to provide data privacy to every data subject.[153] We also explained that the DPD, which preceded the GDPR, attempted to increase data privacy awareness and transparency but had to be revised due to a number of weaknesses. We discovered that the DPD lacked harmonization and was unsuitable with regards to current technological standards.

We scrutinized the considerations preceding the GDPR and explained that the EU intended to further improve data privacy of individuals and improve data flows within the EU by through the establishment of a new regulation. We discovered that the GDPR is characterized by a complex

[152] Reedsmith.com. (n.d.). *GDPR series: Outsourcing contracts — all changed, changed utterly | Perspectives | Reed Smith LLP*. [online] Available at: https://www.reedsmith.com/en/perspectives/2018/03/gdpr-series-outsourcing-contracts--all-changed-changed-utterly [Accessed 20 Apr. 2019].

[153] See fn. 26.

network of provisions and argued that it predominantly focuses on the protection of data subjects' rights at the expense of data controllers and processors.

We examined the main changes of the GDPR, which directly affect the relationship between organizations and their service providers, and explained that it obliges both parties to promote compliance proactively. As opposed to the DPD, both parties bear obligations and responsibilities under the GDPR irrespective of their status as a data controller or processor. We discovered that the classification as a controller or processor depends on how the organization and its service providers process the specific data.

We explained that data controllers shall only use processors that provide sufficient guarantees and hence are well-advised to conduct a comprehensive due diligence.

We elucidated that the lack of accuracy in some of GDPR provisions may further complicate the negotiation of privacy clauses in third party contracts. We examined the vague provisions comprising the controller's right to audit, the obligation of service providers to secure the supply chain, the notification obligations and the obligation to implement adequate security measures. Further we distinguished mandatory contractual requirements from contractual terms, which are not covered by the GDPR; i.e. liability and allocation of costs. We discovered that these are key issues, which must be negotiated carefully considering the high penalties for both controllers and processors. We argued that the GDPR leaves space for extensive negotiations and concluded that the final terms of an agreement will depend on the bargaining power of each party. Finally, we argued that parties with more data privacy expertise could elicit concessions from counterparties, which could have detrimental financial, operational and reputational consequences.

CHAPTER THREE: CLOUD SERVICE INDUSTRY

3.1. Introduction

In Chapter Two, we established that the GDPR does requires internal compliance from data controllers and external compliance from its service providers and their subcontractors with whom it might share personal data directly or indirectly. We explained that the negotiations of a contract or DPA between a customer (data controller) and a service provider (data processor) suffer due to uncertainties associated with translating the GDPR provisions in practice. The negotiation process is further affected by the increased sanctions imposed by the GDPR. Sanctions may amount to fines up to EUR 20 million or 4% of the annual worldwide turnover.[154] We identified that, according to prior research, the relationship between service providers and consumers are most vulnerable to data breaches.[155] Research shows that 63% of data breaches are linked to third-party access.[156] We established that the DPA must contain clear clauses, in order to address GDPR related uncertainties, define responsibilities and outline liabilities between the parties. We found that the mandated procurement/supply chain compliance might only be achieved by customers and service providers with sufficient resources and bargaining power. Data controllers or service provider with a lower level of bargaining power may be deprived of outsourcing or face potential fines.[157] We further found that the increased complexity of the GDPR's provisions coupled with knowledge asymmetries between parties, may favor more knowledgeable parties. These parties may exploit the counterparty in terms of liability and costs concessions, which might result in economic and reputational damages.[158]

In Chapter Three we intend to answer three questions; first, how does the GDPR influences cloud service agreements. Second, do CSPs provide sufficient public information to facilitate the due diligence process carried out by potential customers, acting as data controllers. Third, do CSPs provide

[154] EU GDPR Art. 83.

[155] Pantlin, N., Wiseman, C. and Everett, M. (2018). Supply chain arrangements: The ABC to GDPR compliance — A spotlight on emerging market practice in supplier contracts in light of the GDPR. Computer Law & Security Review, [online] 34(4), p.881. Available at: https://www.sciencedirect.com/science/article/pii/S0267364918302516 [Accessed 20 Apr. 2019].

[156] Iapp.org. (2017). Surprising stats on third-party vendor risk and breach likelihood. [online] Available at: https://iapp.org/news/a/surprising-stats-on-third-party-vendor-risk-and-breach-likelihood/ [Accessed 1 May 2019].

[157] Iapp.org. (2016). *GDPR: Killing cloud quickly?*. [online] Available at: https://iapp.org/news/a/gdpr-killing-cloud-quickly/ [Accessed 1 May 2019].

[158] Reedsmith.com. (n.d.). *GDPR series: Outsourcing contracts — all changed, changed utterly | Perspectives | Reed Smith LLP*. [online] Available at: https://www.reedsmith.com/en/perspectives/2018/03/gdpr-series-outsourcing-contracts--all-changed-changed-utterly [Accessed 20 Apr. 2019].

sufficient contractual flexibility for customers to sustain procurement chain compliance or do potential customers have to accept predetermined onerous terms in order to access the services of CSPs.

3.2. Cloud Services

In this section, we will explain the different types of cloud services, the role of CSPs under the GDPR and discuss the impact of the GDPR on CSPs' vendor agreements. Cloud computing is defined as a scalable network access to shared computing resources, which requires less in-house resources and hard- and software expertise.[159] Generally, customers receive on-demand access to a model for managing, storing and processing data online via the internet in order to reduce customers' costs and improve their service quality. In contrast to cloud services, traditional outsourcing requires the commissioning of an external service provider to provide a business function, which has been conducted internally before.[160]

In addition, Cloud Computing is defined in relation to its three service models and three deployment models (public, private and hybrid). A private cloud is created and maintained by an individual organization, which enables an organization to ensure internal data privacy through firewalls and without any third party access. On the other hand, public clouds are characterized by multi-tenancy. This means that it allows CSPs to distribute the same service to all parties who wants to use it. Hybrid cloud services[161] combine elements of private clouds and publicly available services. The three service models include Software as a service (SaaS), Platform as a service (PaaS) and infrastructure as a service (IaaS).[162] These three service models can occur in a separate or layered form, which means that a SaaS provider may run its services on a PaaS or IaaS.[163]

IaaS providers, such as Microsoft Azure,[164] allow customers to use computing resources, including data storage, virtualization, servers and networking, to avoid purchasing and maintaining its own

[159] The US National Institute for Standards and Technology (NIST) defines cloud computing as a "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interactions."

[160] The IT Law Wiki. (n.d.). *Traditional outsourcing*. [online] Available at: https://itlaw.wikia.org/wiki/Traditional_outsourcing [Accessed 1 May 2019].

[161] For example, IBM Z Hybrid Cloud or SAP Hana Platform.

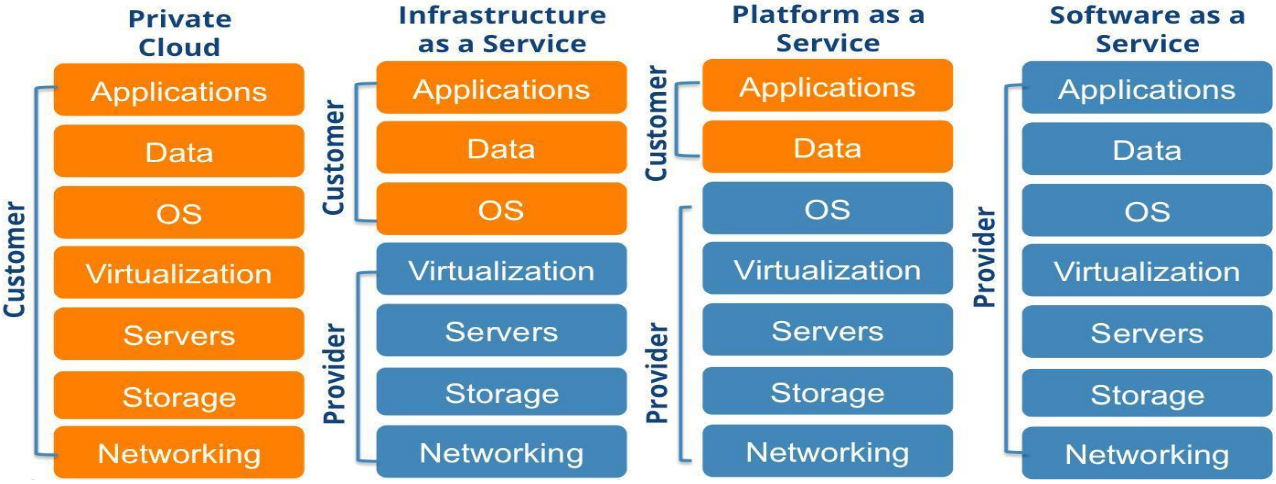
[162] Gartner IT Glossary. (n.d.). *IaaS - Infrastructure as a Service - Gartner IT Glossary*. [online] Available at: https://www.gartner.com/it-glossary/infrastructure-as-a-service-iaas [Accessed 1 May 2019].

[163] Kamarinou, D., Millard, C. and Oldani, I. (2019). *Compliance as a Service*. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3284497 [Accessed 10 May 2019].

[164] Azure.microsoft.com. (n.d.). *What is Azure—Microsoft Cloud Services | Microsoft Azure*. [online] Available at: https://azure.microsoft.com/en-us/overview/what-is-azure/ [Accessed 1 May 2019].

hardware and software.[165] The customer is able to run arbitrary operating systems and applications on the provided infrastructure.[166] PaaS allows customers to deploy self-created or purchased applications using the resources provided by the service provider onto the predefined infrastructure.[167] Software as a service (SaaS) is when software is delivered through the cloud with the consumer typically using thin client interface, most often a web browser to access the provider's applications.[168]

Figure 3.1 – Cloud service models



Source: https://www.sevone.com/white-paper/monitoring-cloud-infrastructure-performance-eliminate-visibility-gaps

Figure 3.1 indicates that private cloud services give the consumer full control over its gathered personal data, which might be useful if the customer already has a functioning data center in place. A drawback to this solution may be that customers must personally update the data center at their own expense. Figure 3.1 further reveals that the service models IaaS, PaaS and SaaS are characterized by an ascending level of provider control. This results in better scalability and cost efficiency for the customers, because the CSP bears the responsibility of data storage and data center maintenance. However, this raises the question of whether CSPs act as data controllers or processors.

As set out above, the GDPR distinguishes between the data controller and data processor, who acts on behalf of the data controller.[169] CSPs, therefore, would have to process personal data, stored at their

[165] Hon, W. and Millard, C. (2013). *Cloud Computing vs. Traditional Outsourcing – Key Differences*. [online] Papers.ssrn.com. p. 1. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2200592 [Accessed 1 May 2019].
[166] Ibid.
[167] Nvlpubs.nist.gov. (2011). *The NIST Definition of Cloud Computing*. [online] Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [Accessed 2 May 2019].
[168] Ibid.
[169] See Appendix A.

database, on behalf of the customer without determining the purpose and means of the processing. As mentioned above, the distinction between controllers and processors carries a different set of obligations with more onerous obligations being placed on the data controller.[170] While the data controller is effectively outsourcing the obligation to provide "data protection by design and by default"[171] and secure processing of personal data, it retains legal responsibility.[172] The extant preferred treatment might be one of the reasons that, as we will see below, CSPs prefer to be classified as data processors.[173] The subsequent sections, hence, assume that CSPs act as data processors.

Next to the classification as a data processor or controller, there are, notwithstanding the impact on third-party contracts,[174] a number of questions arising from the deployment of cloud services. As mentioned before, customers do not retain control over the services processing the personal data due to the storage of the data at the CSP's data center. However, the customer must be assured that the CSP employs acceptable security standards, clarifies where the data will be located, how it is stored and who has access it. Customers further may want to be aware of the procedures in case of a data loss, if there is a backup and if the backup is located in a country with adequate data protection.[175] Furthermore, a customer should be convinced that a CSP is capable of fulfilling its obligations towards data subjects, including data portability.[176] Finally, customers may be concerned about the CSP's procedures after their services end, and if the personal data will be erased or persist somewhere in the cloud. Customers shall consider each of these issues in their due diligence.[177] From this view, the GDPR's enhanced requirements[178] demand financial resources to implement appropriate security measures, and substantial bargaining power to secure their entire supply chain.[179]

[170] See Chapter 2.4.5. and 2.4.6.
[171] EU GDPR Art. 25.
[172] EU GDPR Art. 24.
[173] See Chapter 3.4.
[174] See Chapter 2.5
[175] See Chapter 2.4.4.
[176] EU GDPR Art. 20, "Data portability - The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided."
[177] See Chapter 2.5.1.
[178] See Chapter 2.4.5.
[179] Pantlin, N., Wiseman, C. and Everett, M. (2018). Supply chain arrangements: The ABC to GDPR compliance —A spotlight on emerging market practice in supplier contracts in light of the GDPR. *Computer Law & Security Review*, [online] 34(4), p.883. Available at: https://www.sciencedirect.com/science/article/pii/S0267364918302516 [Accessed 20 Apr. 2019].

We have explained that cloud services can have many different forms, but that all CSPs may prefer to be classified as a data processor. Nevertheless, CSPs need to be cautious with their provided services due to newly imposed responsibilities under the GDPR[180] and the multi-layered and multi-tenanted nature of their business models. The different processing scenarios, therefore, might require tailored contracts between customers (data controllers) and CSPs (data processors).[181] However, there may be limits for public CSPs to provide each customer with customized services. Therefore, customers with lower bargaining power, such as SMEs, might have to accept predetermined terms according to the motto of 'take it or leave it' or opt for traditional outsourcing.[182] The subsequent sections shall examine which information CSPs provide to convince potential customers of their capabilities to be GDPR compliant and whether there is any value for customers by reading these public statements.

3.3 Do Privacy Policies and Public Statements matter?

This section attempts to assess the value, as well as the practical and legal ramifications of CSPs' public statements and privacy policies to its customers. After the implementation of the GDPR on the 25 May 2018, many CSPs published compliance commitment, such as:

We protect your business' data and put you in control. We understand how important data is to your business. That is why we keep your business' data protected and give you control over how your data is used and shared.[183]

Our Legal, Trust and Security teams have carefully scrutinized the GDPR, and have taken the necessary steps to identify where we need to comply and where any changes need to be made. We achieved full compliance before May 2018, and are committed to helping our customers prepare for their obligations.[184]

Yes. The GDPR requires controllers (such as organizations using Microsoft's enterprise online services) only use processors (such as Microsoft) that provide sufficient guarantees to meet key

[180] Ibid.

