The Legal Status of a Controller and a Processor of a Cloud Service Provider Under the GDPR in the Context of the Complete Protection to the Data Subject.

Tilburg Institute for Law, Technology and Society (TILT) LL.M. Law and Technology (2017 – 2018)

Cholada Ratanachuesakul
ANR: 328853 / SNR: 2006994

Thesis Supervisor: Hosna Sheikhattar
Second Reader: Dr N. N. Purtova
May 2018

Table of Contents

Introduction

Chapter 1 – Cloud Computing and Data Protection

Chapter 4 – Conclusion

Chapter 1

INTRODUCTION

1. BACKGROUND AND SIGNIFICANCE

"Law always lags behind technology".[1] This saying has become increasingly true in the fast-paced digitization era. When it comes to the field of data protection, its certainty with regard to the legal status of the actors involved is of prevalent importance. This means that the law should be constructed in a way that unambiguously explains the obligation and responsibility of the actors to sustain compliance with the law; the controllers who have the power to determine the purposes and the means for the processing of personal data[2] need to know what these obligations are, as well as what is the responsibility that they will take on to fulfill their legal compliance. The processor, who processes the data on behalf of the controller, is also responsible for ensuring the legitimacy of the processing procedure.[3]

However, in the situation of cloud computing service, there might be problems in identifying the legal status of either a controller or a processor. Nowadays, most of the services are operating in a cloud platform such as Google Docs, Dropbox and various mobile applications. The ambiguity in the legal status needs to be solved because data subjects need to be able to distinguish who will be responsible in case of damages, for example, when processing their personal data: data subjects need to be able to pinpoint a liable party whom they can address in seeking remedies. Additionally, any entity who is a controller or a processor needs to be able to identify its legal status in order to comply with the law and conduct a legal processing procedure. This necessity enhances the pertinence of better providing data subjects with clearer structures in the legal status of controller and processor to make sure that personal data remains protected, and also to guarantee the flow of the cloud service's business.

This thesis focuses on the operating of the cloud computing service within the context of the upcoming General Data Protection Regulation. Moreover, the legal status of the cloud provider is also examined. Such an assessment will be conducted within the scope of the upcoming Regulation (EU) 2016/679[4] or General Data Protection Regulation (the "GDPR" hereinafter),[5] which will come into force in May 25 2018. The aim of this thesis is to clarify the legal status of cloud providers. Overall, this legal assessment will be followed with the aim to reach a complete protection of data subject.

2. RESEARCH QUESTION AND ROADMAP

The central research question of this thesis is as follows:

[1] Michael I. Meyerson, '*Virtual Constitutions: The Creation of Rules for Governing Private Networks*' Harvard Journal of Law & Technology, Vol.8 Issue 1, 1994) 129.

[2] See Articles 4(7) GDPR.

[3] Recital 46 and Article 17 Directive 95/46/EC and Recital 39 and Article 28(c) and 32 GDPR.

[4] Regulation (EU) 2016/679 of the European Parliament and of The Council of 27 April 2016 on the protection of natural person 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).

[5] Herein referred as "GDPR".

“What is the legal status of the cloud service provider in the GDPR and does the legal status of a cloud provider in the GDPR effectively provide a complete protection for data subjects?”

The sub-questions of the thesis are as followed;

1. What is cloud computing?
2. How can cloud computing be a threat to data protection?
3. Who are controllers and processors under the DPD and the GDPR and what are their obligations and rights?
4. What is the legal status of cloud service providers under the DPD and the GDPR?
5. Does the current legal status of the cloud service provider and its implications lead to the complete protection of data subjects?

The consideration will be based upon the aim to provide complete protection to the data subject.[6] [7]

3. LITERATURE REVIEW

Cloud services have become scalable and cost-effective ways to manage resources.[8] Cloud service can be used to provide computing-service models, including processing and storage service models to users on the online platforms.[9] Yet the cloud service also comes with the inherent problem of its nature and the relationship with the data protection law. The application of the law to the context of cloud service structure is unclear about the role and the exact legal status of a cloud provider. The applicability of the legal status to the cloud service context is hard to map out because the cloud service contains many distinctive characteristics, such as designs of virtualized infrastructure which shared among multiple user including several add-ons service provider.[10] Many key legal issues with cloud computing have been discussed in literatures, but most topics are discussed from the perspective of the cloud service business and not from the viewpoint of the data subject. The focus is placing on the cloud service provider since it is a fast-growing business and draws much public attention for a more data protection attentive version. The key legal issues problem of cloud service can be divided into two main categories according to the Article 29 Working Party[11][12]: lack of control and lack of transparency.

First, lack of control includes several issues that go from lack of interoperability, lack of intervenability, and lack of integrity, to lack of confidentiality and lack of

[6] Case C-131/12 Google Spain SL. v. Agencia Española de Protección de Datos (AEPD) (ECJ 13 May 2014).

[7] The notion of the principle of complete protection of data subject will be further discussed in chapter 4.

[8] The European Network and Information Security Agency (ENISA), Cloud computing: Benefits, risks and recommendations for information security (December 2012) <https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security> accessed 18 November 2017.

[9] J. Cave, and others, ‘Regulating the Cloud: More, Less or Different Regulation and Competing Agendas’ (2012) TRPC <http://paper.sssrn.com/abstract=2031695> accessed 18 November 2017.

[10] Christopher Millard, ‘*Cloud Computing Law*’ (OUP, Oxford 2013) 89.

[11] Herein referred as “29WP”

[12]Article 29 Data Protection Working Party 03/12/EN WP196, Opinion 05/2012 on Cloud Computing

isolation.[13] Lack of interoperability or vendor lock-in is a case in which cloud providers face difficulties when shifting data from one provider to another.[14] Lack of integrity and confidentiality are both caused due to a shared infrastructure of the cloud which can lead to conflicts of interest between users within the same cloud. Another instance in which this infrastructure becomes problematic is when one processing procedure in the cloud is subject to law enforcement request and, thus, the entire cloud is forced to disclose the data within that cloud. Referring to the lack of intervenability, this results from the complexity in the cloud, which usually complies with several service providers and thus makes it hard for users to intervene or make changes. An example of this is the take-it-or-leave-it service level agreements (SLAs),[15] which seems to offer an already structured cloud where it leaves little to no room for customers to negotiate.[16] Another example can be a circumstance in which the cloud provider does not sufficiently assist the customer to exercise their own rights—such as the right to access, delete or correct data. In a different respect, lack of isolation arises when the cloud provider exploits its control and links all of the customer's information.

The second category in which the problem can be divided, lack of transparency, pertains issues caused by the natures of the cloud services, since such natures affect the accountability in the cloud.[17] Problems of transparency also occur when there are many joint processing situations across multinational companies.[18] Particularly, and in line with the focus of this thesis, transparency has decreased due to the ambiguity in the legal status of a controller and a processor the author wishes to refer to. Such a circumstance is usually identified as the problem of binary distinctions.[19] Prior to the GDPR, the Directive recognized that the two most important roles in processing procedure are the controller, which is the entity who defines the mean and purpose of the processing procedure,[20] and

[13] Ibid 5.

[14] The European Network and Information Security Agency (ENISA) (n 8), J. Cave and others (n 9), and A29WP, 'WP196' (n 12).

[15] A29WP, 'WP196' (n 12) 8.

[16]F. Halper, and others, '*Hybrid Cloud for Dummies*' (John Wiley & Sons Inc. 2012) 28; B. Freedman, 'Cloud services – guidelines for service level agreements European'(Lexology, 16 October 2014) <https://www.lexology.com/library/detail.aspx?g=7202771e-3161-401b-aa87-1d550999bdb3> accessed 19 November 2017.

[17] Article 29 Data Protection Working Party 0836-02/10/EN WP179, Opinion 8/2010 on applicable law and A29WP, 'WP196' (n 14), and Halper, and others (n 18) 28, and Freedman (n 18) 72.

[18]L. Moerel, 'Back to basics: when does EU data protection law apply?' (2011) 1(2) IDPL 92–110 <https://doi.org/10.1093/idpl/ipq009> accessed 10 October 2017.

[19] W. Kuan Hon, Christopher Millard and Ian Walden, 'Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2' (2011) 2 (1) IDPL 3 <https://ssrn.com/abstract=1794130> accessed 17th October 2017; Brendan Van Alsenoy, 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC' (2012) 28 Computer Law & Security Review 25-43 <https://ac.els-cdn.com/S0267364911001828/1-s2.0-S0267364911001828-main.pdf?_tid=dab0ab39-e5b0-45a5-bbd9-f7e5a15bdd32&acdnat=1526905339_050d4c9e3ac56ae8d4c05835c32347e1> accessed on 20 May 2018; Patrick Van Eeck, and Maarten Truyens, 'Privacy and social networks' (2010) 26 Computer Law & Security Review 535-546 <https://ac.els-cdn.com/S0267364910001093/1-s2.0-S0267364910001093-main.pdf?_tid=204ffa74-ab8b-46e5-92ee-209db59d4adc&acdnat=1526910933_7893972cb0105b2b933a96dda5d1ac99> accessed on 20 May 2018; Christopher Kuner, '*European Data Protection Law Corporate Compliance and Regulation*' (2nd edn, Oxford University Press, 2007) 71.