[181] https://www.fieldfisher.com/media/3993765/the-gdprs-impact-on-the-cloud-service-provider-as-a-processor-mark-webber-privacy-data-protection.pdf. (2018). *PDPjournal*, 16(4).

[182] Oprysk, L. (2016). The Forthcoming General Data Protection Regulation in the EU: Higher Compliance Costs Might Slow Down Small and Medium-Sized Enterprises' Adoption of Infrastructure as a Service. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3019917 [Accessed 4 May 2019].

[183] Privacy.google.com. (2019). *Businesses and Data | Google protects your data and put your business in control*. [online] Available at: https://privacy.google.com/businesses/ [Accessed 6 May 2019].

[184] Dropbox.com. (2019). *General Data Protection Regulation (GDPR) Guidance Center*. [online] Available at: https://www.dropbox.com/security/GDPR [Accessed 6 May 2019].

requirements of the GDPR. Microsoft has taken the proactive step of providing these commitments to all Volume Licensing customers as part of their agreements.[185]

Today, I'm very pleased to announce that AWS services comply with the General Data Protection Regulation (GDPR). This means that, in addition to benefiting from all of the measures that AWS already takes to maintain services security, customers can deploy AWS services as a key part of their GDPR compliance plans.[186]

These statements attempt to provide reassurance to customers and limit uncertainty surrounding the GDPR. The CSPs in question recognized the business opportunity to allegedly provide customers with the necessary support to achieve GDPR compliance. Such statements have limited value to customers and data controllers due to its non-prescriptive character.

Besides public statements, CSPs' privacy policies constitute a main source of their public communication. The principal of transparency,[187] one of the key principles of the GDPR,[188] obliges service providers to explain to the public in concise, easily accessible and understandable language how personal data will be stored, used and transferred. Although a privacy policy does not suffice to regulate the controller – processor relationship, it is a source of information for the public including potential customers, in understandable language about its handling of personal data.

Prior research has revealed that privacy policies under the scope of the DPD were misleading for individuals. This is mainly because these documents lack references to the particular services and are not transparent about sub-processors.[189] More recent research systematically examined the readability of privacy policies subject to the GDPR in order to assess whether these policies provide increased transparency.[190] Surprisingly the research revealed that privacy policies are only slightly more

[185] Microsoft.com. (2019). GDPR FAQs, Microsoft Trust Center. [online] Available at: https://www.microsoft.com/en-us/trustcenter/privacy/gdpr/gdpr-faqs [Accessed 6 May 2019].
[186] Amazon Web Services. (2018). All AWS Services GDPR ready | Amazon Web Services. [online] Available at: https://aws.amazon.com/blogs/security/all-aws-services-gdpr-ready/ [Accessed 6 May 2019].
[187] EU GDPR Recital 58.
[188] See Chapter 2.1.
[189] Kamarinou, D., Millard, C. and Hon, W. (2015). *Privacy in the Clouds: An Empirical Study of the Terms of Service and Privacy Policies of 20 Cloud Service Providers*. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2646447 [Accessed 4 May 2019], The survey examined the privacy policies and terms of use of twenty cloud service providers in order to assess the treatment of individuals data privacy rights.
[190] Becher, S. and Benoliel, U. (2019). *Law in Books and Law in Action: The Readability of Privacy Policies and the GDPR*. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3334095 [Accessed 4 May 2019].

readable than preceding policies.[191] This seems surprising because simplified and clear language would not only enable individuals and data controllers to make well-informed decisions but also might increase the attractiveness of CSPs. Further, Google received a fine of about EUR 50 million from the French supervisory authority CNIL due to the lack transparency in its privacy policy.[192] This action shows the firm position of EU regulatory bodies have taken in regards to this issue. Some may argue that privacy policies entail complex information that cannot be translated into plain language. The readability may be improvable to some extent, which could lower the level of information asymmetries between CSPs and their customers.[193] Subsequently, this could increase trust amongst customers with regards to the ability of cloud services' to comply with the GDPR and in turn increase overall market efficiency.[194]

We can conclude that privacy policies and public statements are the first indicators used by data controllers when selecting potential CSPs. However, these information resources do not provide significant value to customers due to their lack of enforceability. The primary source of mutual commitment between data controllers and CSPs remains a DPA.[195] In the subsequent section, we will look beyond the external appearance of CSPs and examine whether public statements and privacy policies are backed up by contractual commitments to support customers in their GDPR compliance.

3.4 Analysis of DPAs and Cloud Service Agreements

This section shall examine the contractual framework between customers (data controllers) and CSPs (data processors). As set out above, Article 28 of the GDPR imposes mandatory commitments between data controllers and data processors,[196] which must be incorporated in a DPA or other legal act under Union or Member State law.[197] Even though data controllers carry the ultimate burden of responsibility to demonstrate compliance, the outsourcing of services to CSPs creates mutual dependency in terms of GDPR compliance.

[191] Ibid.

[192] Cnil.fr. (2019). The CNIL’ s restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC | CNIL. [online] Available at: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc [Accessed 9 May 2019].

[193] Becher, S. and Benoliel, U. (2019). *Law in Books and Law in Action: The Readability of Privacy Policies and the GDPR*. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3334095 [Accessed 4 May 2019].

[194] Ibid.

[195] EU GDPR Art. 28(3).

[196] See Chapter 2.5.

[197] EU GDPR Art. 28(3).

This section will conduct an empirical survey of publicly available DPAs, service agreements and terms of use provided by 17 selected CSPs.[198] The survey discusses the GDPR's negotiable provisions,[199] which needed to be updated by CSPs. The DPAs, service agreements and terms of use included in this survey are publicly available on the CSPs' websites. The survey acknowledges that some agreements with CSPs require further negotiations in practice, especially with more significant customers, but these agreements exceed the scope of this thesis.

The survey first takes a closer look at the concept of the controller's right to issue 'documented instructions' to the processor.[200] Part two examines the appointment of sub-processors and the controllers' right to object.[201] Part three shall focus on Article 32 of the GDPR and the controllers' and processors' obligation to demonstrate the implementation of appropriate security measures. Part four will discuss the data controller's contractual right to audits.[202] Subsequently, part five shall assess the mutual data breach notification obligations[203] and part six will address the allocation of risk in terms of liabilities and indemnifications.

3.4.1. Controllers Right to Issue Documented Instructions

Article 28(3)(a) of the GDPR enables data controllers to issue arbitrary 'documented instructions' for processing personal data. CSPs tend to confine the exercise of this right to the instructions within their DPAs, or other legal act covering their mutual commitments. The concept of a controller giving arbitrary instructions to a processor seems unrealistic, especially for CSPs, which have a magnitude of customers.[204] The right to give documented instructions was included in the GDPR as a means to avoid the data processors' use and disclosure of data for their own specific purposes. However, this objective has not been adequately achieved. A more effective policy choice may have been the inclusion of a simple ban on the self-serving use of data.[205]

The survey shows that the interpretation of the controller's 'documented instructions' differs among the CSPs. Most of the CSPs specifically define that the DPA and every other applicable agreement

[198] See Appendix D.
[199] See Chapter 2.5.2.
[200] EU GDPR Art. 28(3)(a).
[201] EU GDPR Art. 28(2).
[202] EU GDPR Art. 28(3)(h).
[203] EU GDPR Art. 33.
[204] Iapp.org. (2016). *GDPR: Killing cloud quickly?*. [online] Available at: https://iapp.org/news/a/gdpr-killing-cloud-quickly/ [Accessed 1 May 2019].
[205] Ibid.

constitute the complete and final documented instructions.[206] Some CSPs allow additional instructions but under the condition of another agreement, which must be agreed upon separately.[207] Other CSPs, such as Oracle Cloud, commit to accepting additional instructions at no additional costs.[208] Further, SAP attempts to use reasonable efforts to comply with instruction going beyond the initial agreements.[209] On the other hand, some CSPs refuse this more flexible approach and even charge customers for every additional instruction.[210]

The concept of 'documented instruction' may constitute an unrealistic approach, especially in the context of cloud services, and results in increased costs for the CSPs. These costs are then shifted onto the customer, which detracts from the cost-effective nature of cloud services. This leaves the customer with the choice to either accept the additional costs or terminate the contract.

3.4.2. The Appointment of Sub-processors

This section attempts to examine the provided transparency and cooperation of CSPs in the context of newly appointed sub-processors. As part of the 'documented instructions', the data controller is entitled to authorize the appointment of sub-processors in general or specifically.[211] Theses sub-processors could potentially cause data leaks, which would fall back on the customer, being subject to the central liabilities under the GDPR. The survey shows that CSPs mainly provide a frequently updated list of sub-processors on their website[212] and a notification mechanism, which informs about the appointment of new sub-processors.[213] This approach may not be compliant with Article 28(2) of the GDPR, which requires the processor to give an ex-ante notification to the controller. Only 7 out of 17 CSPs commit to notifying the customer within a specific timeframe before every new hiring.[214] The timeframe usually ranges from 7 days[215] to 30 days,[216] but can amount to 6 months for specific cloud services, such as Microsoft's 'core online services'.[217] Also, the majority of the CSPs do not provide

[206] See for example Alibaba Cloud GDPR Addendum Section 5(b), Kamatera states that the 'Processor shall not Process Processed Personal Data other than on the Controller's instructions in this DPA' Kamatera DP Agreement Section 4.1.
[207] Microsoft Online Services Terms Section 'Processor and Controller Roles and Responsibilities'.
[208] Oracle Cloud DP Agreement Section 5.
[209] SAP DP Agreement Section 3.1.
[210] See for example IBM Cloud DP Agreement Section 10.2, VMware DP Addendum Section 2.3.
[211] See chapter 2.5.2.
[212] For example Salesforce DP Agreement Section 5.2.
[213] See for example Dropbox states that 'Customers that wish to receive email notifications if this list is updated may subscribe to receive such notifications on behalf of their team by completing this form' Dropbox List of Sub-Processors.
[214] For example Google Data Processing and Security Terms (Customers) Section 11.4(a).
[215] Rackspace Cloud DP Agreement Section 2.3.1.
[216] OVH Cloud DP Agreement Section 7.
[217] Microsoft Online Services Terms Section 'Notice and Controls on use of Subprocessors'.

the customer with sufficient information about the new sub-processors. Kamatera is the only CSP that endeavors to include “relevant details of the Processing to be undertaken by the new Sub-Processor”.[218]

As opposed to the ex-ante time frame, the majority of the CSPs surveyed provide the controller with an objection period after being notified. The granted objection periods range from 7 days[219] to 90 days.[220] If controllers want to exercise their right to object, most CSPs demand a written justification.[221] Most of the CSPs do not limit the variety of potential justifications,[222] but some CSPs require the controller to provide a reasonable justification.[223] VMware for example entitles the controller to object only on reasonable data protection grounds.[224] Oracle goes one step further and requires the controller to provide “objectively justifiable grounds related to the ability of such Third Party Subprocessor or Oracle Affiliate to adequately protect Personal Data in accordance with this DPA or Applicable Data Protection Law”.[225] After accepting the justifications, some of the surveyed CSPs accommodate the customer by assuring to take reasonable steps[226] or to find a mutually acceptable solution.[227] These concessions constitute no guarantee for customers to reach consensus with the CSP. For most of the CSPs the objection to the appointment or replacement of a sub-processor equates to a termination of the contract directly,[228] which forces the customer to either accept the new sub-processor or accept the transition costs of switching to a new CSP. Google, for example, obliges the customer to delete the software instantly[229] upon written notice about an objection.[230]

The GDPR requires the controller’s consent for each appointed sub-processor, which might be difficult to achieve especially for CSPs due to their interconnectedness with a variety of sub-processors. The survey shows that some CSPs are willing to cooperate, but only to a certain extent. The majority of CSPs refuse to provide sufficient information about new sub-processors ex-ante. Furthermore, the

[218] Kamatera DP Agreement Section 6.3.
[219] Ibid.
[220] Google Data Processing and Security Terms (Customers) Section Section 11.4(b).
[221] For example IBM DP Addendum Section 7.1.
[222] For example AWS DP Addendum Section 6.1., Cisco Meraki DP Addendum Section 5.2.
[223] See for example VMware DP Addendum Section 3.4., Oracle Cloud DP Agreement Section 8.3.
[224] See for example VMware DP Addendum Section 3.4.
[225] Oracle Cloud DP Agreement Section 8.3.
[226] For example Kamatera DP Agreement Section 6.3.
[227] Oracle Cloud DP Agreement Section 8.3.
[228] Rackspace Cloud DP Agreement Section 2.3.1.
[229] Google Cloud Platform Terms of Service Section 9.5.
[230] Google Data Processing and Security Terms (Customers) Section 11.4(b).

ultimate remedy always remains the termination of the agreement, which will have an economic impact on customers. As a consequence, this creates a ‘take it or leave it’ dilemma for customers.

3.4.3. Security Obligations

This section attempts to examine the technical and organizational security measures which might be ‘appropriate’ to the risk of potential data breaches. Furthermore, the section attempts to examine whether CSPs support customers in their compliance with Article 32 of the GDPR.

According to Article 32 of the GDPR the controller and processor shall take “nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons” into account when implementing appropriate security measures. As explained above,[231] the ‘nature’ of cloud services can be divided into three service models, SaaS, PaaS and IaaS. An IaaS service provider, for example, provides the infrastructure, and the processor manages the access and security of the data storage. In this scenario, the CSP might need a lower level of security in terms of data privacy. A SaaS provider on the other hand, which manages the used applications and processes the customer’s data (on its behalf), may have to implement more robust security measures. However, cloud services can be constructed in a layered nature (e.g. a SaaS provider using IaaS), and the CSPs (data processors) bear the legal responsibility to impose the same security standards on its sub-processors. Therefore, even if CSP’s services require a low level of security, the inappropriate security standards of sub-processors could force the CSP to implement higher security levels. The CSPs being surveyed did not include any distinctions in their DPAs between the different security measures provided. The specific security measures provided for each service may be found in the respective service agreement. The analysis of these specific service agreements goes beyond the scope of the survey, but the DPA might be used as a generic template for any additional service agreements.