[20] Article 2 (d) DPD.

the processor, who acts on behalf of a controller.[21] These two are crucial for the allocation of obligation and liability, the application of applicable law, and the compliance with other provision under the GDPR.[22]

According to the Directive, a controller has the main responsibility to ensure the compliance with data protection law and is mainly liable for any damages that are presented in a form of strict liability.[23] The factors that determine controllership are the determinative influence over the processing procedure and the object of such influence, which are the purpose and means of the processing procedure.[24] Conversely, a processor is a "mere executor" who simply acts under the controller's instruction without any direct liability placed upon it.[25]

With such an interpretation of the legal status, much criticism has been raised regarding the fact that, in practice, these statuses are not easily applicable because of the complexity in the business's role and in the responsibilities of a processing procedure.[26] Together with the outdated processing model, the issue of binary distinction has been brought to the fore since, nowadays, a processing procedure cannot clearly outline the distinction between controller and processor.[27] Thus, such an issue impedes the free flow of the businesses operation, with which it is debatable who a controller or a processor is in a particular processing procedure.[28] This situation has been addressed particularly in relation to cloud services by W. Kuan Hon, who explains that when cloud providers merely provide platform infrastructures and leave the rest of the responsibilities to the customer—responsibilities such as determining the mean and purpose of the processing and operating the processing procedure[29]—the legal status of actors, whether controller or processor, must be spelled out clearly. This needs to be done so as to show transparency in the processing process and to be easily understood by the data subject, whose data has been processed. Moreover, structural changes that occur without customer notifications and complex outsourcing chains with multiple processors and subcontractors have been

[21] Article 2 (e) DPD.

[22] Van Alsenoy, 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC' (n 19).

[23] Brendan Van Alsenoy, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation' (JIPITEC 2016) <http://www.jipitec.eu/issues/jipitec-7-3-2016/4506/van_alsenoy_liability_under_eu_data_protection_law_jiptec_7_3_2016_271.pdf> accessed 20 May 2018; Van Alsenoy, 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC' (n 19).

[24] Article 29 Data Protection Working Party 00264/10/EN WP 169, Opinion 1/2010 on the concepts of controller and processor" 9, 13

[25] Van Alsenoy, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation' (n 25).

[26] Ibid and Kuner (n 19) 71-72.

[27] Van Alsenoy, 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC' (n 19); Hon, Millard and Walden, (n 19) 24; Van Eecke and Truyens (n 19); Kuner (n 19) 71.

[28] Information Commissioner's Office (ICO), 'The Information Commissioner's (United Kingdom) response to the European Commission's consultation on the legal framework for the fundamental right to protection of personal data in the European Union' (European Commission, 31 December 2009) 9 <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/public-consultation/2009/pdf/contributions/public_authorities/ico_uk_en.pdf> accessed on 15 May 2018; Van Eecke and Truyens (n 19)

[29] Hon, Millard and Walden, (n 19) 3.

defined as legal problems with the cloud providers in the report of the WP29.[30] While the above-mentioned issues are considered to be a major concern in the context of cloud computing, the problem of binary distinction or the problem of the legal status of the cloud provider and customer have not been thoroughly discussed in the literature. Most reports on the legal status of the cloud providers have assumed that the cloud providers take on the roles of the processors and the customers take on the roles of controllers.[31]

At present, most legal issues are resolved using negotiation through contracting methods,[32] such as User Licensing Agreements (ULAs) and Service Level Agreement (SLAs). These resolutions confirm Christopher Millard's idea [33] that the law is insufficient for the sphere of cloud computing because it is allowing the parties to negotiate the controllership contractually. This can be detrimental for the data subject or party who does not possess the negotiation power and, thus, has to receive much of the obligation than it actually contributed to due to its lacking in power of negotiation. Furthermore, the allocation of obligation to ensure an efficient protection of personal data that the law is aiming for can be distorted by this imbalance in control. With the approach of the GDPR, this concern is increasing, especially with the multiple obligations and liabilities toward a processor which have been introduced by the GDPR for the first time.[34] It is expected in the business field that the GDPR will mitigate legal issues that the Directive cannot adequately address in relation to cloud computing services. Those concerns are presented in the survey conducted by the public consultation of the European Commission.[35] [36] The survey's results showed that the respondents feel that the Directive is not fit to address liability issues with cloud computing frameworks and should provide more transparency concerning the security and protection of users' data.[37] Although it is evident that efforts have been made in public and private fields to create a platform for compliance with the GDPR, the results of the applicability and compliance still need to be observed.

This thesis aims to incorporate the issues of legal status in the cloud service that have not been assessed thoroughly from the perspective of the complete protection of a data subject. It will try to evaluate the GDPR from the perspective of the complete protection of the data subject to solve the legal status issue of the cloud provider which has not been mentioned in the literature before. Moreover, it will also suggest which points that can be amended or changed in the GDPR to provide better protection for the data subject. This will contribute to diminishing the gap in the literature where there is no

[30] 29WP, 'WP196' (n 12).

[31] 29WP, 'WP196' (n 12); The European Network and Information Security Agency (ENISA) (n 8).

[32] The European Network and Information Security Agency (ENISA) (n 8) 83.

[33] Millard (n 10)

[34] Mirena. Taskova, 'Cloud Service Provider and Their use of Personal Data' (Lexology, June 2016) accessed <https://www.lexology.com/library/detail.aspx?g=0dd03d8e-0916-4d95-8a96-2cdae9613fe6> 18 November 2017.

[35] The consultation is considered as a part of the Digital Single Market Strategy

[36] European Commission, 'Shaping the Digital Single Market' (European Commission, 25 March 2015) accessed <https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market#The%20Strategy> 20 November 2017.

[37] Vera Demary, 'The Platformization of Digital Markets: Comments on the public consultation of the European Commission on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy' (Econster, 21 December 2015) accessed <https://www.econstor.eu/bitstream/10419/126091/1/845730703.pdf> 20 November 2017.

clarification in the legal status of cloud provider in the context of the principle of complete protection of data subject. Since the objective of GDPR is to protect the personal data and to assess whether the GDPR reach such objective or not, there is a need to evaluate whether the GDPR provide a decent complete protection to data subject or not.

4. METHODOLOGY

- Research methodology

This thesis is a legal doctrinal research. This kind of research considered as a parasitic on practice which usually will not establish a new knowledge.[38] It will collect the existing raw materials which hold authority such as case, statutes and other primary sources in particular topic. Later, such material will be critical analyze in order to construct a systematic statement in that particular topic.

This text-based research will aim to find the solution or propose the way that the law can be developed in the future to a certain legal question.[39] The research method will start by gathering the data in the coherent structure, then defining the distinction, identifying the difference, and presenting the problem. After assessing the data, the solution or proposal for further development of the law will be introduced.[40]

The step that the author used to conduct the research are as follows:

- Choosing the problem-based approach[41] to construct the research.
- Gathering the fact by taking one or series of a legal topic as a starting point which is the problem of legal status of a controller and a processor in a cloud service environment.
- Do background reading, synthesize and integrate all the issue in the context.
- Come to a conclusion.

5. CHAPTER OVERVIEW

The second chapter will provide general knowledge about cloud computing systems as a whole, specifically in terms of the various types of cloud services on the market. It will also elaborate on the direction that the development of cloud computing in the market is taking. Furthermore, the author will also explain the risks in data protection that can be generated from the nature of the cloud computing. The third chapter will analyze an interpretation of a controller and a processor in the view of the GDPR, case

[38] Douglas W. Vick, ‘Interdisciplinarity and the Discipline of Law’ (2004) 31(2) Journal of Law and Society 177-178.

[39] Salim Ibrahim Ali, Dr. Zuryati Mohamed Yusoff, Dr. Zainal Amin Ayub, ‘Legal Research of Doctrinal and Non-Doctrinal’ (Researchgate, January 2017), accessed <https://www.researchgate.net/profile/Salim_Ali8/publication/316895684_Legal_Research_of_Doctrinal_and_Non-Doctrinal/links/5917225a4585152e19a102a3/Legal-Research-of-Doctrinal-and-Non-Doctrinal.pdf> 30 October 2017.

[40] Terry Hutchinson, Nigel Duncan, ‘Defining and Describing What We Do: Doctrinal Legal Research’ (Deakin Law Review, 2017) accessed <https://ojs.deakin.edu.au/index.php/dlr/article/view/70> 30 October 2017.