The survey shows that all CSPs include information and details of their implemented security measures to comply with the GDPR and thereby followed the structure of Article 32. An analysis of the definitions and explanations of the specific technologies exceeds the scope of the survey, but it is worth mentioning that the CSPs provide a wide range of different technologies. The security measures, for instance, include data integrity controls, such as antivirus and firewalls,[232] and physical protection,

[231] See Chapter 3.2.

[232] SAP DP Agreement Appendix 2 Section 1.2.

such as CCTV cameras and alarm systems,[233] electronic access control validation (e.g. card access systems)[234] and lead-lined containers.[235]

The survey further demonstrates that some CSPs[236] are willing to comply with one of the three code of conducts, comprising the CISPE,[237] Cloud Security Alliance (CSA)[238] and the EU Cloud Code of Conduct.[239] According to Article 28(5) of the GDPR the adherence to one of these codes of conduct may serve as proof of the implementation of appropriate security measures, but this does not eliminate any contractual audit right[240] of the customer (data controller).

As set out above, both the controller and processor of personal data must implement appropriate security measures. The survey, however, shows that some CSPs impose the entire responsibility to confirm the compliance of the CSPs' security measures with the GDPR onto the customer (data controller).[241] This implies that customers not only have to implement appropriate internal security measures but also need to understand the CSPs' security measures.

Since smaller customers (i.e. SMEs) might lack the expertise and financial resources to bear both of these responsibilities it may be necessary that CSPs offer additional support. This would result in the reallocation of risk onto the CSPs, who have the necessary resources to mitigate the risk. For customers, which might not always be technology-based companies, the outsourcing of security obligations may be highly beneficial. However, this is unlikely because customers cannot delegate

[233] Google Cloud Data Processing and Security Terms (Customers) Appendix 2 Section 2(a).

[234] AWS DP Addendum Appendix 1 Section 1.2.1.

[235] SAP DP Agreement Appendix 2 Section 1.4.

[236] For example Alibabacloud.com. (2019). Alibaba Cloud Security & Compliance Center for Cloud Computing Infrastructure. [online] Available at: https://www.alibabacloud.com/trust-center?spm=a2c63.o282931.879956.5.5e1518acplAQfp [Accessed 8 May 2019], Amazon Web Services. (2017). AWS Announces CISPE Membership and Compliance with First-Ever Code of Conduct for Data Protection in the Cloud | Amazon Web Services. [online] Available at: https://aws.amazon.com/blogs/security/aws-announces-cispe-membership-and-compliance-with-first-ever-code-of-conduct-for-data-protection-in-the-cloud/ [Accessed 8 May 2019].

[237] CISPE - The Voice of Cloud Infrastructure Service Providers in Europe. (2019). CISPE - Code of Conduct, for Cloud Infrastructures Services. [online] Available at: https://cispe.cloud/code-of-conduct/ [Accessed 8 May 2019].

[238] Cloud Security Alliance. (2018). Cloud Security Alliance Issues Code of | Cloud Security Alliance. [online] Available at: https://cloudsecurityalliance.org/articles/cloud-security-alliance-issues-code-of-conduct-self-assessment-and-certification-tools-for-gdpr-compliance/ [Accessed 8 May 2019].

[239] Eucoc.cloud. (2018). Home: EU Cloud CoC. [online] Available at: https://eucoc.cloud/en/home.html [Accessed 8 May 2019].

[240] EU GDPR Art. 28(h), See Chapter 3.4.4.

[241] Microsoft Online Services Terms Section 'Customer Responsibilities', Rackspace Cloud DP Agreement Section 2.2.3.

their substantive obligations imposed by the GDPR.[242] The survey supports this argument, because none of the surveyed CSPs provides a similar compliance support solution.

3.4.4. Audits

This section examines whether CSPs grant customers the right to audit and hence access to their company premises in order to demonstrate compliance with the GDPR. As set out above,[243] Article 28(3)(h) obligates data processors to allow audits and inspections conducted by the controller or a third-party mandated by the controller. The survey reveals, however, that many of the CSPs solely offer the controller to outsource the right to audit and provide access to the auditing reports and certificates upon controllers' request.[244] Some of the DPAs provide alternative audit options if the customer is not satisfied by the CSP's auditing or compliance reports.

The survey shows that the CSPs choose differing approaches in order to address the controllers' contractual auditing right under Article 28(3)(h). SAP, for example, allows audits by the controller or an independent third party if SAP failed to provide sufficient evidence to prove compliance with security measures.[245] Other CSPs allow on-site inspections under certain conditions. Slack and IBM, for example, grant permission to the extent that it is impossible to otherwise satisfy an audit obligation mandated by applicable law.[246] Rackspace "permits Customers to perform reviews of the security of the Services or evaluate and monitor the Applicable Rackspace Entity's compliance with its security obligations set forth under the Addendum."[247] Google also allows audits, including inspections, after receiving the customer's request. Google requires the customer to negotiate "the reasonable start date, scope and duration of and security and confidentiality controls"[248] of each audit and will charge a fee.[249] SAP, Rackspace and OVH Cloud also demand the customer to bear the costs of an audit.

[242] Kamarinou, D., Millard, C. and Oldani, I. (2019). *Compliance as a Service*. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3284497 [Accessed 10 May 2019].
[243] See Chapter 2.5.2.
[244] For example VMware DP Addendum Section 6, Alibaba Cloud GDPR Addendum Section 4(h), Dropbox DP Agreement Section 2.5.
[245] SAP DP Agreement Section 5.1(a).
[246] Slack DP Agreement Section 5.2, IBM Cloud DP Addendum Section 5.1(d).
[247] Rackspace Cloud DP Addendum Section 3.2(a).
[248] Google Cloud Data Processing and Security Terms (Customers) Section 7.5.2(a) and 7.5.3(a), Other providers also require to agree upon the scope, timing and duration of the audit: Kamatera DP Agreement Section 11.1., OVH Cloud DP Agreement Section 12, Slack DP Agreement Section 5.2.
[249] Google Cloud Data Processing and Security Terms (Customers) Section 7.5.3(b).

Furthermore, most of the CSPs tie the permission to conduct on-site audits to the obligation to sign an NDA. Oracle[250] and Rackspace[251] impose such obligations on customers. For some CSPs an NDA is also required if a customer requests access to auditing reports or certifications. AWS for example grant access to their 'Audit Reports' only upon written request and provided that the customer signed an NDA.[252] The survey also shows that some CSPs limit the frequency of customer audits to once a year.[253] Rackspace for instance charges the customer for every additional requested audit.[254]

The survey shows that CSPs tend to avoid granting each customer access to its infrastructure. This approach may not be entirely compliant with the GDPR, but as the Article 29 Working Party already claimed in 2012, it may be "impractical technically and can in some instances serve to increase risks to those physical and logical network security controls in place".[255] The survey, therefore, may reflect the practical implications of Article 28(3)(h). As a consequence, the customer (data controller) either accepts the CSPs' auditing reports and certifications as sufficient or bears the costs of additional audits, if permitted.

3.4.5. Data Breach Notification

This section addresses the interaction of CSPs and customers in the event of a data breach. As we already mentioned data processors are obliged to notify data controllers without undue delay[256] and the controller must notify the responsible supervisory authority within 72 hours after becoming aware of it.[257] Even though Article 33 of the GDPR does not explicitly mention the notification obligation of sub-processors, the processors' is obliged to impose the same legal responsibilities arising from the DPA to its sub-processors.[258] This might be especially important in the context of cloud services, considering their layered nature.[259]

[250] Oracle Cloud DP Agreement Section 10.2.
[251] Rackspace Cloud DP Addendum Section 3.2(a).
[252] AWS DP Addendum Section 10.3.
[253] For example Oracle Cloud DP Agreement Section 10.1.
[254] Rackspace Cloud DP Addendum Section 3.2(a).
[255] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, Section 4.2. [online] Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf [Accessed 7 May 2019].
[256] EU GDPR Art. 33(2).
[257] EU GDPR Art. 33(1).
[258] See EU GDPR Art. 28(3)(f) and (4).
[259] See Chapter 3.1.

The survey shows that most of the CSPs, describing a data breach as a "security incident", commit to notify their customers without undue delay. Only Oracle, however, determined a timeframe of maximum 24 hours.[260] The definition of a security incident also varies among the surveyed CSPs; whereas the majority defines it as the "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data",[261] other CSPs also subsume each event that is reasonably likely to result in such disclosure of access.[262]

The reviewed DPAs further revealed two different approaches in terms of controller notifications. First, some of the CSPs deny notifying the data controller about security incidents, which do not suffice to the exposure of personal data. Rackspace, for example, states that it "shall be under no obligation to notify routine security alerts in respect of the Customer Configuration (including without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers, or similar incidents)".[263] The GDPR does not clarify whether the processor or the controller is entitled to assess the likelihood of risk arising from a security incident.[264] Nonetheless, the data processor must identify a data breach before notifying it to the controller.

Second, some CSPs surveyed acknowledge the full responsibility of the controller "for complying with its obligations under incident notification laws applicable".[265] This might comply with the GDPR, but does not release the CSPs from the responsibility to notify and assist the controller in fulfilling its notification obligations.[266] Some CSPs offer their assistance, but at the expense of the customer.[267]

The customer (data controller) may benefit most from a broader obligation of the CSP to notify each security incident, irrespective of its likely risk, to enable the controller to take a substantiated decision before notifying to the supervisory authority.

[260] Oracle Cloud DP Agreement Section 11.3.
[261] EU GDPR At. 4(12), See for example AWS DP Addendum Section 17, Rackspace DP Addendum Section 1.
[262] For example Dropbox DP Agreement Section Exhibit B Section 4, Oracle Cloud DP Agreement Section 11.2.
[263] Rackspace DP Addendum Section 2.2.6.
[264] The Article 29 Working Party claims that "the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach."
[265] Microsoft Online Services Terms Section 'Security Incident Notification'.
[266] EU GDPR Art. 28(3)(f).
[267] IBM Cloud DP Addendum Section 10.2, Kamatera DP Agreement Section 8.2, Rackspace DP Addendum Section 2.2.6.

3.4.6. Liability and Indemnification

This section examines how CSPs attempt to allocate risk and liabilities in their agreements with customers (data controllers). As set out above,[268] liability can arise from individual claims, fines issued by a supervisory authority or contractual commitments.

The survey shows that the majority of CSPs does not include a separate liability cap in their DPAs, but prefer to do so in the general service agreement.[269] Most of the CSPs determine that their liability is limited to the fees paid by the customer prior to the event giving rise to the liability.[270] Some of these CSPs limit this amount to the fees paid 12 months prior to the incident,[271] or a multiple of the paid fees.[272] Other CSPs cap the liability to the lower of the paid fees or a certain amount. These amounts range from USD 100[273] to USD 100.000,[274] which seems very low considering the level of potential fines and penalties.[275] Separate liability caps subject to data breaches or higher general liability caps may be negotiated on a case-by-case basis, if the customer has sufficient bargaining strength. The analysis of these proprietary agreements exceeds the scope of this paper, but the intention of CSPs to minimize liability is evident.

The survey further shows that CSPs include indemnifications against any claims, damages, losses, liabilities, costs, and expenses suffered as a result of a data breach.[276] These provisions are problematic in light of the legal principle "ex turpi causa non oritur action", which deprives a plaintiff of pursuing legal remedies based on its illegal acts.[277] Therefore, it might be at least questionable whether an accused CSP should be entitled to pass the liability to the customer unless the customer is solely liable

[268] See Chapter 2.5.3.
[269] Oracle Cloud Services Agreement Section 7.
[270] See for example AWS Service agreement Section 1.10.9.
[271] IBM Cloud Service Agreement Section 6, Dropbox Business Agreement Section 8.1, Kamatera Terms of Use Section 15.
[272] For example IBM Cloud Service Agreement Section 6.
[273] Alibaba Cloud Membership Agreement Section 11.5.
[274] Dropbox Business Agreement Section 10.2.
[275] Please note that DLA Piper, a global law firm located in every continent, typically sees liability caps "varying from low millions of pounds to many multiples of the contract value.", See Blogs.dlapiper.com. (2019). *UK: Liability Limits for GDPR in commercial contracts – the law and recent trends | Privacy Matters*. [online] Available at: https://blogs.dlapiper.com/privacymatters/uk-liability-limits-for-gdpr-in-commercial-contracts-the-law-and-recent-trends/ [Accessed 9 May 2019].
[276] Dropbox Business Agreement Section 8.1, Alibaba Cloud Membership Agreement Section 10, AWS Service Terms Section 13.10, Dropbox Business Agreement Section 8.
[277] TheFreeDictionary.com. (2019). *ex turpi causa non oritur actio*. [online] Available at: https://legal-dictionary.thefreedictionary.com/ex+turpi+causa+non+oritur+actio [Accessed 9 May 2019].

or has accepted responsibility under the contract.[278] Nevertheless, small customers (data controllers) with insufficient bargaining powers must accept these terms and incur the risk that a court may enforce them.

The GDPR leaves enough leeway for CSPs to cap liability, recover fines and receive compensations. The limitations of the study render a final assessment impossible, but there is a strong tendency that liability and indemnification clauses mainly favor CSPs.

3.5. Summary

In this section we attempted to answer three questions; i) what is the influence of the GDPR on the contractual relationship of CSPs (data processors) and its customers (data controllers); ii) what value and implications do public statements and privacy policies have for potential customers; iii) Do CSPs provide sufficient contractual flexibility to support customers' GDPR compliance or do potential customers have to accept predetermined onerous terms in order to access these services.

We explained that cloud services enable customers to reduce costs and improve service quality through on-demand online access. We discovered that CSPs prefer to act as a data processor, which entails fewer responsibilities under the GDPR. We found that CSPs might not allow vendor agreements tailored to the customer's needs and that SMEs might have to accept predetermined terms.