[41] The Problem based approach is a Presentation of an "ill-structured" (open-ended, "messy") problem and try to define or formulate the problem (the problem statement). Then constructing the list of a "knowledge inventory" (a list of "what we know about the problem" and "what we need to know"). And lastly, generating some possible solution.

law and opinion of WP29. Such analysis will be used to determine what factors are used to interpret who a controller or a processor is in a certain processing procedure. This chapter will also explain the legal status of a cloud provider in different scenarios, including the notion of binary distinction of controllers and processors. After this, the fourth chapter will examine whether the current interpretation of a legal status of the cloud provider is sufficient to provide a complete protection to a data subject or not. And closing off with the conclusion of the thesis, which will include suggestions about can be further expanded or amended in the GDPR.

Chapter 1

Cloud Computing and Data Protection

This chapter will be devoted to the general context regarding cloud computing, which will be explained and defined presently (see 1.1). The direction of its development will be covered in (1.2) and (1.3). The chapter will close with a reflection on the ways in which cloud computing threatens the protection of personal data (in 1.4). This general information is imperative before the actual legal assessment because it constitutes the basis on which the legal status of a cloud service provider and its ensuing complications are to be developed.

1.1 WHAT IS CLOUD COMPUTING?

Cloud computing is a convenient way of providing computing resources in a model of utility service.[42] It is a computing paradigm that can be utilized in a variety of architectures under wide ranges of service and deployment models and can also complement and collaborate with other software designs and technologies.[43] It can also be viewed as an on-demand service program via an internet network or computer network.[44] From a business perspective, cloud computing is an on-demand service of computing power with a pay-as-you-go manner,[45] similar to the traditional public utilities such as water, electricity, and gas. The most used definition is the one from the Nation Institution of Standards and Technology (NIST)[46]: “the cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.”[47]

The report of ENISA[48] has listed the benefit of cloud computing as follows: geographic spread, elasticity cloud, physical security, server-side storage, security-as-a-

[42] Millard (n 10).

[43] Lee Badger, and others, ‘NIST SP 800-146, Cloud Computing Synopsis and Recommendations’ (NIST, 2012) <http://nvlpubs.nist.go v/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf> accessed 10 January 2018; Robert L. Grossman, ‘The Case for Cloud Computing’ (2009) 11(2) IEEE 23-27 <https://pdfs.semanticscholar.org/fd95/05897a97b2f82a73148dc87ce3067a33c6ab.pdf> accessed 10 January 2018; William Voorsluys, James Broberg, and Rajkumar Buyya, ‘Introduction to Cloud Computing’ in James Broberg, Andrezej Goscinski and Rajkumar Buyya (eds), *Cloud Computing Principles and Paradigm* (John Wiley & Sons Inc. 2011).

[44] Ibid.

[45] William V., James B., and Rajkumar B. (n 43); Borko Furht, ‘Cloud Computing fundamental’ in Borko Furht and Armando Escalante (eds), *Handbook of Cloud Computing* (Springer 2010).

[46] The Nation Institution of Standards and Technology herein referred as “NIST”.

[47] https://www.nist.gov

[48] The European Union Agency for Network and Information Security (ENISA) is a center of expertise for cyber security in Europe which has been actively contributing to a high level of network and information security (NIS) within the Union since 2004. The Agency works closely together with Members States and private sector to deliver advice and solutions and also supports the development and implementation of the European Union's policy and law on matters relating to NIS.

service and certification and compliance.[49] [50] In sum, the varied types of cloud offer several benefits, such as cost effectiveness with no need for lengthy installation and maintenance.[51] Additionally, the scalability, flexibility and mobility of cloud computing also play an important role in attracting more customers. [52] Cloud computing can be seen as a perfect access to information anytime and anywhere, since it functions on virtual infrastructure and is not fixed to a certain location base, like the traditional computing method.[53]

1.2 WHAT IS A CLOUD SERVICE?

A cloud service is an IT product built from a cloud computing technology.[54] Cloud services can be separated according to model of services they provide and to the deployment structures used. The most widely used classification of cloud service comes from the US NIST. The three primary types of cloud computing service are Software-as-Service (SaaS), [55] Platform-as-a-Service (PaaS) [56] and Infrastructure-as-a-Service (IaaS).[57] [58] These service models are classified by the level of abstraction of the resources provided to the customer.[59] These abstraction levels are an example of distinctive

[49] ENISA, 'Cloud Security Guide for SMEs' (ENISA, 2015) <https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes> accessed 10 January 2018; Ayob Sether, 'Cloud Computing Benefits' (SSRN, 2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2781593> accessed 10 January 2018.

[50] This benefit has been approved and further clarify in an official opinion of the Article 29 working party in the Opinion 05/2012 on Cloud Computing which has listed beneficial point of cloud computing which are "Cloud computing can generate important economic benefits, because on-demand resources can be configured, expanded and accessed on the Internet quite easily. Next to economic benefits, cloud computing may also bring security benefits; enterprises, especially small-to-medium sized ones, may acquire, at a marginal cost, top-class technologies, which would otherwise be out of their budget range. And there is a wide gamut of services offered by cloud providers".

[51] L. Leung, ' Cloud Customers Report Capital Cost Savings' (DataCenter Knowleadge, 26 January 2010) < http://www.datacenterknowledge.com/archives/2010/01/26/cloud-customers-report-capital-cost-savings> accessed 10 January 2018; Arno Christian, 'The Advantages of Using Cloud Computing' (@CloudExpo Journal, 14 April 2014) <http://cloudcomputing.sys-con.com/node/1792026> accessed 10 January 2018.

[52] Jeff Spivey and others. 'Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives. ISACA Information Security White Paper' (ISACA, 2009) <http://www.klcconsulting.net/security_resources/cloud/Cloud_Computing_Security_&_Governance-ISACA.pdf> accessed 10 January 2018; Michael Miller, 'Cloud Computing Pros and Cons for End Users' (informIT, 13 February 2009) <http://www.informit.com/articles/article.aspx?p=1324280> accessed 10 January 2018.

[53] Jonathan Koomey, '4 reasons why cloud computing is efficient' (REUTERS, 25 July 2011) < http://www.reuters.com/article/2011/07/25/idUS59089929820110725> accessed 10 January 2018; Alexa Huth, and James Cebula, 'The basics of cloud computing' (US-CERT, 2011) <https: //www.us-cert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf> accessed 10 January 2018.

[54] ibid

[55] Hereinafter referred as "SaaS".

[56] Hereinafter referred as "PaaS".

[57] Hereinafter referred as "IaaS".

[58] Peter Mell and Timothy Grance, 'NIST SP 800-145, The NIST Definition of Cloud Computing' (NIST, 2011) <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublicatio n800-145.pdf> accessed 10 January 2018.

[59] Ibid.

characteristic of cloud service, which can compile multiple layers of different features within one service.[60]

Apart from different types of service model, the cloud computing service can also be categorized according to their deployment models. These are the private cloud, the community cloud, the public cloud and the hybrid cloud.[61]

1.2.1 Service Models of Cloud Computing

a) Software-as-a-Service (SaaS)

According to NIST, a SaaS's model delivers the application and the computational resources in an on-demand service.[62] The applications can be easily accessed on various devices through web browsers or application programs.[63] With SaaS, there is no need for technical expertise in order to receive such a high-performance service's system because the cloud consumer does not manipulate the fundamental cloud infrastructure, such as the network, the server, or the operating system.[64] With no requirement of technical know-how, SaaS is the most widely used type of cloud service on the market.[65] Some of the well-known SaaS are Google Apps[66], Salesforce[67] and Desktop as a Service.[68] For example, instead of buying a word-processing software and installing it on every computer, Google Apps or Microsoft Office 365 SaaS can be used for the same purpose.

A SaaS system is very different from the traditional style of computing infrastructure, in this scenario, what is being rented and paid for by the customer is access to an application, not the actual software or hardware.[69] With SaaS, the cloud service provider is the one who processes and runs the software on its computer; the customer only pays the fee to rent it or buys a subscription to use a service.[70] The main benefits of

[60] Lamia Youseff, Maria. Butrico, and Dilma. Da Silva, 'Toward a Unified Ontology of Cloud Computing' (8 May 2015) <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.176.3634&rep=rep1&type=pdf> accessed 10 January 2018.

[61] Wayne Jansen and Timothy Grance, 'NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing. (NIST, 2011) <http://nvlpubs.nist.gov/nistpubs/ Legacy/SP/nistspecialpublication800-144.pdf> accessed 10 January 2018.

[62] Jansen and Grance (n 60).

[63] Badger, and others (n 43).