We further established that public statements and privacy do not have any value to data controllers and that the only source of mutual commitments remains the contract with a CSP. We found that the critical sections in DPAs are the definition of controllers' instructions,[279] the appointment of sub-processors,[280] the security obligations imposed on both parties,[281] the controllers' contractual right to conduct or mandate audits,[282] the data breach notification obligations[283] as well as the allocation of liabilities and indemnifications. We explained that the GDPR either does not provide clear guidance or lacks implementation potential especially in the context of cloud services. We found that CSPs use their bargaining strength to impose predetermined terms on the customer. We argue that these onerous

[278] Blogs.dlapiper.com. (2019). *UK: Liability Limits for GDPR in commercial contracts – the law and recent trends | Privacy Matters*. [online] Available at: https://blogs.dlapiper.com/privacymatters/uk-liability-limits-for-gdpr-in-commercial-contracts-the-law-and-recent-trends/ [Accessed 9 May 2019].
[279] EU GDPR Art. 28(3)(a).
[280] EU GDPR Art. 28(2).
[281] EU GDPR Art. 32.
[282] EU GDPR Art. 28(3)(h).
[283] EU GDPR Art. 33(1) and 33(2).

terms would go diametrically against the initial intention of cloud services; namely low transaction costs and on-demand access to scalable resources. Small customers, which already have to invest heavily on internal compliance, face an increase of transaction costs which might outweigh benefits. Subsequently, the only logical consequence might be to consider alternative options, such as reverting to traditional outsourcing.

We can conclude that the GDPR assumes the existence of equal bargaining power between different parties. The analysis of third-party contracts in the Cloud Service Industry shows that this assumption may be unsuitable in today’s reality. Moreover, this chapter supports our initial argument that the GDPR mainly promotes data subjects’ rights and neglects to address business-to-business relationships. Clearer guidance in this context, could support controllers compliance and benefit data subjects in the long run.

CHAPTER FOUR: INNOVATION

4.1 Introduction

In Chapter Three we established the contractual framework between customers and CSPs as an example for the hostile legal environment created by the GDPR's provisions. The GDPR creates complications between data controllers and data processors by assuming equal bargaining power of each party. We found that the GDPR ignores the diversity of business models and demands the same level of compliance from each party involved. We argued that some of the GDPR's provisions cannot be translated into practice, especially in the cloud service context. The survey conducted in this paper revealed that CSPs impose predetermined onerous terms on their customers in order to pass the risk of non-compliance. Customers with lower bargaining strength, therefore, will face increased transaction costs due to heavy negotiations with CSPs. We concluded that the increased imbalance of costs and benefits may result in customers reverting back to traditional outsourcing. This conflicts with the EU Commission's assurance of a technology neutral-regulation, which "enables innovation to continue to thrive".[284]

This chapter will focus on blockchain technology as an alternative tool to achieve GDPR compliance. Although still in its infancy, blockchain technology has already provided exciting solutions in the areas of food safety, health care and global trade. This section will be divided into the following four sections. First, this chapter will outline the key characteristics of blockchain technology. Second, it will examine which aspects of blockchain technology resonate or conflict with the GDPR and assess which blockchain structure is most suitable to support data controllers GDPR compliance. Third, this chapter will provide a compliance guide for companies, considering to use blockchain technology to support their data security. Finally, section four contains a summary of the key findings.

4.2. Blockchain Technology

This section shall explain the key characteristics of blockchain technology, its classification into different blockchain models, and how these models can be deployed. An in-depth analysis of

[284] Europa.eu. (2015). *European Commission - PRESS RELEASES - Press release - Questions and Answers - Data protection reform*. [online] Available at: http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm [Accessed 11 May 2019].

blockchain technology is outside the scope of this paper, but this section will clarify its key concepts to build a foundation, which may be useful for the understanding of the subsequent sections.

In general, blockchain is a decentralized database technology. The technology enables a large number of natural or legal persons to store identical copies of the same cryptographically signed data records or transactions, so-called ‘blocks’, without any third-party intermediaries.[285] The crucial difference between blockchain and other services, such as cloud services, is that blockchain aims to avoid relying on a central institution or company to store and process data.[286]

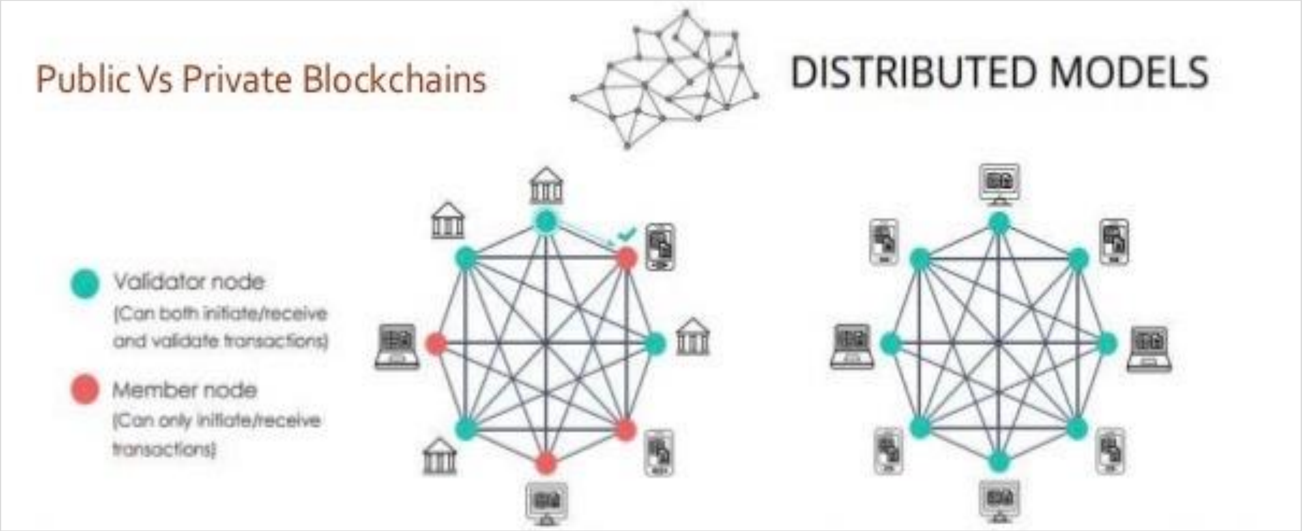
In a blockchain, each block contains the data records of users’ transactions and a hash value as a header, which includes the value of the previous block.[287] Further, blockchain technology is an append-only list, which means that users can only add transaction to the blockchain, after receiving the consent of the other users.[288] Every appended transaction must be verified ex-ante by the other server nodes. In this context nodes are devices storing the same data. The validation process requires the classification of users into two different types of nodes; the participating and the validating nodes (miners).[289] While participating nodes store a synchronized copy of the specific data and initiate transaction requests, the validating nodes are entitled to append data to the blockchain by applying a consensus mechanism.[290] The permission required to act as participating or validating node varies depending on the blockchain model.

As indicated in Figure 4.1, blockchains can generally be divided into public and private blockchains. In a public blockchain, every user can choose to become either a participating or validating node by installing the specific software and copying a full copy of the blockchain. Public blockchains can be defined as decentralized peer-to-peer networks, which enable anyone to participate with anonymous

[285] Eprints.soton.ac.uk. (2018). On Blockchains and the General Data Protection Regulation. [online] Available at: https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf [Accessed 20 May 2019].
[286] Hlengage.com. (2018). A guide to blockchain and data protection. [online] Available at: https://www.hlengage.com/_uploads/pdfs/DataProtection-BlockchainPaperNov16Low-res.pdf [Accessed 20 May 2019].
[287] Millard, C. (2018). *Blockchain and Law: Incompatible Codes?*. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3220406 [Accessed 22 May 2019].
[288] Eprints.soton.ac.uk. (2018). On Blockchains and the General Data Protection Regulation. [online] Available at: https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf [Accessed 20 May 2019].
[289] Eublockchainforum.eu. (2018). *Blockchain and the GDPR*. [online] Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf [Accessed 20 May 2019].
[290] Ibid, Consensus protocols constitute a set of rules and actions, which a block needs to follow to be accepted, to guarantee that the transaction or data records a valid and accurate. Also, consensus protocols compensate validating nodes to incentivize them. The consensus process, however, is a time and energy consuming task especially in public permission-less blockchains.

counterparties.[291] The access to a private blockchain, on the other hand, is dependent on permission by a single entity or a consortium, which means that only pre-approved parties can participate or validate nodes. The latter model limits the number of nodes dramatically, which renders it more efficient and flexible since consensus among the parties can be reached faster. Moreover, private blockchains might serve the purposes of the GDPR by providing tighter control over personal data on the blockchain.[292]

Figure 4.1 The difference between public and private blockchains


Public Vs Private Blockchains
DISTRIBUTED MODELS
Validator node
(Can both initiate/receive and validate transactions)
Member node
(Can only initiate/receive transactions)

Source: https://www.slideshare.net/Nitishsharma77/blockchain-73134967

In addition to the strict classification into public and private, blockchains could be designed as a combination of both structures, such as public permissioned blockchains. This alternative would allow all parties to participate, but only a pre-approved number of nodes could validate additional blocks.[293]

After the validation of a transaction or data record, the resulting block is irreversibly connected to the chronologically ordered blockchain. The immutable character of blockchain shall create trust, but simultaneously raises concerns with respect to GDPR compliance. Since appended data cannot, or only under extreme efforts,[294] be deleted, blockchain may be contradictory to specific provisions of the

[291] Finck, M. (2017). *Blockchains and Data Protection in the European Union*. [online] SSRN. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3080322 [Accessed 16 May 2019].
[292] Eublockchainforum.eu. (2018). *Blockchain and the GDPR*. [online] Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf [Accessed 20 May 2019].
[293] Ibid.
[294] Finck, M. (2017). *Blockchains and Data Protection in the European Union*. [online] SSRN. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3080322 [Accessed 16 May 2019].

GDPR, such as data subject's 'right to be forgotten'[295] or the 'right to rectification'.[296] The immutability, hence, constitutes one of the main obstacles to the reconciliation of blockchain and GDPR.[297]

This brief outline shows that blockchain technology shares similarities with the GDPR, comprising transparency, the intention to strengthen data subject rights and to provide increased security for personal data.[298] On the other hand, we have seen that some data subject rights, such as the right to be forgotten, seem to be in direct conflict with blockchain technology. Therefore, the subsequent section will address the interpretation of the GDPR in the blockchain context.

4.3. GDPR Compliance

This section attempts to examine the GDPR compliance of blockchain technology based on existing attempts of clarification. This section focuses predominantly on the CNIL's guidance paper on the "responsible use of the blockchain in the context of personal data".[299] Subsequently, this section will examine which type of blockchain might be most suitable to preserve data privacy.

Who is the Data Controller in a Blockchain?

As we have already established, the accountability of data controllers is a central issue of the GDPR. However, the GDPR principles were designed to apply to centrally managed service or product providers. The range of parties involved and the decentralized character of blockchain technology might complicate the identification of data controllers.[300] The CNIL concluded that participating nodes can be observed as data controllers, due to the ability to define the purpose and means of the processing.[301] In particular, the CNIL argues that a participant defines the objectives of the processing,

[295] EU GDPR Art. 17 obliges data controllers to delete data subjects' personal data under specific circumstances; e.g. the personal data is not needed anymore for the purpose it was stored and processed.

[296] EU GDPR Art. 16 grants data subjects the right to the rectification of inaccurate data with undue delay by the data controller.

[297] Forbes.com. (2018). Can Blockchain Help Brands Become GDPR Compliant?. [online] Available at: https://www.forbes.com/sites/andrewarnold/2018/11/20/can-blockchain-help-brands-become-gdpr-compliant/#63f36cc31203 [Accessed 20 May 2019].

[298] Anwar, H. and Anwar, H. (2018). *Blockchain GDPR Paradox: Rising Conflict Between Law and Technology?*. [online] 101 Blockchains. Available at: https://101blockchains.com/blockchain-gdpr/ [Accessed 20 May 2019].

[299] Cnil.fr. (2018). *Solutions for a responsible use of the blockchain in the context of personal data*. [online] Available at: https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf [Accessed 20 May 2019].

[300] Cnil.fr. (2018). *Solutions for a responsible use of the blockchain in the context of personal data*. [online] Available at: https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf [Accessed 20 May 2019].

[301] Ibid.

the data format, and how it uses the blockchain technology.[302] Further, the CNIL states that natural persons qualify as data controllers if the processing is related to commercial activity and more importantly, legal persons if they register personal data on a blockchain.[303]

On a private blockchain, this assumption may be easier to justify because the number of possible entities defining the purpose and means of data processing is limited to one single entity or a consortium. In a consortium of companies interacting on a private permissioned blockchain, the CNIL suggests identifying one company as data controller up front.[304]

On a public permission-less blockchain, which lacks a central intermediary, the task of identifying the data controller might be much more complex. The task of identifying the data controller has not been explicitly clarified by the CNIL nor the European Data Protection Board (EDPB) and the EU Commission.[305] As discussed above, public blockchains enable the interaction with a random number of anonymous users, transferring equal rights to every node. Therefore the nodes in a public blockchain may categorically be classified as data controllers.[306] This would raise considerable concerns with regards to the number, location and identification of all nodes.[307] This paper further assesses the facilitation of GDPR compliance through blockchain technology through private blockchains, which allows for easier identification of a single data controller. The role of public blockchains' participants would have to be assessed on a case-by-case basis until data protection authorities or the EDPB provide further guidance.

Who is the Data Processor in a Blockchain?

Having established that participating nodes can be qualified as data controllers at least in private blockchains the classification of validating nodes remains. Validating nodes or miners solely validate the transaction requests of participating nodes and therefore cannot be classified as data controllers.[308] The fulfilment of a data controller's instruction, however, could qualify miners as data processors. For

[302] Ibid.
[303] Ibid.
[304] Ibid.
[305] Eublockchainforum.eu. (2018). *Blockchain and the GDPR*. [online] Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf [Accessed 20 May 2019].
[306] Finck, M. (2017). *Blockchains and Data Protection in the European Union*. [online] SSRN. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3080322 [Accessed 16 May 2019].
[307] Ibid.
[308] Cnil.fr. (2018). *Solutions for a responsible use of the blockchain in the context of personal data*. [online] Available at: https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf [Accessed 20 May 2019].

instance, a consortium of financial institutions may appoint one single responsible data controller. This would mean that the remaining institutions validate the transactions on the private blockchain acting as miners and a data processor.[309] As a result the members of a consortium may enter into an agreement, defining their mutual responsibilities and duties.[310]

Under which Format the Personal Data shall be registered?