[64] Cloud Industry Forum, 'Cloud UK: Paper Four Cloud Adoption and Trends for 2012' (2012) <https://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwim3Z_b9d_YAhWJLFAKHaA7DcgQFggzMAE&url=https%3A%2F%2Fwww.cloudindustryforum.org%2Ffile%2F121%2Fdownload%3Ftoken%3D1nfl3_ue&usg=AOvVaw06-af00NshQ9U4b6okOCbc> accessed 10 January 2018.

[65] Mell and Grance (n 57).

[66] Google App (2010). http://www.google.com/apps/intl/en/business/index.html.

[67] Salesforce Homepage (2010). http://www.salesforce.com/crm/

[68] For example, of Desktop as a Service is G.ho.st Homepage (2010). http://g.ho.st/.

[69] Software and Information Industry Association, 'Strategic Backgrounder: Software as a Service' (12 May 2010) <https://www.slideshare.net/Shelly38/software-as-a-service-strategic-backgrounder> accessed 10 January 2018

[70] Levinson Meridith, 'Software as a Service (SaaS) Definition and Solutions' (CIO, 15 May 2007) < https://www.cio.com/article/2439006/web-services/software-as-a-service--saas--definition-and-solutions.html> accessed 10 January 2018.

SaaS are the organization and the fact that users reduce their IT expenses since they are not required to constantly but software licenses.[71] Additionally, the burden of software maintenance for the customer is reduced.[72]

b) Platform-as-a-Service (PaaS)

PaaS is a service which is considered to be between SaaS and IaaS.[73] Popular examples of PaaS are Google App Engine[74], Microsoft Azure[75] and Force.com.[76] [77] PaaS provides the customer with a computing platform ready to use for developing and deploying software applications.[78] It typically comprises application management tools.[79] Moreover, the cloud customer has full control over the configuration of the platform, which can be set according to their preferences.[80] Yet, although the cloud user has no control over the network, server, operating system or storage, it can be managed through the security system by both a cloud service provider and a customer.[81] The key objective of PaaS is cost and complexity reduction in hardware and software by offering a virtualized infrastructure at an affordable cost.[82]

c) Infrastructure-as-a-Service (IaaS)

IaaS is the "Everything as a Service" model.[83] The IaaS providers rent out their computing utilities, such as the server, the network and the software, to the customer

[71] Scott Sehlhorst, 'The Economics of Software as a Service (SaaS) vs. Software as a Product' (Pragmatic Marketing, 25 November 2008) <https://www.pragmaticmarketing.com/resour ces/articles/the-economics-of-software-as-a-service-saas-vs-software-as-a-product> accessed 10 January 2018.

[72] Youseff, Butrico, and Da Silva (n 59); Brian Hayes, 'Cloud computing' (2008) 51(7) ACM 9-11 <https://cacm.acm.org/magazines/2008/7/5368-cloud-computing/fulltext> accessed 10 January 2018.

[73] Badger, and others (n 43).

[74] Google App Engine (GAE)'s main goal is to efficiently run users' web applications. It maintains Python and Java runtime environments on application servers, along with some simple APIs to access Google services. Google App Engine (2010) <http://code.google.com/appengine/>.

[75] Windows Azure employs a "fabric controller" to manage all virtual machines and storage servers on the physical machines in a Microsoft data center (David, 2009b). Also provide database service called SQL Azure to store data in the cloud. Windows Azure platform (2010). <http://www.microsoft.com/windowsazure/>.

[76] Force.com is an enterprise cloud computing platform offered by Salesforce. It helps service venders develop and deliver stable, secure and scalable applications. <www.salesforce.com/platform/>

[77] Hai Jin and others, 'Cloud Computing Technologies and Applications' in Borko Furht and Armando Escalante (eds), *Handbook of Cloud Computing* (Springer 2010); Ayob Sether, 'Cloud Computing Benefits' (SSRN, 19 May 2016) <https://papers.ssrn.com/sol3/paper s.cfm?abstract_id=2781593> accessed 10 January 2018.

[78] Ibid.

[79] Ibid.

[80] Jinzy Zhu, 'Cloud Computing Technologies and Applications' in Borko Furht and Armando Escalante (eds), *Handbook of Cloud Computing* (Springer 2010).

[81] Badger, and others (n 43).

[82] Garudatt Kulkarni, Ramesh Sutar, and Jayant Gambhir, 'Cloud Computing-Storage as Service' (2012) 2(1) IJERA 945-950 <https://pdfs.semanticscholar.org/8ad9/bab2356b6f397645d2dd4b2c7ae35485cd13.pdf> accessed 10 January 2018; Zhu (n 79).

[83] Ibid.

according to their request. Examples of IaaS are Amazon Elastic Compute Cloud (EC2),[84] GoGrid,[85] The Amazon Simple Storage Service (S3),[86] and Rackspace Cloud.[87] The cloud consumers that use this type of service generally have much freedom regarding the configuration of the operating system, the storage, the deployed application, and the development environment including security systems.[88] Sometimes, IaaS can be referred to as Hardware as a Service.[89] This is because the cloud provider rents out their computing infrastructure, including virtual machines, operating systems, the network and other infrastructure.[90] The benefits of IaaS are flexibility and control of the system and lower costs in obtaining, keeping and utilizing basic hardware and software infrastructure by using a third party's computing and storage infrastructure.[91] The drawback of IaaS is the requirement of user expertise with more micromanagement of resources.[92]

1.2.2 Deployment Models of Cloud Computing

a) Private cloud

Private cloud is an infrastructure in which the computing environment is owned by, operated by, and exclusively benefits a single organization on a private network.[93] Nevertheless, the system can be managed by the cloud user, the cloud provider or by a third party. The operating center can also be on-site or located elsewhere.[94] Private cloud is mainly chosen by a private cloud consumer in the form of a large company or government sector which has a need for stricter control and more secure environment.[95]

[84] The Amazon Elastic Compute Cloud (EC2) provides many useful features for customers, including a mature and inexpensive billing system able to charge for computing at a very fine-grained level (memory usage, CPU usage, data transfer, etc.), deployment between multiple locations, elastic IP addresses, connection to a customer's existing infrastructure through a Virtual Private Network, monitoring services by Amazon Cloud Watch, and elastic load balancing <http://aws.amazon.com/ec2>.

[85] GoGrid provides customers with a user-friendly web service interface, easy-to-understand video demonstrations, a strict but inexpensive billing system and a Hybrid Hosting. <http://www.gogrid.com/index.v2.php>.

[86] The Amazon Simple Storage Service (2010) (S3) is an online storage web service offered by Amazon Web Services. <http://aws.amazon.com/s3>.

[87] Rackspace Cloud is a cloud files service which offers cloud storage service with unlimited online storage and a Content Delivery Network (CDN) for media on a utility computing basis. <http://www.rackspacecloud.com/>.

[88] Zhu (n 79) and Badger, and others (n 43).

[89] Jin and others (n 76).

[90] Ken Hess, 'Why You Need Infrastructure as a Service (IaaS)' (The Frugal Networker, 7 January 2012) <https://frugalnetworker.com/2012/01/07/why-you-need-infrastructure-as-a-service-iaas/> accessed 10 January 2018.

[91] Millard (n 10); Badger, and others (n 43).

[92] Jin and others (n 76); Millard (n 10).

[93] Cisco, 'State Government Deploys Private Cloud to Provide Services to Agencies' (CISCO, 2011) <http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/state_ of_alaska_cs.pdf>, Jansen and Grance (n 60); Badger, and others (n 43); Furht (n 45).

[94] Ibid.

[95] Jin and others (n 76); Millard (n 10).

For example, the Office of the Director of National Intelligence (ODNI) opt for private cloud operating by Amazon Web Service.[96]

b) Community cloud

This type of cloud is a mixture of private and public cloud which is used to serve more than one customer with the same goal or concern.[97] An example is Microsoft Office 365 SaaS as a ‘multi-tenant service that stores US government data in a segregated community cloud’.[98]

c) Public cloud

This type of cloud deployment is the most widely used type of service, which is accessible via internet to all in the pay-as-you-go manner.[99] The infrastructure and computing resource may be owned and operated by third parties such as a commercial, academic or government sector or a combination of such.[100] For example, the Lakehead University in Canada use Google’s public cloud to operate its email system.[101]

d) Hybrid cloud

Hybrid cloud is a mixture of the abovementioned cloud deployment (private, community or public) and is considered to be more complex than other cloud models. One reason for using the hybrid cloud is to reduce the workload during a time of high demand. For instance, a company can keep their critical information within their private cloud, while hosting the less substantial information in the public cloud.[102]

1.3 THE DEVELOPMENT OF CLOUD COMPUTING

The introduction of cloud computing has created a phenomenon which fundamentally changes how information technology (IT) services are invented and developed. The innovation has changed computing power to a mere commodity in the eyes of the consumer.[103] The cloud computing innovation has answered the demand for and complexity of larger and faster computing power for an organization with affordable

[96] Dan tynan, ‘How the feds learned to stop worrying and love the cloud’ (enterprise.nxt 2017) <https://www.hpe.com/us/en/insights/articles/how-the-feds-learned-to-stop-worrying-and-love-the-cloud-1711.html> accessed on 21 May 2018.

[97] Jansen and Grance (n 60); Badger, and others (n 43).

[98] Kirk Koenigsbauer, ‘Announcing Office 365 for Government: A US Government Community Cloud’ (Silicon, 30 May 2012) < http://www.silicon.co.uk/workspace/microsoft-office-365-government-80702?print=pdf> accessed 10 January 2018.

[99] Jin and others (n 76).

[100] Jansen and Grance (n 60); Badger, and others (n 43).

[101] Safiya Okai and others, ‘Cloud Computing Adoption Model for Universities to Increase ICT Proficiency’ (2014) 4(3) SAGE <http://journals.sagepub.com/doi/full/10.1177/2158244014546461> accessed on 18 May 2018.

[102] Jin and others (n 76).

[103] Maricela-Georgina Avram, ‘Advantages and challenges of adopting cloud computing from an enterprise perspective’ (2014) 12 529-534 <https://www.sciencedirect.com/science/article/pii/S221201731300710X> accessed 10 January 2018.

price by delivering all functionality of IT services with dramatically lower upfront cost than traditional IT method.[104] Chip Childers, CTO of Cloud Foundry Foundation says that "We are shifting to a 'cloud-first' world more and more."[105] In 2018, cloud computing continues to be integrated into more businesses and organizations as companies start to see the benefits that cloud service can offer.[106] [107] This is further supported by the prediction issued by Forbes which suggests that the total global cloud market will be more than $150B in 2018 and will continue to grow.[108] Due to the cloud service trend in 2018, many of the companies and organizations will opt for the multi-cloud strategy with which they split their workload across more than one public cloud.[109] To sum up, this will be a year of cloud consolidation, but with all the advantages that the cloud has to offer, there are also threats to our personal data in multiple ways which will be discussed below.

1.4 THREAT TO PERSONAL DATA IN A CLOUD COMPUTING SERVICE

Cloud computing technology offers many benefits, as clarified in the opinion of WP29.[110] The technology offers the user unique features that can be at odds with the idea of traditional computing method where there is a physical and tangible computing infrastructure. It offers the program as a service instead of regular hardware-based computing.[111] However, cloud computing can also endanger personal information that is collected within the cloud. In this 21st century what has become valuable is the storing of data. Cloud computing, which acts as a bank vault securing a vast amount of data, becomes a valuable target of unauthorized access or appropriation.[112] Moreover, unlike traditional computing methods in which the owners of the information are responsible for controlling their own data, cloud computing relies on virtualized resources. The control of the cloud is under third party control and its use is mostly shared among other unknown

[104] Paul Roehrig, 'New Market Pressures Will Drive Next-Generation IT Services Outsourcing' (Forrester, 9 October 2009) <https://www.sciencedirect.com/science/article/pii/S221201731300710X> accessed 10 January 2018; Sean Marston and others, 'Cloud Computing – The Bussiness Perspective' (2011) <https://pdfs.semanticscholar.org/2531/00590bbd1b3fb2653ee2ba7983992f247796.pdf> accessed 10 January 2018.

[105] Sam Clark, 'Cloud computing in 2018: what the future holds' (The Stack, 14 December 2017) <https://thestack.com/cloud/2017/12/14/cloud-computing-in-2018-what-the-future-holds/> accessed 10 January 2018.

[106] Nigel Kersten (Chief Technical Strategist, Puppet), Issy Ben-Shaul (CEO and founder of Velostrata), Rob Strechay (SVP Product, Zerto), Andrius Ulenskas (Technical Director, Hyve Managed Hosting), and Mat Clothier, (CEO, CTO and Founder at Cloudhouse).

[107] Clark (n 104).

[108] Louis Columbus, 'Forrester's 10 Cloud Computing Predictions For 2018' (Forbes, 7 November 2017) <https://www.forbes.com/sites/louiscolumbus/2017/11/07/forresters-10-cloud-computing-predictions-for-2018/#2017784a4ae1> accessed 10 January 2018.

[109] Clark (n 104).

[110] 29WP, 'WP196' (n 12) 4.

[111] Badger, and others (n 43); Jonathan Strickland, 'How cloud computing works' (howstuffworks, 8 April 2008) <https://computer.howstuffworks.com/cloud-computing/cloud-computing.htm> accessed 10 January 2018.

[112] Brent R. Rowe, 'Will Outsourcing IT Security Lead to a Higher Social Level of Security?' (Research Triangle Institute International, 2007) <http://weis2007.econinfosec.org/papers/47.pdf> accessed 10 January 2018; Jansen and Grance (n 60).

parties—with the exception of the private cloud.[113] Given the nature of the cloud, it is hard for the customer to efficiently inspect the quality and efficiency of the cloud's system and thus discern whether it poses a risk to the data protection.[114] Such risks can be worsened when the cloud computing involves multiple transfers of data between clouds.[115]

The threat to personal data which can generated in the cloud service, then, relates to the fact that the flexibility of the location of storage and the processing procedure—such as being able to use multiple locations—leads to many legal complexities and difficulties in complying with the law.[116] The data in a cloud can be kept in several locations simultaneously to enable efficient and real-time services. An example of this is Amazon, which offers data storage both in the US and the EU.[117] With multiple storing and processing locations, it is difficult to ascertain which jurisdiction is applicable to the data processing procedure which can be even more difficult if the data is transferred through multiple locations.[118] Additionally, another threat can originate from a cloud provider who wishes to lessen its own obligation or liability by establishing a data center in a country with an inadequate level of protection.[119] [120] In the case of shared infrastructure, a cloud's customer may be requested to provide its processing information under the law. The untargeted information stored within the same cloud, such as information pertaining to other customers, might be exposed to external parties and thus, resulted in a colocation's risk.[121] [122]

Broadly speaking, these factors can pose a threat to the confidentiality, integrity, privacy and security of the data.[123] The integrity and the confidentiality of the data can be compromised if the cloud provider or third parties can access the user's data in an

[113] Millard (n 10).

[114] The European Network and Information Security Agency (ENISA) 'Cloud computing: Benefits, risks and recommendations for information security' (n 8).

[115] Ibid.

[116] Christopher Millard and W. Kuan Hon, 'Cloud Computing vs Traditional Outsourcing—Key Differences' (2012) 23(4) Computers & Law <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2200592> accessed 10 January 2018.

[117] The Amazon Simple Storage Service (S3) Services <http://aws.amazon.com/s3>.

[118] Paolo Balboni, 'Data Protection and Data Security Issues Related to Cloud Computing in the EU' (Tilburg University Legal Studies Working Paper Series No. 022/2010, 2010) <https://ssrn.com/abstract=1661437> accessed 10 January 2018.

[119] The European Network and Information Security Agency (ENISA) 'Cloud computing: Benefits, risks and recommendations for information security' (n 8).

[120] Customer data may be held in multiple jurisdictions, some of which may be high risk. If data centers are located in high-risk countries, e.g., those lacking the rule of law and having an unpredictable legal framework and enforcement, autocratic police states, states that do not respect international agreements and etc. Those sites could be raided by local authorities and data or systems subject to enforced disclosure or seizure.

[121] James Urquhard, 'FBI Seizures Highlight Law as Cloud Impediment' (CNET, 16 April 2009) <http://news.cnet.com/8301-19413_3-10220786-240.html> accessed 10 January 2018; The European Network and Information Security Agency (ENISA) 'Cloud computing: Benefits, risks and recommendations for information security' (n 8).

[122] With the colocation risk, it is advisable to the cloud consumer to specify in a contractual clause how a law enforcement entity may be given an access and what type of notice is required when such situation has occurred.

[123] 29WP, 'WP196' (n 12) 5-6.

intelligible form.[124] Alternatively, this can also happen when a system fails to secure the information against unauthorized actions. [125] Privacy and security are considered the main issue, and they entail a technical challenge due to the nature of cloud computing services which share infrastructures among multiple customers in unknown locations.[126] Moreover, the majority of cloud services that have been offered on the market are public clouds which are exposed to multiple users and carry a higher risk of being targeted in a cyber-attack.[127] It is therefore important for the cloud customer to choose a trustworthy cloud service provider to host their personal data in order to mitigate risks.[128]

Furthermore, the character of the content stored in the cloud can cause a greater risk impact—as when dealing with know-how, copyrighted work or valuable information. The impact of a breach is critical with these kinds of information, and the damages may never be fully recovered through legal proceeding.[129] [130] Data breach can seriously harm both hardware and software infrastructure and the data stored within.[131] Another major issue of cloud computing system is its security.[132] A risk can occur when the cloud does not have suitable security measures installed or if the system has not been installed properly. These problems can lead the system to malfunctioning or to failure and, thus, to collapsing the operation of the entire system.