The main question is how the immutability of data stored on a blockchain would coexist with the GDPR. The obligation in data controllers' to keep personal data for no longer than is necessary for the processing[311] and to erase,[312] correct[313] and amend[314] personal data upon request by data subjects' seems to stand in direct conflict with the immutable character of blockchain technology. To address possible compliance solutions, we must clarify which data on a blockchain qualifies as personal data under Article 4(1) of the GDPR.

On a blockchain, there can be two different types of personal data, including the identifiers of participating and validating nodes and additional data, which can be related to other individuals.[315] The CNIL argues that the identification of participants and miners is possible by their visible public key, which constitutes an allegedly random series of alphanumeric numbers. The CNIL further argues that the private key, which is linked to the public key and only accessible by the participant, can also serve as an identifier. The CNIL concluded that the data minimization[316] of these identifiers cannot be optimized, which implies that their retention period complies with the GDPR's data retention obligation.[317]

The additional personal data processed on a blockchain must be kept in a format with the least impact on the data subjects' rights due to Article 25 of the GDPR.[318] The CNIL explains that the most

[309] Ibid.

[310] Eublockchainforum.eu. (2018). *Blockchain and the GDPR*. [online] Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf [Accessed 20 May 2019].

[311] EU GDPR Art. 5(e).

[312] EU GDPR Art. 17.

[313] EU GDPR Art. 16.

[314] Ibid.

[315] Cnil.fr. (2018). *Solutions for a responsible use of the blockchain in the context of personal data*. [online] Available at: https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf [Accessed 20 May 2019].

[316] EU GDPR Recital 39, the principle of "data minimization" requires a data controller to store and process only the minimum amount of data necessary for the processing purpose.

[317] Cnil.fr. (2018). *Solutions for a responsible use of the blockchain in the context of personal data*. [online] Available at: https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf [Accessed 20 May 2019].

[318] See Chapter 2.4.6., 'Data protection by design'.

favorable format might be the storage of personal data outside the blockchain.[319] For personal data stored on the blockchain, the CNIL recommends to avoid clear text and use a so-called commitment[320] or a hash function with a key.[321] As a last resort, encryption is recommended to ensure sufficient confidentiality.[322] The storage of personal data on the blockchain, however, is mainly unexplored and data protection authorities and the EDPB have failed to issue guidance in this area. Unless complete anonymization of personal data, which results in the inapplicability of the GDPR, can be guaranteed, the processing on a blockchain should be avoided. Hashing, for example, was classified as pseudonymized data by the Article 29 Working Party[323] and encryptions can mostly be decrypted,[324] which triggers the application of the GDPR[325] and hence increased compliance risk.[326] We can conclude that, until sufficient anonymization techniques are clarified by data protection authorities, the EDBP or in court, the nature of data stored on a blockchain must be assessed individually.[327]

How to ensure effective exercise of rights?

There are major benefits using blockchain technology, comprising improved transparency and data security, in comparison with traditional fully centralized data management systems. However, the incompatibility with blockchains' immutability could cause complications with respect to data subjects' rights; especially the right to erasure.[328] Although the use of commitments or a keyed-hash function could allow an action similar to erasure,[329] the erasure of personal data is technically

[319] Cnil.fr. (2018). *Solutions for a responsible use of the blockchain in the context of personal data*. [online] Available at: https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf [Accessed 20 May 2019].

[320] A "commitment" allows to both prove what has been committed to and other the other hand renders it impossible to recognise the data behind the proof without further information.

[321] "Hashing" transforms a random input into a 64 characters long (SHA-256 algorithm) number, which represents the input.

[322] Cnil.fr. (2018). *Solutions for a responsible use of the blockchain in the context of personal data*. [online] Available at: https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf [Accessed 20 May 2019].

[323] Ec.europa.eu. (2014). *Article 29 Data Protection Working Party , Opinion 05/2014 on Anonymisation Techniques*. [online] Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf [Accessed 21 May 2019].

[324] Hlengage.com. (2018). *A guide to blockchain and data protection*. [online] Available at: https://www.hlengage.com/_uploads/pdfs/DataProtection-BlockchainPaperNov16Low-res.pdf [Accessed 20 May 2019].

[325] See Chapter 2.4.1.

[326] Hlengage.com. (2018). A guide to blockchain and data protection. [online] Available at: https://www.hlengage.com/_uploads/pdfs/DataProtection-BlockchainPaperNov16Low-res.pdf [Accessed 20 May 2019].

[327] Bakermckenzie.com. (2018). *EU Blockchain Observatory says Blockchain is not incompatible with GDPR | Insight | Baker McKenzie*. [online] Available at: https://www.bakermckenzie.com/en/insight/publications/2018/11/eu-blockchain-observatory-blockchain-gdpr [Accessed 27 May 2019].

[328] EU GDPR Art. 17.

[329] The CNIL explains that in a commitment scheme the element allowing verification can be erased and make the proof of the committed information inaccessible. The same effect might be achievable in a keyed-hash function by deleting its secret key.

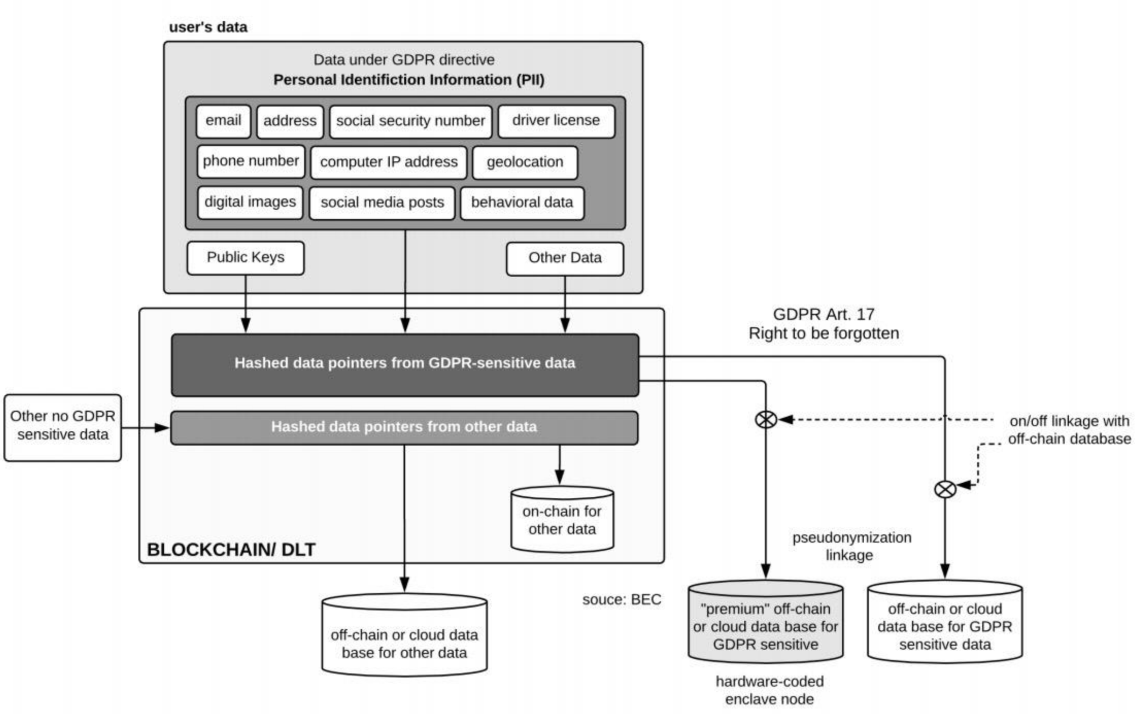
impossible on a blockchain. Again, the preferred solution, therefore, might be a data storage outside the blockchain.[330]

Therefore we may refrain from questioning whether there is a GDPR compliant blockchain, but rather accept that there can only be a compliant use of blockchain technology. The most favorable blockchain model may be a private permissioned blockchain due to easier identification of a data controller or joint controllers and the better control of data transfers outside the EU.[331]

Prior research has developed two different variations of private blockchains to create compliance with the GDPR. First, the Queen Mary University proposes a private blockchain with an integrated "right to be forgotten".[332] Second, scholars and blockchain platform providers, such as IBM, argue that a hybrid of a private blockchain and an "off-chain", which stores the personal data externally, might be most suitable.[333] The former solution intends to delete decryption keys of data encrypted on the blockchain, which makes the personal data inaccessible. This idea, which is supported by the reports of the CNIL, is much more promising in terms of upholding the purposes of blockchain technology,[334] but since it does not delete data, it will need approval by data protection authorities and the EDPB. Figure 4.2 shows an example of the second alternative, which integrates cloud-based or distributed data storage outside the blockchain and simultaneously stores a proof or hash of the stored personal data on the blockchain. The hash cannot be reconstructed to the underlying personal data. This solution, however, neglects the idea of blockchain technology as the single source of truth and may require counterparties to preserve their own records.[335]

[330] Cnil.fr. (2018). *Solutions for a responsible use of the blockchain in the context of personal data*. [online] Available at: https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf [Accessed 20 May 2019].
[331] Ibid.
[332] Jolt.richmond.edu. (2018). *Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers*. [online] Available at: https://jolt.richmond.edu/files/2018/11/Michelsetal-Final-1.pdf [Accessed 21 May 2019], states that an
[333] Eublockchainforum.eu. (2018). *Blockchain and the GDPR*. [online] Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf [Accessed 20 May 2019], Enigma.co. (2015). *Decentralizing Privacy: Using Blockchain to Protect Personal Data*. [online] Available at: https://enigma.co/ZNP15.pdf [Accessed 20 May 2019].
[334] See Chapter 4.2.
[335] Hlengage.com. (2018). *A guide to blockchain and data protection*. [online] Available at: https://www.hlengage.com/_uploads/pdfs/DataProtection-BlockchainPaperNov16Low-res.pdf [Accessed 20 May 2019].

Figure 4.2 GDPR Compliant Off-Chain Model



user's data
Data under GDPR directive
Personal Identifiction Information (PII)
email
address
social security number
driver license
phone number
computer IP address
geolocation
digital images
social media posts
behavioral data
Public Keys
Other Data
Hashed data pointers from GDPR-sensitive data
Other no GDPR sensitive data
Hashed data pointers from other data
on-chain for other data
BLOCKCHAIN/ DLT
off-chain or cloud data base for other data
souce: BEC
GDPR Art. 17
Right to be forgotten
on/off linkage with off-chain database
pseudonymization linkage
"premium" off-chain or cloud data base for GDPR sensitive
hardware-coded enclave node
off-chain or cloud data base for GDPR sensitive data

Source: Claudio Lima (2018), Blockchain by Design, How Decentralized Blockchain Internet will Comply with GDPR Data Privacy, https://blockchain.ieee.org/images/files/pdf/blockchain-gdpr-privacy-by-design.pdf

In summary, the notion of blockchain technology being entirely incompatible with current data privacy laws is not correct. Indeed, blockchain can not only improve transparency and data security in comparison with traditional fully centralized data management systems but could also be architected in a GDPR compliant way.[336] However, current solutions might attempt to circumvent the initial purpose – the elimination of centralized data storage - of blockchain technology, by suggesting the external storage of personal data on an off-chain.[337] Nevertheless, the proposed alternative blockchain architectures require a deep understanding of blockchain technology in order to implement a GDPR compliant blockchain architecture.[338]

[336] Blockchain.ieee.org. (2018). *Blockchain by Design, How Decentralized Blockchain Internet will Comply with GDPR Data Privacy*. [online] Available at: https://blockchain.ieee.org/images/files/pdf/blockchain-gdpr-privacy-by-design.pdf [Accessed 21 May 2019].

[337] Eublockchainforum.eu. (2018). *Blockchain and the GDPR*. [online] Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf [Accessed 20 May 2019], Enigma.co. (2015). *Decentralizing Privacy: Using Blockchain to Protect Personal Data*. [online] Available at: https://enigma.co/ZNP15.pdf [Accessed 20 May 2019],

[338] Ibid.

Companies with the intention to use blockchain to support GDPR compliance must first assess if one of the two outlined solutions is feasible for their specific needs. The assumption that the use of blockchain technology principally equals data privacy and automatically leads to a more secure and cheaper business model is misleading.[339] The next section shall outline the necessary considerations for companies willing to the use of blockchain technology to increase data protection.

4.4. Guide to Compliance

The current lack of clarification by data protection authorities, government agencies and the EDPB result in an omnipresent tension between blockchain technology and data privacy. Although this paper and in particular this section cannot resolve this tension, it seeks to provide key principles for companies which intend to use or design blockchain technology.

Companies should be aware of how data will be used to create value for its users. In particular, a business must assess which kind of data will be processed, the purpose and duration of the processing and its legal basis.[340] Subsequently, companies might, under consideration of data protection by design and default, architect its individual solution.[341] As we have seen, in business-to-business relationships, each party could deal with its users' data via an off-chain and transact with the business partner on a private blockchain. This example, however, cannot blindly be applied to every data processing scenario. Hence, companies must first recognize the appropriateness of using blockchain technology in order to implement it in their data management structure.[342]

Furthermore, the storage of personal data on the blockchain should be avoided.[343] In particular, this recommendation is essential for companies which can be identified as a data controller in a blockchain environment, which will mainly be the case in private blockchains. Previously we outlined a non-exhaustive list of possible data concealments,[344] there seems to be an underlying consensus between

[339] Eublockchainforum.eu. (2018). *Blockchain and the GDPR*. [online] Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf [Accessed 20 May 2019].
[340] Ibid.
[341] Ibid.
[342] Ibid, Cnil.fr. (2018). *Solutions for a responsible use of the blockchain in the context of personal data*. [online] Available at: https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf [Accessed 20 May 2019].
[343] Eublockchainforum.eu. (2018). *Blockchain and the GDPR*. [online] Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf [Accessed 20 May 2019].
[344] See Chapter 4.2.1.

the CNIL[345] and scholars[346] that these techniques should preferably be used to store immutable proofs of the existence of personal data on the blockchain rather than the data itself.[347]

Therefore, it is preferable to store personal data on an off-chain.[348] In case the storage on a blockchain is inevitable, such as in the financial sector, the blockchain solution must allow tight control of processed data. A permissioned private blockchain, consisting of a small consortium, could serve to restrict the personal data.[349] Consortium members could agree to contractual terms determining the respective responsibilities and duties towards end-users. Further, a separate legal entity could be formed to act as a data controller on behalf of the consortium, while the remaining members would act as validating nodes (data processors).[350]

Companies should first conduct a feasibility check, before considering to use blockchain technology. The implementation of blockchain technology may demand high levels of computational resources and technical understanding. These demanding requirements and the necessity of a GDPR compliance assessment on a case-by-case basis lead to the conclusion that under the current data privacy framework, companies should be cautious with the use of blockchain.

4.5. Findings

In this chapter, we explained that the GDPR is tailored to regulate centralized data storage management and that blockchain technology, which is characterized by decentralization, does not fall outside its scope. Blockchain technology uses obfuscations of data, including hashing and encryption, but according to current interpretations, these techniques pseudonymize but do not anonymize data. This triggers the application of the GDPR, which results in increased non-compliance risk. It would seem

[345] Cnil.fr. (2018). *Solutions for a responsible use of the blockchain in the context of personal data*. [online] Available at: https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf [Accessed 20 May 2019].

[346] Ibáñez, L., O'Hara, K. and Simperl, E. (2018). On Blockchains and the General Data Protection Regulation. [online] Eprints.soton.ac.uk. Available at: https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf [Accessed 21 May 2019], describes the technique, using hashes as proof of existing data, as "hashing out", Enigma.co. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. [online] Available at: https://enigma.co/ZNP15.pdf [Accessed 20 May 2019], Finck, M. (2017). *Blockchains and Data Protection in the European Union*. [online] SSRN. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3080322 [Accessed 16 May 2019].

[347] Eublockchainforum.eu. (2018). *Blockchain and the GDPR*. [online] Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf [Accessed 20 May 2019].

[348] Ibid, See Chapter 4.2.1.

[349] Ibid.

[350] See Chapter 4.2.

obvious to refrain from storing personal data on a blockchain, which would be possible for personal data itself, but not for public and private keys, which qualify as personal data under the GDPR.[351]

We further established that some aspects of blockchain technology are in direct conflict with the provisions of the GDPR. In particular, the right to erasure and the principle of data minimization seem not in line with the presumed immutability of blockchain technology. We explained that developers and scholars work on possibilities to implement the "right to be forgotten" into the blockchain, but that the status quo only allows for alternative tailor-made solution, such as an off-chain. Moreover, future technological developments rely on cryptography, which could cause long-term insecurity.[352]

In addition, blockchain technology impedes the distribution of accountability and liability as the roles of the participating parties must be analyzed on a case-by-case basis. The identification of one single data controller or joint controllers is essential under the GDPR, but highly sophisticated in the context of blockchain technology.

We discovered that the GDPR poses an obstacle to blockchain solutions and its range of benefits, which can be considered controversial since it could support companies' ability to provide data security. Legislators, therefore, will need to provide new legislative acts or more explicit guidelines about the use of blockchain under the scope of EU data privacy laws. Keeping this in mind, it is encouraging that the EU Data Protection Supervisor has endeavored to examine the underlying tensions with blockchain technology, according to its Annual Report 2018.[353] Legislators might have to apply a purposive approach, which shall reflect the need to interpret the GDPR as being business model and technology neutral, in order to avoid the preferential treatment of other technologies over blockchain technology.[354]

Some scholars even support the development in the direction of complete data sovereignty.[355] This means that blockchain might change or unsettle the foundation of the GDPR's underlying conception

[351] Finck, M. (2017). *Blockchains and Data Protection in the European Union*. [online] SSRN. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3080322 [Accessed 16 May 2019].
[352] Ferrari, V. (2018). *EU Blockchain Observatory and Forum Workshop on GDPR, Data Policy and Compliance*. [online] SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3247494 [Accessed 22 May 2019].
[353] Edps.europa.eu. (2018). *European Data Protection Supervisor, 2018 Annual Report*. [online] Available at: https://edps.europa.eu/sites/edp/files/publication/ar2018_en.pdf [Accessed 21 May 2019].
[354] Ibid., Hildebrandt, M. (2013). *Data Protection by Design and Technology Neutral Law*. [online] Works.bepress.com. Available at: https://works.bepress.com/mireille_hildebrandt/62/ [Accessed 21 May 2019].
[355] Finck, M. (2017). *Blockchains and Data Protection in the European Union*. [online] SSRN. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3080322 [Accessed 16 May 2019].

of singular data silos, data controllers and processors, being responsible for data management.[356] Instead of sharing personal data with companies, data subjects could allow companies to access the data from the blockchain by sharing a key, which could be revoked at the data subject's discretion. The company would be restricted to the use of personal data without being able to change or misinterpret the original data. Giving the ownership of data back to the user would relieve companies of the obligation to store all this data in its own data storage.[357] The implementation of this solution, however, would require that the shared keys do not qualify as personal data under the GDPR, which triggers compliance risks. We explained that recent clarifications by the CNIL argue exactly that public and private keys of nodes constitute personal data. This matter, however, seems at least debatable and requires further clarification.[358]

As we have seen, blockchain technology is currently not capable of serving as an alternative tool to achieve GDPR compliance. This is due to many uncertainties regarding the identification and obligations of data controllers and processors, the anonymization of data, data minimization, the right to erasure and data protection by design and default. We showed that only private blockchains in combination with an off-chain might serve as a sufficient alternative to achieve GDPR compliance at this moment. However, we argue that the "off-chain" architecture attempts to circumvent the initial ideas of blockchain technology. The GDPR does not accommodate, but rather impedes the underlying intentions of blockchain technology. As a consequence, only companies, with a deep understanding of blockchain technology and its vulnerabilities related to the GDPR, may be equipped to create a blockchain architecture to fit their specific needs. The potential legal issues of implementation and the associated costs render GDPR compliance through blockchain technology almost impossible and might not be desirable on a cost/benefit analysis. Taking all of these points into account there is little room for further exploration.

[356] Ibid.

[357] Forbes.com. (2018). *Can Blockchain Help Brands Become GDPR Compliant?*. [online] Available at: https://www.forbes.com/sites/andrewarnold/2018/11/20/can-blockchain-help-brands-become-gdpr-compliant/#66dead861203 [Accessed 21 May 2019].

[358] Rampone, F. (2019). *Data Protection in the Blockchain Environment: GDPR is not a hurdle to DLT solutions*. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3383619 [Accessed 22 May 2019].

CHAPTER FIVE: CONCLUSION

The contractual framework between data controllers and data processors has become an increasingly important issue since the introduction of the GDPR. In this paper, we analyzed the impact of the GDPR on these third-party relationships, with a primary focus on the cloud service industry.

In this sense, the paper asked the following four questions; first, does the GDPR provide a level playing field for data processors and data controllers in the context of contract negotiations. Second, do the current EU data protection laws accommodate novel technologies. Third, do the responsible bodies, including the Article 29 Working Party of the EDPB offer sufficient guidance for data controllers and processors in order to facilitate contract negotiations. Fourth, does blockchain technology constitutes a valid alternative solution to achieve GDPR compliance.

In Chapter II, we explained that the EU regulators decided to implement the GDPR to harmonize existing data protection laws of its Member States and to adjust the EU's regulatory framework to contemporary technological developments. The GDPR expanded the scope of data protection to companies outside of the EU and obliged both data controllers and data processors to promote compliance proactively. We saw that the GDPR, and especially Article 28, entails a range of ambiguous provisions applicable to the relationship of data controllers and processors; especially in the areas with increasing technological challenges, including the identification of data breaches, frequent audits and security arrangements. In this context, we emphasized that despite the newly introduced statutory obligations for data processors, unclear contractual arrangements in DPAs can cause legal implications for the data controller. We argued that the lack of clarification leaves space for extensive negotiations and concluded that the final terms of an agreement would depend on the bargaining strength of each party.

In Chapter III, we applied these findings to the contractual framework between data customers (data controllers) and CSPs (data processors). The analysis of publicly available DPAs, service agreements and terms of use from 17 selected CSPs revealed that it is common practice for CSPs to exploit their superior negotiating position by imposing onerous terms on customers. We explained that customers, however, bear the main responsibility of compliance and are obliged to "use only processors providing sufficient guarantees to implement appropriate technical and organizational measures".[359] We clarified

[359] EU GDPR Art. 28(1).

that customers' acceptance of CSPs' terms shifts the risk to the customer (data controller) and might result in financial, operational and reputational ramifications. We argued that increasing transaction costs might force smaller customers to reconsider their outsourcing strategy and revert to traditional outsourcing methods, which are more secure.

Moreover, we showed that the GDPR failed to address business-to-business relationships. Based on the empirical survey, we showed that the contractual requirements under Article 28 are difficult to reconcile with cloud computing since the GDPR assumes the data controller to be the party instructing and controlling the data processors' processing activities. However, in the cloud service industry, the reality differs dramatically from this assumption. The survey proved that especially in the cloud service industry the data processors establish the rules of processing through standardized DPAs or service agreements, which confirmed that many of the GDPR's provisions are difficult to apply to novel technologies. We showed that the GDPR fails to accommodate innovation as it can hardly be implemented in the cloud service context.

Besides, we could not identify any helpful guidance provided by the Article 29 Working Party of the EDPB to resolve uncertainties about the contractual requirements under the GDPR. These advisory bodies, however, should have scrutinized the new relationship between data controllers and processors in the absence of clear guidance by the GDPR.

In Chapter IV we examined whether blockchain technology can support companies' GDPR compliance. Upon review of available literature, it became apparent that these two phenomenon share similar objectives, such as the strengthening of data subject rights and increased data security. On the other hand, there is direct conflict between blockchain technology and the GDPR. In particular, blockchains' immutability contradicts the GDPR's right to erasure and principle of minimization. Scholars, therefore, unanimously recommend the use of a hybrid between a permissioned private blockchain and an off-chain, which stores the personal data, as GDPR compliant blockchain solution.

We argued that uncertainties about critical concepts of the GDPR would require additional clarifications. As such, only companies with a deep understanding of blockchain and its vulnerabilities to the GDPR may be capable of creating a compliant blockchain architecture which fits their specific needs. However, we argued that the suggested blockchain architectures attempt to circumvent the GDPR's provisions, which stand in direct conflict with the immutable character of blockchain technology, but simultaneously neglect blockchains' fundamental purpose, to decentralize data silos.

We concluded that the shortcomings, such as potential legal implications and costs, of current blockchain solutions outweigh the benefits concerning data privacy. The paper, therefore, concluded that there is limited space for further exploration.

This paper proves that the tension between data controllers and their service providers, created by the GDPR's new regulatory framework, results in increased transaction costs and an increased risk of financial, operational and reputational ramifications for data controllers. The EU legislator and its advisory body, the Article 29 Working Party and the EDPB, missed the opportunity to address business-to-business relations in the GDPR or relevant opinion papers. However, more guidance and clarity could resolve uncertainties related to the GDPR's contractual requirements, especially related to new emerging technologies, such as IoT and cloud computing. Also, blockchain technology has not proved to be a solid solution to this problem, since it can only be compliant with the GDPR by circumventing its key aspects, especially its immutability, and lacks marketability on a cost/benefit analysis.

Appendix A

GDPR Terms and Definitions

Term	Definition	Sources[360]
Data subject	The GDPR qualifies “an identifiable natural person”, irrespective of its nationality or residence, as a data subject. Legal persons, such as entities and corporations, fall outside this scope of application and thus information on legal persons do not enjoy protection of the GDPR.	EU GDPR Article 4(1) Calder, A. (2016). *EU GDPR: A Pocket Guide, School's edition* (p. 17). IT Governance Publishing. Available at: https://ebookcentral.proquest.com/lib/uvtilburg-ebooks/detail.action?docID=4647636
Personal data	“any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;” The GDPR provides a listing of personal data, which can be used to identify a data subject. However, due to the non-exhaustive character of the listing every kind of data, which can be used to identify a data subject, qualifies as personal data.	EU GDPR Article 4(1) Calder, A. (2016). *EU GDPR: A Pocket Guide, School's edition* (p. 17). IT Governance Publishing. Available at: https://ebookcentral.proquest.com/lib/uvtilburg-ebooks/detail.action?docID=4647636
Personal data breach	“a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;” The GDPR’s primary focus is to avoid personal data breaches, but always in consideration of that more general data breaches, falling outside the scope of the could ultimately lead to personal data breaches, depending on the data being leaked.	EU GDPR Article 4(12) Calder, A. (2016). *EU GDPR: A Pocket Guide, School's edition* (p. 17). IT Governance Publishing. Available at: https://ebookcentral.proquest.com/lib/uvtilburg-ebooks/detail.action?docID=4647636
Data Controller	“the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; “ These are the legal entities, which receive personal data directly from data subjects. In theory a legal entity would even remain data controller if it provides parts of its online services via third party cloud service providers, because it determines why and how the data is processed by the service provider. Data controller, however, do not automatically own personal data.	EU GDPR Article 4(7) Hintze, M. (2018). Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR (p.1.). Journal of Internet Law (Wolters Kluwer), August 2018. Available at: https://ssrn.com/abstract=3192721

[360] An exhaustive list of definitions used in the GDPR can be found under Article 4, Available at: https://gdpr.algolia.com/gdpr-article-4 [Accessed 10 April 2019]