A survey shows that the major concern of cloud customers is security risks.[133] This fear is caused by the invisibility of the infrastructure and resources, which lack a physicality that can be controlled and accessed, as is the case with traditional computing security.[134] Due to the dynamism and flexibility of the cloud system, the traditional security is not sufficient to protect the system and meet the various inherent limitation.[135] There is an urgent need for the innovative security measures for virtualized infrastructure. As it is, this still remains a challenge for cloud computing.[136] Moreover, these risks have

[124] Millard (n 10).

[125] Ibid.

[126] Badger, and others (n 43).

[127] Michael Armbrust and others, 'Above the Clouds: A Berkeley View of Cloud Computing' (UC Berkeley Reliable Adaptive Distributed Systems Laboratory White Paper, 10 February 2009) <https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf> accessed 10 January 2018; Furht (n 45).

[128] Rajkumar Buyya, Suraj Pandey, and Christian Vecchiola, 'Cloudbus Toolkit for Market-Oriented Cloud Computing' (2009) <http://www.cloudbus.org/papers/Cloudbus-Keynote2009.pdf> accessed 10 January 2018.

[129] The European Network and Information Security Agency (ENISA) 'Cloud computing: Benefits, risks and recommendations for information security' (n 8); Yves Poullet and others, 'Cloud Computing and its Implication on Data Protection' (CRID, 5 March 2010) <http://www.crid.be/pdf/public/6471.pdf.> accessed 10 January 2018.

[130] To mitigate such risk, the author recommends to addresses the remedies and role for each actor in a contractual clause for example Confidentiality or Non-Disclosure Clause or Intellectual Property Clause. The obligation, responsibility and liabilities of each relevant actor must be clarified thoroughly.

[131] Janine A. Bowen, 'Legal Issues in Cloud Computing' in James Broberg, Andrezej Goscinski and Rajkumar Buyya (eds), *Cloud Computing Principles and Paradigm* (John Wiley & Sons Inc. 2011).

[132] Susan Morrow, 'Data Security in the Cloud' in James Broberg, Andrezej Goscinski and Rajkumar Buyya (eds), *Cloud Computing Principles and Paradigm* (John Wiley & Sons Inc. 2011)

[133] Morrow (n 131).

[134] Zhu (n 79).

[135] Morrow (n 131).

[136] Ibid.

been confirmed by many experts, such as ENISA and NIST, along with an official report by the WP169 on cloud computing.

To sum up, cloud computing is an on demand-computing infrastructure which is used in a cloud service to provide the software and hardware as a pay-as-you-go manner. There are multiple types of cloud models that can be chosen from according to the abstraction level such as PaaS, SaaS and IaaS. It is also offered in multiple model, such as public cloud, private cloud or hybrid cloud. Nevertheless, due to the nature of a cloud itself, it can pose a threat to the data stored within it system such as jurisdiction issue, colocation risk, malicious insider or incomplete data deletion, and etc. And such general information will be used as a basis for further assessment in the legal status of cloud service provider in a following chapter.

Chapter 2

The Cloud Service Provider, the Controller and the Processor

In this chapter, the author answers the following questions: Who are the controller and processor and what are their obligations under the Directive and GDPR? (2.1) How do the case law and the Article 29 WP Opinions interpret the legal status of a controller and a processor? (2.2) What is the legal status of the cloud service provider and the problem of binary distinction? (2.3)

2.1 WHO IS A CONTROLLER AND A PROCESSOR?

The legal status of a controller and processor are an essential factor in allocating the responsibility of players in the processing procedure.[137] It determines what needs to be done to demonstrate compliance with the data protection law. This importance was reaffirmed in WP169[138] and WP196.[139] Additionally, the legal status of a controller and processor needs to be a community concept which means that the concept does not differ among the Union members to sustain the effective application of the GDPR.[140]

The definition of a controller according to the GDPR is the same as in the Directive.[141] It contains three main parts: the personal aspect ("a natural or legal person, public authority agency or any other body"), the pluralistic control ("which alone or jointly with other"), and the essential element to distinguish the controller from other actors ("determines the purpose and the means of the processing of personal data").

For example, Company A is the controller because it determines the purpose and the means of the processing procedure. The purpose for this procedure will be to calculate and manage the employee's payroll. Company A chose to outsource the operation to the Company B, which provides a system or service that Company A prefers.

The controller is the one who determines the purpose of the processing procedure and chooses the means of processing, which is a major part in a processing procedure. Consequently, the controller is usually responsible for most of the obligations required by the law. Examples are an obligation to conduct lawful processing procedure,[142] obligation to apply appropriate security measure[143], the implementation of principle of accountability[144] and the principle of data protection by default and design.[145]

[137] European Union Agency for Fundamental Rights, '*Handbook on European Data Protection Law'* (Publication office of the European Union, 2014) 49.

[138] 29WP, 'WP 169' (n 24) 2, 4.

[139] 29WP, 'WP196' (n 12) 7.

[140] 29WP, 'WP 169' (n 24) 8.

[141] Article 4(7) GDPR, article 2(d) DPD.

[142] Article 24 GDPR, article 6 DPD.

[143] Article 32 GDPR, article 17 DPD.

[144] In the GDPR, the processor will be required to cooperated more in utilizing appropriate security measure, informing or suggesting any potential infringement action, adherence to the approved code of conduct, processing data according to the instruction of the controller, apply the principle of data protection by default and design and etc.

For the processor, both the GDPR and the Directive used the same definition of "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".[146]

The most important task of the processor is processing the data that the controller has assigned on behalf of that controller. In the example given above, Company B will receive all the data from Company A and process the data according to Company A's instruction to determine the employee's salary.

The significant development in the GDPR comparing to the Directive is the increase in a responsibility and liability of a processor. Examples of new obligations for a processor are the informing duty to a controller in case of any possibility of infringements[147], obligation to record processing activity[148], obligation to implement suitable security measure[149] and obligation to notify data breach.[150]

2.2 THE CONTROLLER AND THE PROCESSOR UNDER THE DIRECTIVE, GDPR AND CASE LAW

Determining the legal status in processing procedure involves multiple factors, such as the factual situation and the contractual context. The complex and multiple layers of processing procedure and the plurality of actors, leads to the confusion in the distribution of such roles.[151] To uphold the effectiveness of the data protection law, the WP29 issued a guideline in WP169 to better illustrate the allocation of the title of controller and processor. [152]

With the identical definition of controller and processor in both GDPR and the Directive, the WP29's guideline and case law published in the time of the Directive can also be used in this assessment of legal status. This will help better predict the interpretation of the controller and processor's legal status under the GDPR, since the GDPR has not been enforced yet.

The controllership is usually determined from the contract agreement, which usually indicates the power, responsibility and liability of each party. It can also be expressed by a legal provision where the law obliged one party to assume the role of controller.[153] It can also arise from the implicit competence, such as the employer-employee relationship.[154] Nevertheless, due to the complexity of the agreement and service used in the processing procedure, the controllership as defined in contract, law,

[146] Article 4(8) GDPR, article 2(e) DPD.

[147] The informing duty is an obligation which required in article 28(3)(h) GDPR for processor shall inform its controller in case of any possibility of infringement with the GDPR or other Union data protection law in the controller's instruction or opinions. This obligation has not been introduced in the Directive.

[148] Article 30(2) GDPR, this obligation has not been introduced in the Directive.

[149] Article 28, 32 GDPR, this obligation has not been introduced in the Directive.

[150] The processor has an obligation to notify its controller after it becomes aware of a personal data breach without any delay. (Article 33(2) GDPR, this obligation has not been introduced in the Directive).

[151] 29WP, 'WP 169' (n 24) 2, 27; Information Commissioner's Officer, 'Data controllers and data processors: what the difference is and what the governance implications are' (ICO, 2014) 14 <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf> accessed 10 January 2018.

[152] 29WP, 'WP 169' (n 24).

[153] 29WP, 'WP 169' (n 24) 10.

[154] Ibid.

and implicit competence is not enough to sufficiently allocate the obligation for each actor.

WP169 defined the term of controller as a functional concept and suggests using the factual influence to determine the title of each actor.[155] The evaluation should be also done from the factual influence together with the legal provision.[156]

This means that even though the arranged contractual relationship may indicate that A has a power to define the means and purpose for the procedure, B could actually decide on those two notions. With the factual influence, the legal status of B is a controller of that processing procedure, even if this differs from the contract.