	The concepts of data controller and data owner must be considered separate and are not dependent on each other, although they correlate frequently. Further there has to be a clear distinction between data controller and data processor, because of different obligations imposed by the GDPR.	
Data Processor	“a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;” Every time a data controller refrains from processing data itself, the third parties collecting and processing the data on behalf of the data controller are data processors under the GDPR.	EU GDPR Article 4(8)
Processing	“any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;” The extremely vague definition of data processing might cover every interaction with personal data. Therefore data controller and processors must be aware of the data spectrum they are responsible for to comply with the GDPR.	EU GDPR Article 4(2), EU GDPR Art 51-59 Calder, A. (2016). *EU GDPR: A Pocket Guide, School's edition* (p. 17). IT Governance Publishing. Available at: https://ebookcentral.proquest.com/lib/uvtilburg-ebooks/detail.action?docID=4647636
Supervisory Authority	“an independent public authority which is established by a Member State pursuant to Article 51;” The public body officially responsible for data breaches is the supervisory authority of each EU Member State. For instance, the national supervisory authority of France is the Commission Nationale de l'Informatique et des Libertés – CNIL, of Germany is the Bundesbeauftragte für den Datenschutz und die Informationsfreiheit and of the Netherlands is the Autoriteit Persoonsgegevens.	EU GDPR Article 4(21)
Third Party	“means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;” Both data controller might use the services of a third party, which do not qualify as data controller or processor themselves. These parties are defined as third parties under the GDPR.	EU GDPR Article 4(10)

Appendix B

Obligations of Organizations deploying Services from Cloud Service Providers

Obligation	Services from Processors	Services from Controllers
Contractual commitments	Contracts with terms complying with Article 28	Generally not required
Data Security	Service provider must meet same security requirements under Article 32, irrespective of its classification as a processor or a controller;	
Data breach notification	Provider required to notify Enterprise pursuant to Article 33(2); Enterprise subsequently responsible for notifying supervisory authority and data subjects pursuant to Articles 33 and 34	Provider responsible for notifying supervisory authorities and data subjects directly pursuant to Articles 33 and 34
Cross-border data transfers	Enterprise may use either controller-to-controller or controller-to-processor model clauses, or can rely on other transfer mechanisms (such as the provider being Privacy Shield certified); provider responsible for its own compliance with Articles 44-49 whether acting as a processor or a controller (but certain derogations under Art. 49 do not apply to processors)	
Data protection by design and default	Article 28 contract will specify data retention	Provider responsible for determining and disclosing its own data retention; enterprise should review provider's policy as part of due diligence
Documenting data processing activities	Enterprise & provider must each document its own data processing per Article 30; provider acting as processor subject to slightly narrower set of obligations under Art. 30, but additional items must be documented in Art. 28 contract	Provider responsible for Article 30 documentation (no specific requirement for enterprise)
Data protection impact assessments (DPIAs)	Enterprise must complete DPIA for "high risk" data processing per Article 35; provider must assist enterprise as needed under Article 28(3)(f)	Provider responsible to completing its own DPIA for "high risk" data processing per Article 35
Cooperating with supervisory authority	Either the enterprise or the provider can be required to cooperate directly with a supervisory authority, whether acting as a data processor or a data controller, per Article 31	

Source: Hintze, M. (2018). Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR. [online] SSRN. Available at: https://ssrn.com/abstract=3192721

Appendix C

GDPR Documentation Requirements

Category	Controllers	Processors
Name and contact details of the parties involved	"[T]he name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer." Art. 30(1)(a).	"[T]he name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer." Art. 30(2)(a).
Description of processing	"[T]he purposes of the processing; a description of the categories of data subjects and of the categories of personal data; the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations." Art. 30(1)(b)-(d).	"[T]he categories of processing carried out on behalf of each controller." Art. 30(2)(b). The contract must also document "the subject-matter . . . of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects." Art. 28(3).
International data transfers	"[W]here applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards." Art. 30(1)(e).	"[W]here applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards." Art. 30(2)(c).
Data Retention	"[W]here possible, the envisaged time limits for erasure of the different categories of data." Art. 30(1)(f).	The contract must document "the duration of processing." Art 28(3). The contract further must stipulate the processor will return or delete all personal data at the end of the provision of services. Art. 28(3)(g).
Data Security	"[W]here possible, a general description of the technical and organizational security measures referred to in Article 32(1)." Art. 30(1)(g).	"[W]here possible, a general description of the technical and organizational security measures referred to in Article 32(1)." Art. 30(2)(d)

Source: Hintze, M. (2018). Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR. [online] SSRN. Available at: https://ssrn.com/abstract=3192721

Appendix D

List of Cloud Service Providers included in the Survey and Accompanying Documents

No	Provider	Service	Legal documents
1	Alibaba Group	Alibaba Cloud	• GDPR Addendum to Alibaba Cloud International Website Membership Agreement, 25 May 2018[361] • Alibaba Cloud International Website Terms of Use, 25 May 2018[362]
2	Amazon	Amazon web services	• AWS Service Terms, 30 April 2019[363] • AWS Data Processing Addendum[364] • AWS Customer Agreement[365]
3	Box	Box	• Box Data Processing Addendum incorporating: GDPR, Box Processor Binding Corporate Rules, and Privacy Shield
4	Cisco Meraki	Cisco Meraki	• Cisco Meraki EU Data Processing Addendum [366]
5	Dropbox	Dropbox	• Business Agreement, 17 April 2018[367] • Data Processing Agreement, 25 May 2018[368] • List of Sub-Processors[369]
6	Facebook	Facebook Workplace Premium	• Workplace premium GDPR addendum[370]

[361] Alibabacloud.com. (2018). GDPR Addendum to Alibaba Cloud International Website Membership Agreement - Membership Agreement| Alibaba Cloud Documentation Center. [online] Available at: https://www.alibabacloud.com/help/faq-detail/72443.htm [Accessed 6 May 2019].

[362] Alibabacloud.com. (2018). Alibaba Cloud International Website Terms of Use - Terms of Use| Alibaba Cloud Documentation Center. [online] Available at: https://www.alibabacloud.com/help/faq-detail/42417.htm?spm=a2c63.q38357.a3.1.4da652d6HqCizA [Accessed 6 May 2019].

[363] Amazon Web Services, Inc. (2019). AWS Service Terms. [online] Available at: https://aws.amazon.com/service-terms/ [Accessed 6 May 2019].

[364] D1.awsstatic.com. (2019). AWS GDPR Data Processing Addendum. [online] Available at: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf [Accessed 6 May 2019].

[365] Amazon Web Services, Inc. (2019). AWS Customer Agreement. [online] Available at: https://aws.amazon.com/agreement/ [Accessed 6 May 2019].

[366] Meraki.cisco.com. (2018). Cisco Meraki EU Data Processing Addendum. [online] Available at: https://meraki.cisco.com/lib/pdf/meraki_eu_dpa.pdf [Accessed 6 May 2019].

[367] Dropbox. (2018). Dropbox - Terms. [online] Available at: https://www.dropbox.com/en_GB/privacy#business_agreement [Accessed 6 May 2019].

[368] Assets.dropbox.com. (2018). Dropbox Data Processing Agreement. [online] Available at: https://assets.dropbox.com/documents/en/legal/data-processing-agreement-dfb-013118.pdf [Accessed 6 May 2019].

[369] Assets.dropbox.com. (2019). *List of Sub-Processors*. [online] Available at: https://assets.dropbox.com/documents/en/legal/subprocessors-dfb-013118.pdf [Accessed 7 May 2019].

[370] Workplace.com. (2018). Workplace Data Processing Addendum. [online] Available at: https://www.workplace.com/legal/Workplace_GDPR_Addendum?fbclid=IwAR1guXj0NloNIKwswz04SyoavGBnm9ln18Oz5uvqwOlw20ic0tfmnIT-idc [Accessed 6 May 2019].

			- Workplace premium Privacy Policy, 25 May 2018[371]
7	Google	Google Cloud Platform	- Google Cloud Platform Terms of Service[372] - Google Cloud Service Specific Terms, 9 April 2019[373] - Data Processing and Security Terms (Customers), 25 May 2018[374] - Google Cloud Platform Sub-processors, 7 March 2019[375]
8	IBM	IBM Cloud	- IBM Cloud Service Agreement, April 2019[376] - Data Processing Addendum, 2 March 2019[377] - IBM Data Security and Privacy Principles, May 2018[378] - Statement of Limited Warranty, 22 May 2018[379]
9	Kamatera	Kamatera	- Terms of Use[380] - Data Processing Agreement[381]
10	Microsoft	Microsoft Azure	- Online Service Terms, 2 May 2019[382] (include Microsoft's core privacy and security commitments, data processing terms, Model Clauses, and our GDPR Terms)

[371] Workplace.facebook.com. (2018). Workplace Premium Privacy Policy. [online] Available at: https://workplace.facebook.com/legal/FB_Work_Privacy [Accessed 6 May 2019].

[372] Google Cloud. (2018). Google Cloud Platform Terms of Service | Google Cloud Platform Terms | Google Cloud. [online] Available at: https://cloud.google.com/terms/ [Accessed 6 May 2019].

[373] Google Cloud. (2019). Google Cloud Service Specific Terms. [online] Available at: https://cloud.google.com/terms/service-terms [Accessed 6 May 2019].

[374] Google Cloud. (2018). Data Processing and Security Terms (Customers). [online] Available at: https://cloud.google.com/terms/data-processing-terms [Accessed 6 May 2019].

[375] Google Cloud. (2019). Google Cloud Platform Subprocessors. [online] Available at: https://cloud.google.com/terms/subprocessors [Accessed 6 May 2019].

[376] Ibm.com. (2019). IBM Cloud Services Agreement. [online] Available at: https://www.ibm.com/support/customer/csol/contractexplorer/cloud/csa/gb-en/10 [Accessed 6 May 2019].

[377] Ibm.com. (2019). IBM Data Processing Addendum. [online] Available at: https://www.ibm.com/support/customer/csol/terms/?ref=Z126-7870-02-03-2019-zz-en [Accessed 6 May 2019].

[378] ibm.com. (2018). IBM Data Security and Privacy Principles. [online] Available at: https://www-03.ibm.com/software/sla/sladb.nsf/pdf/7745WW3/$file/Z126-7745-WW-3_05-2018_en_US.pdf [Accessed 6 May 2019].

[379] Www-01.ibm.com. (2019). IBM Machine warranties and license information - Overview. [online] Available at: https://www-01.ibm.com/support/docview.wss?uid=isg3T1025361 [Accessed 9 May 2019].

[380] Kamatera.com. (n.d.). Kamatera | Terms and Conditions | Terms of Use. [online] Available at: https://www.kamatera.com/Terms_of_Use [Accessed 6 May 2019].

[381] Kamatera.com. (2018). Kamatera Data Processing Agreement. [online] Available at: https://www.kamatera.com/GDPR_%7Cfamp%7C_Data_Processing [Accessed 6 May 2019].

[382] Microsoftvolumelicensing.com. (2019). Microsoft Online Services Terms. [online] Available at: https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31 [Accessed 6 May 2019].

11	Oracle	Oracle Cloud	- Online Oracle Cloud Service Agreement, 24 January 2018[383] - Data Processing Agreement. 27 July 2018[384]
12	OVH cloud	OVH cloud	- Terms of Service (OVH US LLC), 25 May 2018[385] - Data Processing Agreement[386]
13	Rackspace	Rackspace Cloud	- Data Processing Addendum[387]
14	Salesforce	Salesforce Cloud	- Data Processing Addendum, November 2018[388]
15	Slack	Slack	- Data Processing Agreement [389]
16	SAP	SAP Cloud Patform	- General Terms and Conditions, October 2018[390] - Data Processing Agreement [391]
17	VMware	VMware	- Terms of Service, 19 November 2019[392] - Data Processing Addendum, 8 January 2019[393]

[383] Oracle.com. (2018). Oracle Cloud Service Agreement. [online] Available at: https://www.oracle.com/assets/cloud-csa-v012418-uk-eng-4419923.pdf [Accessed 6 May 2019].

[384] Oracle.com. (2018). Data Processing Agreement for Oracle Cloud Services. [online] Available at: https://www.oracle.com/assets/data-processing-agreement-072718-5029569.pdf [Accessed 6 May 2019].

[385] Us.ovhcloud.com. (2018). Terms of Service - Legal | OVHcloud. [online] Available at: https://us.ovhcloud.com/legal/terms-conditions [Accessed 6 May 2019].

[386] Ovh.co.uk. (n.d.). Data Processing Agreement. [online] Available at: https://www.ovh.co.uk/support/termsofservice/Data%20Processing%20Agreement_UK.pdf [Accessed 6 May 2019].

[387] Rackspace Hosting. (n.d.). Rackspace Data Processing Addendum. [online] Available at: https://www.rackspace.com/information/legal/GSAdataprocessingaddendum_MC [Accessed 6 May 2019].

[388] C1.sfdcstatic.com. (2018). Salesforce Data Processing Addendum. [online] Available at: https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/legal/Agreements/data-processing-addendum.pdf [Accessed 6 May 2019].

[389] A.slack-edge.com. (n.d.). Slack Data Processing Addendum. [online] Available at: https://a.slack-edge.com/d6f09/marketing/downloads/legal/slack-data-processing-addendum.pdf [Accessed 6 May 2019].

[390] SAP. (2018). GENERAL TERMS AND CONDITIONS FOR SAP CLOUD SERVICE. [online] Available at: https://www.sap.com/about/trust-center/agreements/cloud/cloud-services.html?search=General Terms and Conditions&sort=title_asc#pdf-asset=88f84a7c-217d-0010-87a3-c30de2ffd8ff&page=1 [Accessed 6 May 2019].

[391] SAP. (2018). Personal Data Processing Agreement for SAP Cloud Services. [online] Available at: https://www.sap.com/about/trust-center/agreements/cloud/cloud-services.html?search=Data Processing&sort=title_asc&tag=language:english#pdf-asset=480677ba-fd7c-0010-87a3-c30de2ffd8ff&page=5 [Accessed 6 May 2019].

[392] Vmware.com. (2019). TERMS OF SERVICE. [online] Available at: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/vmware-cloud-services-universal-tos.pdf [Accessed 6 May 2019].

[393] Vmware.com. (2019). Data Processing Addendum. [online] Available at: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/vmware-data-processing-addendum.pdf [Accessed 6 May 2019].

REFERENCES

PRIMARY SOURCES

2010/87/: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) (Text with EEA relevance).

2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271)Text with EEA relevance).

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.

Article 29 Data Protection Working Party Opinion 05/2012 on Cloud Computing.

Article 29 Data Protection Working Party , Opinion 05/2014 on Anonymisation Techniques.

Commission of the European Communities on the protection of Individuals In relation to the processing of personal data In the Community and Information security, COM 90 (314) final (September 1990)

European Data Protection Supervisor, *2018 Annual Report*.

Fair Credit Reporting Act of 1970 15 USC §1681.

Privacy Act of 1974 5 USC 552a.

Proposal for a 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 (General Data Protection Regulation), COM(2012) 11 final (January 2012).

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

SECONDARY SOURCES

BOOKS

EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide - Second Edition. (2017). IT Governance Ltd., pp.18-21.

Calder, A. (n.d.). EU GDPR: A Pocket Guide, School's edition. IT Governance Publishing, pp.14-19.

González Fuster, G. (2014). Emergence of personal data protection as a fundamental right of the EU. Springer.

Lindqvist, J. (2017). New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?. 26th ed. Springer, pp.45–63.

PUBLICATIONS AND WEBSITES

Albrecht, J. (2013). *EUDataP: State of the Union*. [online] Media.ccc.de. Available at: https://media.ccc.de/v/30C3_-_5601_-_en_-_saal_2_-_201312281400_-_eudatap_state_of_the_union_-_jan_philipp_albrecht#t=315 [Accessed 17 Apr. 2019].

Anwar, H. and Anwar, H. (2018). *Blockchain GDPR Paradox: Rising Conflict Between Law and Technology?*. [online] 101 Blockchains. Available at: https://101blockchains.com/blockchain-gdpr/ [Accessed 20 May 2019].

Bakermckenzie.com. (2018). EU Blockchain Observatory says Blockchain is not incompatible with GDPR | Insight | Baker McKenzie. [online] Available at: https://www.bakermckenzie.com/en/insight/publications/2018/11/eu-blockchain-observatory-blockchain-gdpr [Accessed 27 May 2019].

Becher, S. and Benoliel, U. (2019). Law in Books and *Law in Action: The Readability of Privacy Policies and the GDPR*. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3334095 [Accessed 4 May 2019].

Blockchain.ieee.org. (2018). *Blockchain by Design, How Decentralized Blockchain Internet will Comply with GDPR Data Privacy*. [online] Available at: https://blockchain.ieee.org/images/files/pdf/blockchain-gdpr-privacy-by-design.pdf [Accessed 21 May 2019].

Blogs.dlapiper.com. (2019). *UK: Liability Limits for GDPR in commercial contracts – the law and recent trends* | *Privacy Matters*. [online] Available at: https://blogs.dlapiper.com/privacymatters/uk-liability-limits-for-gdpr-in-commercial-contracts-the-law-and-recent-trends/ [Accessed 9 May 2019].

Brook, D. (2018). GDPR puts vendor contracts in the security spotlight. *Computer Fraud & Security*, [online] 2018(4), pp.5-7. Available at: https://www.sciencedirect.com/science/article/pii/S1361372318300319?via%3Dihub [Accessed 20 Apr. 2019].

CISPE - The Voice of Cloud Infrastructure Service Providers in Europe. (2019). *CISPE - Code of Conduct, for Cloud Infrastructures Services*. [online] Available at: https://cispe.cloud/code-of-conduct/ [Accessed 8 May 2019].

Cloud Security Alliance. (2018). *Cloud Security Alliance Issues Code of | Cloud Security Alliance*. [online] Available at: https://cloudsecurityalliance.org/articles/cloud-security-alliance-issues-code-of-conduct-self-assessment-and-certification-tools-for-gdpr-compliance/ [Accessed 8 May 2019].

Cnil.fr. (2017). *FACEBOOK sanctioned for several breaches of the French Data Protection Act | CNIL*. [online] Available at: https://www.cnil.fr/en/facebook-sanctioned-several-breaches-french-data-protection-act [Accessed 18 Apr. 2019].

Cnil.fr. (2018). *Solutions for a responsible use of the blockchain in the context of personal data*. [online] Available at: https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf [Accessed 20 May 2019].

Cnil.fr. (2019). *Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC.*. [online] Available at: https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf [Accessed 4 May 2019].

Cnil.fr. (2019). *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC | CNIL*. [online] Available at: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc [Accessed 9 May 2019].

de Hert, P. and Czerniawski, M. (2016). *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*. [online] Oxford Academic. Available at: https://academic.oup.com/idpl/article/6/3/230/2447252 [Accessed 17 Apr. 2019].

Deloitte United States. (2018). *2018 Global Outsourcing Survey*. [online] Available at: https://www2.deloitte.com/us/en/pages/operations/articles/global-outsourcing-survey.html [Accessed 29 May 2019].

DLA Piper. (n.d.). *EU General Data Protection Regulation - Key changes | DLA Piper Global Law Firm*. [online] Available at: https://www.dlapiper.com/en/netherlands/focus/eu-data-protection-regulation/key-changes [Accessed 19 Apr. 2019].

Enigma.co. (2015). *Decentralizing Privacy: Using Blockchain to Protect Personal Data*. [online] Available at: https://enigma.co/ZNP15.pdf [Accessed 20 May 2019].

Eprints.soton.ac.uk. (2018). *On Blockchains and the General Data Protection Regulation*. [online] Available at: https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf [Accessed 20 May 2019].

Eublockchainforum.eu. (2018). *Blockchain and the GDPR*. [online] Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf [Accessed 20 May 2019].

Eucoc.cloud. (2018). *Home: EU Cloud CoC*. [online] Available at: https://eucoc.cloud/en/home.html [Accessed 8 May 2019].

Europa.eu. (2015). European Commission - Press release - Questions and Answers - Data protection reform. [online] Available at: http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm [Accessed 11 May 2019].

Gellman, R. (2019). *Fair Information Practices: A Basic History*. [online] SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020 [Accessed 16 Apr. 2019].

Grant, H., Lambert, A. and Pickering, K. (2016). *Data Protection Day—data processors and the GDPR - Fieldfisher*. [online] Fieldfisher.com. Available at: https://www.fieldfisher.com/publications/2016/02/data-protection-day-data-processors-and-the-gdpr#sthash.eCrAKFYy.dpbs [Accessed 19 May 2019].

Ferrari, V. (2018). *EU Blockchain Observatory and Forum Workshop on GDPR, Data Policy and Compliance*. [online] SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3247494 [Accessed 22 May 2019].

Finck, M. (2017). *Blockchains and Data Protection in the European Union*. [online] SSRN. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3080322 [Accessed 16 May 2019].

Forbes.com. (2018). *Can Blockchain Help Brands Become GDPR Compliant?*. [online] Available at: https://www.forbes.com/sites/andrewarnold/2018/11/20/can-blockchain-help-brands-become-gdpr-compliant/#66dead861203 [Accessed 21 May 2019].

Gartner IT Glossary. (n.d.). *IaaS - Infrastructure as a Service - Gartner IT Glossary*. [online] Available at: https://www.gartner.com/it-glossary/infrastructure-as-a-service-iaas [Accessed 1 May 2019].

Hildebrandt, M. (2013). *Data Protection by Design and Technology Neutral Law*. [online] Works.bepress.com. Available at: https://works.bepress.com/mireille_hildebrandt/62/ [Accessed 21 May 2019].

Hintze, M. (2018). *Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR*. [online] SSRN. Available at: https://ssrn.com/abstract=319272 [Accessed 19 Apr. 2019].

Hlengage.com. (2018). *A guide to blockchain and data protection*. [online] Available at: https://www.hlengage.com/_uploads/pdfs/DataProtection-BlockchainPaperNov16Low-res.pdf [Accessed 20 May 2019].

Hon, W. and Millard, C. (2013). *Cloud Computing vs. Traditional Outsourcing – Key Differences*. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2200592 [Accessed 1 May 2019].

Hon, W. and Millard, C. (2013). *Control, Security, and Risk in the Cloud*. [online] Oxfordscholarship.com. Available at: https://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780199671670.001.0001/acprof-9780199671670-chapter-2 [Accessed 8 May 2019].

Hoofnagle, C., van der Sloot, B. and Zuiderveen Borgesius, F. (2019). *The European Union General Data Protection Regulation: What It Is And What It Means*. [online] SSRN. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3254511 [Accessed 17 Apr. 2019].

Lee, P. (2019). *How do EU and US privacy regimes compare? - Privacy, Security and Information Law Fieldfisher*. [online] Privacylawblog.fieldfisher.com. Available at: https://privacylawblog.fieldfisher.com/2014/how-do-eu-and-us-privacy-regimes-compare [Accessed 16 Apr. 2019]

Iapp.org. (2015). *Article 29 Working Party Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing*. [online] Available at: https://iapp.org/media/pdf/resource_center/wp232_%20Cloud-Computing_09-2015.pdf [Accessed 1 May 2019].

Iapp.org. (2016). *GDPR: Killing cloud quickly?*. [online] Available at: https://iapp.org/news/a/gdpr-killing-cloud-quickly/ [Accessed 1 May 2019].

Iapp.org. (2017). *Surprising stats on third-party vendor risk and breach likelihood*. [online] Available at: https://iapp.org/news/a/surprising-stats-on-third-party-vendor-risk-and-breach-likelihood/ [Accessed 1 May 2019].

Ibáñez, L., O'Hara, K. and Simperl, E. (2018). *On Blockchains and the General Data Protection Regulation*. [online] Eprints.soton.ac.uk. Available at: https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf [Accessed 21 May 2019].

Ico.org.uk. (n.d.). *Guidance on the use of cloud computing*. [online] Available at: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf [Accessed 25 Apr. 2019].

Ico.org.uk. (2018). *Some basic concepts*. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/ [Accessed 6 Mar. 2019].

Jolt.richmond.edu. (2018). *Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers*. [online] Available at: https://jolt.richmond.edu/files/2018/11/Michelsetal-Final-1.pdf [Accessed 21 May 2019].

Journal.binarydistrict.com. (2018). *Can Blockchain Operators Comply with EU Data Protection Law?*. [online] Available at: https://journal.binarydistrict.com/can-blockchain-operators-comply-with-eu-data-protection-law/ [Accessed 1 May 2019].

Kamarinou, D., Millard, C. and Hon, W. (2015). *Privacy in the Clouds: An Empirical Study of the Terms of Service and Privacy Policies of 20 Cloud Service Providers*. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2646447 [Accessed 4 May 2019].

Kamarinou, D., Millard, C. and Oldani, I. (2019). *Compliance as a Service*. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3284497 [Accessed 10 May 2019].

Kantei.go.jp. (1983). *OECD Recommendation Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. [online] Available at: https://www.kantei.go.jp/jp/it/privacy/houseika/dai11/11siryou5.html [Accessed 18 Apr. 2019].

Lincke, K. and Nourbakhsh, A. (2017). An Analysis of the GDPR's Effects on the Future of Cloud Outsourcing. *Computer Law Review International*, [online] 18(6). Available at: https://www.degruyter.com/downloadpdf/j/cri.2017.18.issue-6/cri-2017-0604/cri-2017-0604.pdf [Accessed 22 May 2019].

Millard, C. (2018). *Blockchain and Law: Incompatible Codes?*. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3220406 [Accessed 22 May 2019].

Nvlpubs.nist.gov. (2011). *The NIST Definition of Cloud Computing*. [online] Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [Accessed 2 May 2019].

Oprysk, L. (2016). *The Forthcoming General Data Protection Regulation in the EU: Higher Compliance Costs Might Slow Down Small and Medium-Sized Enterprises' Adoption of Infrastructure as a Service*. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3019917 [Accessed 4 May 2019].

Pantlin, N., Wiseman, C. and Everett, M. (2018). Supply chain arrangements: The ABC to GDPR compliance —A spotlight on emerging market practice in supplier contracts in light of the GDPR. *Computer Law & Security Review*, [online] 34(4), pp.881-885. Available at: https://www.sciencedirect.com/science/article/pii/S0267364918302516 [Accessed 20 Apr. 2019].

Pdpjournals.com. (2010). *Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor"*. [online] Available at: https://www.pdpjournals.com/docs/88016.pdf [Accessed 20 May 2019].

Pdpjournals.com. (2017). *Article 29 Data Protection Working Party - Guidelines on Personal data breach notification under Regulation 2016/679*. [online] Available at: https://www.pdpjournals.com/docs/887876.pdf [Accessed 19 Apr. 2019].

Rampone, F. (2019). *Data Protection in the Blockchain Environment: GDPR is not a hurdle to DLT solutions*. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3383619 [Accessed 22 May 2019].

Reedsmith.com. (n.d.). *GDPR series: Outsourcing contracts — all changed, changed utterly | Perspectives | Reed Smith LLP*. [online] Available at: https://www.reedsmith.com/en/perspectives/2018/03/gdpr-series-outsourcing-contracts--all-changed-changed-utterly [Accessed 20 Apr. 2019].

Richard Watson. (2018). *Stop Agonizing Over GDPR Opt-In Emails and Start Thinking about How Your Use of Cloud Impacts GDPR Compliance - Richard Watson*. [online] Available at: https://blogs.gartner.com/richard-watson/stop-agonising-gdrp-opt-emails-start-thinking-cloud-providers/ [Accessed 24 May 2019].

Robinson, N., Graux, H., Botterman, M. and Valeri, L. (2009). *Review of the European Data Protection Directive*. [online] RAND Europe, pp.26-37. Available at: https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf [Accessed 17 Apr. 2019].

Rubinstein, I. and Petkova, B. (2018). *The International Impact of the General Data Protection Regulation*. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3167389 [Accessed 19 Apr. 2019].

https://www.fieldfisher.com/media/3993765/the-gdprs-impact-on-the-cloud-service-provider-as-a-processor-mark-webber-privacy-data-protection.pdf. (2018). *PDPjournal*, 16(4).

The IT Law Wiki. (n.d.). *Traditional outsourcing*. [online] Available at: https://itlaw.wikia.org/wiki/Traditional_outsourcing [Accessed 1 May 2019].

TheFreeDictionary.com. (2019). *ex turpi causa non oritur actio*. [online] Available at: https://legal-dictionary.thefreedictionary.com/ex+turpi+causa+non+oritur+actio [Accessed 9 May 2019].