An example is the SWIFT case.[157] The company has a contractual relationship as a processor for financial institutions into processing the financial transaction for their client.[158] Later, the company transferred this data under a US subpoena without any prior consent or notice to either the financial institutions or the clients. This transfer was solely initiated by the company and occurred outside the contractual scope agreed with the financial institution.[159] The autonomous act of the company to transfer the client's personal data to US authorities made the company accounted as a controller in this processing procedure.[160] This de facto decision regarding means and purpose will assign the company the responsibility and liability of a controller in this new processing procedure.[161]

The factual influence also helps determine when there is a case of multiple controllers in one processing procedure. This pluralistic control can happen in multiple ways where multiple actors exert power jointly in determining the means and purpose of the processing procedure.[162] The degree of power for each actor can vary, which can result in different degrees of liability.[163] The involvement level can also vary, for instance, they can jointly determine the purpose but not the means or jointly determine part of the processing procedure.[164]

An example of joint controllership is supermarket A partner with restaurant B offering a sales promotion. They both process each other client's list to send out the discount coupon to the customers. They decide together the purpose of the processing procedure. However, supermarket A chooses the means of processing by using cloud service. These example shows that even if the responsibility are not equally shared among A and B, they are both still considered as controllers.[165]

Nonetheless, cooperation between parties without sharing the same purpose or means cannot always be interpreted as a joint controllership. Consequently, due to the

[155] 29WP, 'WP 169' (n 24) 8, 11.

[156] 29WP, 'WP 169' (n 24) 1, 8.

[157] Kuner (n 19).

[158] Article 29 Data Protection Working Party 01935/06/EN WP128, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) 11, 10.

[159] Ibid 11.

[160] Ibid 13.

[161] 29WP, 'WP 169' (n 24) 8,15, 17.

[162] 29WP, 'WP 169' (n 24) 4; Information Commissioner's Officer (ICO), 'Data controllers and data processors: what the difference is and what the governance implications are' (n 150) 15

[163] Information Commissioner's Officer (ICO), 'Data controllers and data processors: what the difference is and what the governance implications are' (n 150).

[164] 29WP, 'WP 169' (n 24) 21, 22.

[165] 29WP, 'WP 169' (n 24) 19.

complexity of business models nowadays, it is recommended to evaluate both the contractual relationship and factual influences to determine the role for the controller.

To determine the legal status in a processing procedure, a processor needs to be a separate entity from a controller and process data according to the instruction of the controller or "on behalf" of the controller.[166] For example, Company A instructs Company B to process their client data to come up with a new marketing strategy. Company B processes this data according to the means and purpose set by Company A. Company B processes the data on behalf of Company A and is therefore a processor.

In certain cases, one entity can be both controller and processor in the same time, but not within the same processing procedure.[167] For instance, Company A outsources Company B to process their customer data to invent new market strategy. Later, Company B use the same set of data for their own commercial purpose without consent from Company A. Such act will constitute as another processing procedure and Company B will be titled as a controller in this new processing procedure. However, Company B will still be a processor in the initial processing procedure.

Additionally, processing beyond the instruction of controller can be constituted as a joint controller within the same procedure.[168] For example, Company A outsources Company B to implement a new market strategy by processing their client list. If Company B can autonomously act by choosing the target client for that market strategy and implement that marketing strategy. Company B has certain room for maneuver in the execution of the processing procedure initiated by Company A. Company A still holds certain power in the execution by determine the purpose and choosing the outsourcing company to execute such purpose. Together, they jointly control the processing procedure to reach its purpose, which is implementation of a new marketing strategy. This is considered a joint controllership between A and B in the processing procedure.

However, the guideline by the WP29 no legally binding power. So, to understand the actual implementation of the legal status, it is necessary to assess the case law. Present, there are few case law that can be used to clarify the interpretation of the legal status of a controller and a processor: Wirtschaftsakademie,[169] Jehovan todistajat,[170] SWIFT,[171] and Google Spain.[172]

In those cases, the court affirmed the interpretations of a controllership which certain issues have already been expressed in the report of WP29. There is no case law that explicitly clarifies the legal status of a processor. However, certain notions from the above case law can be adapted to define the scope of a processor. Three main categories of issues have been clarified in case law:

- The broad interpretation of controllership
- The factual influence
- The joint controllership

[166] 29WP, 'WP 169' (n 24) 1, 4.

[167] 29WP, 'WP 169' (n 24) 25; Information Commissioner's Officer (ICO), 'Data controllers and data processors: what the difference is and what the governance implications are' (n 150).

[169] Case C-210/16 Wirtschaftsakademie Schleswig v Holstein (ECJ 24 October 2017), Opinion of AG Bot.

[170] Case C-25/17 Jehovan todistajat v. uskonnollinen yhdyskunta (ECJ 1 February 2018), Opinion of AG Mengozzi.

[171] 29WP, 'WP128' (n 157).

[172] Case C-131/12 (n 6); Case C-131/12 Google Spain SL. v. Agencia Española de Protección de Datos (AEPD) (ECJ 25 June 2013), Opinion of AG Jääskinen.

First, the broad interpretation of the controllership was explicitly mentioned in Wirtschaftsakademie, Jehovan todistajat , and Google Spain. The broad interpretation is beneficial in the scenario where multiple parties all have influence over a processing procedure.[173] The judgement in Google Spain stated that to uphold the objective of the data protection law, in certain scenarios a broad interpretation of a controller is needed. [174] While the advocate general opinions in Wirtschaftsakademie case and Jehovan todistajat also following such direction of broad interpretation.[175]

Moreover, there also other notions that the court has defined which can also be classified within the broad interpretation topic.

There is no requirement that the controller needs to fulfil all their obligations to be considered a controller. Jehovan todistajat is a religious community where their members conduct a door-to-door proselytize and, in that process, collected personal data and processed it for subsequent visits. The Advocate General stated that a religious community is controller even it does not have access to the data collected by its members. The reason is the inability to fulfil all the controller's obligations required by law, namely the right to access, does not affect a party from being considered a controller.[176] This notion was also defined in the WP169 and such affirmation by the court's decision will provide the legally binding power on this issue.[177]

The imbalance in degree of controllership also does not affect the controllership. Wirtschaftsakademie is a fan page administrator who uses Facebook for their web page's platform. Facebook use cookie to collects visitors' personal data and processes it to provide statistics for the Wirtschaftsakademie and targeted advertisements for itself. The administrator claimed that they have no negotiation power when signing the contract with Facebook and therefore should not be a controller. However, the Advocate General disagreed and affirmed the point that has been made by WP169.[178] When a user signs a contract with service provider, this means that such user accepts full responsibility from that processing procedure. The imbalance between two parties does not prevent the user from being considered as a controller.[179]

Additionally, incomplete control within the processing procedure does not exclude a party from being a controller. The Belgian government commented in the Wirtschaftsakademie case that relying on complete control of the entire processing procedure to be a controller is impractical, since in reality, complete control in one processing procedure can be difficult to find.[180] The Advocate General reinforced this notion; the web administrator who has no control over the processing data was still accountable as a controller.[181]

The incomplete control in the processing procedure has also been mentioned in the Jehovan todistajat, the religious community considered a controller even if it has no control in the access of personal data. The Advocate General opinion in this case explicitly agree with the Advocate General Bot in the Wirtschaftsakademie case to fully

[173] Case C-210/16 (n 168) [63]; Case C-131/12, 'Opinion of AG Jääskinen' (n 171) [38] [83].
[174] Case C-131/12 (n 6) [34].
[175] Case C-210/16 (n 168) [45]; Case C-25/17 (n 169) [63] [70].
[176] Case C-25/17 (n 185) [169].
[177] 29WP, 'WP 169' (n 24) 22.
[178] Ibid 26, 28.
[179] Case C-210/16 (n 168) [61].
[180] Ibid [62].
[181] Ibid.

rely on the complete control as of the factor in the interpretation will lead to a gap in the data protection law.[182]

Lastly, this notion was also stated by the court in Google Spain. The court ruled that even if the search engine provider does not have control over the content published by third parties' websites or the web page can choose to opt out from being include in the search engine's index, these factors do not affect the interpretation of the court in whether the search engine provider is a controller or not.[183] With the control in creating an index for search result, this considered sufficient to account a search engine provider as a controller in a processing procedure.[184]

Without the broad interpretation it can lead to a situation where an entity opts for third party service provider to escape from obligations in data protection law. Because it does not have direct and complete control in processing procedure.[185] However, too broad of an interpretation can result in an unfair judgement, and risk holding actors who do not fit as a controller liable as a controller.

Second category is the factual influence. This has been introduced by the WP169 and has been affirmed in many case law where there is a complex scenario of processing procedure involving multiple characters.

The use of factual influence resulted from the functional concept character of controllership. [186] It means that, the controllership is primarily about allocating responsibility among each party and to efficiently allocate it, the assessment must be based on the reality of that processing procedure.

In SWIFT case, the contract between the SWIFT company and the financial institutions portrayed the legal status of company as a processor. However, the company could autonomously decide the means and purpose of the processing by developing and adapting the structure of a service and marketing scope.[187] These direct influences go beyond the scope of processor, which merely acts on behalf or according to the instruction of a controller, in this case, the financial institution. Without factual influence, SWIFT would have been considered as a processor, and thus avoid the responsibility of a controller. With the factual influence, SWIFT was considered a controller, despite what was written in the contractual agreement.[188]

Another similar issue was raised in the Wirtschaftsakademie and Jehovan todistajat. Without the factual influence, the responsibility can easily be artificially put on the party that possesses less negotiation's power and incorrectly reflect the controllership within the processing procedure.[189]

Finally, the third category, the joint controllership. This title was also presented in the WP169, which introduced the concepts of sharing control and varying degrees of responsibility among parties within a processing procedure.[190] Joint control means the parties jointly determine the means and purpose for a processing procedure.

In Wirtschaftsakademie case, Facebook is a service provider and has two establishments relevant to this processing procedure. One establishment is in the US and

[182] Case C-25/17 (n 169) [71].

[183] Case C-131/12 (n 6) [28], [29], [39].

[184] Case C-131/12 (n 6) [28], [29], [33], [41].

[185] Case C-210/16 (n 168) [64].

[186] Case C-131/12, 'Opinion of AG Jääskinen' (n 171) [83]; Case C-210/16 (n 168) [46].

[187] 29WP, 'WP128' (n 157) 10, 11.

[188] 29WP, 'WP128' (n 157) 11.

[189] Case C-210/16 (n 168) [60]; Case C-25/17 (n 169) [64] [69].

[190] 29WP, 'WP196' (n 12) 17.

responsible for developing Facebook's general economic model and storing the data of customers who reside in the European Union.[191] The other establishment is Facebook Ireland, which concluded the service agreement with the Wirtschaftsakademie.[192] And the control of the Wirtschaftsakademie are customizes the target audience[193], chooses the service provider and has power to end the service.[194] In this scenario, all parties have power to determine the means and purpose of the procedure in different ways. And the court decided that all three parties are a joint-controller in this processing procedure.[195]

A similar situation occurred in SWIFT. SWIFT has autonomously control in the processing of customer transaction through the service development and marketing strategy.[196] On the other hand, the financial institution exerts control by participating in the SWIFT board of directors and participating in decision making.[197] They both possessed controllership in the processing procedure.

All these cases concluded that controllership can vary in degree of involvement and responsibilities among controllers. The sharing of control need not be equally distributed between parties.[198]

Overall, in the Directive and the GDPR, controller is a legal status of an entity that decides the means and purpose for a processing procedure. This power needs to be implemented in a real scenario and there can be more than one entity that can exercise this power. A processor is a party that acts on behalf of a controller or according to its instructions. Any autonomous action of a processor is a factor that can change its legal status to a controller.[199]

2.3 THE CONTROLLER AND THE PROCESSOR IN A CLOUD COMPUTING CONTEXT

The interpretation of the legal status of controller previously mentioned can also be used within the processing procedure of cloud service. In processing procedure of cloud service, it primarily cooperates with two main actors which are a cloud service provider and a cloud customer. A cloud service provider is an entity who provides a cloud service facility to the customer. And a cloud customer is an individual or legal entity that requests the service from cloud service provider.

There are four main legal status scenarios of a cloud service provider: processor, controller, joint controller, and neutral intermediary. These are explained below.

[191] Case C-210/16 (n 168) [48] [50].

[192] Ibid [47], [50].

[193] "The 'Facebook Insights' tool is a feature which allow a fan page administrator to influence the specific way in which that tool is put to use by defining the criteria for the compilation of the viewing statistics. By using the filters in Facebook Insights' tool, a fan page administrator can define a personalized audience, which enables him not only to narrow down the group of people to whom information relating to his commercial offer will be published, but also, and most importantly, to designate the categories of people whose personal data will be collected by Facebook" Case C-210/16 (n 184) [57]

[194] Case C-210/16 (n 168) [56], [57], [58].

[195] Ibid [42], [51], [73].

[196] 29WP, 'WP128' (n 157) 12, 13.

[197] Ibid 12, 13.

[198] Case C-210/16 (n 168) [63], [75], [76]; Case C-25/17 (n 169) [72]; 29WP, 'WP128' (n 157) 13.

[199] Information Commissioner's Officer (ICO), 'Data controllers and data processors: what the difference is and what the governance implications are' (n 150) 17-19

2.3.1 Cloud service provider as a processor

This scenario is the most assumed legal status of cloud service provider.[200] The author will first provide an example in a normal business scenario then later will compare it with a similar situation which happen in a cloud service scenario. This comparison is to provide an idea in the similarity in the extent of control which can happen in both contexts.

Example 1: In a normal business scenario, Company A operates a department store and decides to increase sales rate by introducing a sale promotion. So, they decided to outsource to a marketing team from Company B to conduct research into their customers and come up with a sale promotion. Company A needs to provide their customer data to Company B, which will process the data to figure out the best marketing strategy for a promotion. This procedure will be done according to the means and purposes Company A has established. Company A has listed a very detailed instruction for Company B to follow such as how to store the data, what types of server should be use and what security measure should be applied. The processing of client data will be performed by Company B, but this will be performed within the tightly controlled scope stipulated by Company A.

Example 2: In a cloud context scenario, Company A with the same purpose may opt for Company B's SaaS, which is a marketing software operating as a cloud service. It functions by using algorithm to processed data to analyze the target customers. Instead of hiring actual marketing staff from Company B, Company A signs a service agreement to upload their customer data to Company B's server. After that, the server will process the data and determine what the sale promotion of Company A should be. This procedure generates the same result as using a traditional outsourcing method, but with a different medium. With a cloud service, Company A still retains all authority they have in traditional outsourcing. It still determines the means and purpose for this processing procedure of their client's data. Company B will still be recognized as a processor in this processing procedure for Company A.

In both scenarios, Company B cannot autonomously make decisions that significantly affect the processing procedure; all actions must be authorized by Company A. This control by Company A will title it as a controller, with Company B acting as a processor.

2.3.2 Cloud service as a controller

In these scenarios, the author will present the situation where cloud service provider which usually assumed as a processor can also be a controller when it possesses enough autonomous in its actions.

Example 3: Using the same scenario as above, Company A is a department store while Company B is a cloud service provider, but in this case, Company B used the client

[200] Hon, Millard and Walden, (n 19); The European Network and Information Security Agency (ENISA) (n 8); Lisa J. Sotto, Bridget C. Treacy, and Melinda L. McLellan, 'Privacy and Data Security Risks in Cloud Computing' (Electronic Commerce & Law Report, 3 February 2010) <https://www.hunton.com/files/Publication/4845e31f-63d8-4f9a-9a36-a074e4170225/Presentation/PublicationAttachment/6f52b2fd-2973-48cc-9f23-c941f1e19358/Privacy-Data_Security_Risks_in_Cloud_Computing_2.10.pdf> accessed 8 May 2018.

data of Company A and processed it for their own advertising purposes, such as sending email ads.

This action extends beyond the scope of Company A's instruction and is irrelevant to the means and purpose of Company A. Additionally, Company A does not acknowledge or consent to such action. This leaves Company B in autonomous control over this set of data and establishes a new processing procedure. The new purpose of this process will be the analysis of A's client detail for advertisement of Company B. Including, Company B decided the means. In this scenario, even though the data set is the same as examples 1 and 2, Company B's email advertisements are a separate processing procedure. Therefore, Company B is a controller that holds absolute power in managing this data and processing procedure.

A real scenario, where former processor exceeded their authority and was later considered to be a controller is the SWIFT case.[201]

As a side note, one entity can be titled a processor in one processing procedure and act as a controller in another processing procedure. Such assessment should be conduct procedure-by-procedure.[202]

2.3.3 Cloud service as a joint controller

This scenario introduces a plurality of control, where multiple actors collectively decide the means and purpose for a processing procedure.[203]

Example 5: Company A want to install a new security system to store their data. Company A decided to use the cloud service of Company B where it offers a virtual infrastructure equipped with security measures. Company A is solely decided in what data will be stored within the cloud while Company B can autonomously decide in the security measure and the operation of the cloud. For example, Company B can analyze the data and decided to encrypt certain part of data, it can choose to create a mirror server and it can conduct system testing.

Company A is still responsible for choosing and assessing which data will be stored in the cloud and also decides in the overall scope of the cloud service. For example, only the customer's data will be stored in the cloud and Company B need to make sure that the cloud will ceaselessly operating without any problem. Company B needs to follow the overall instruction of Company A by choosing the security measure and other features that will together provide an error-free cloud to Company A as it deemed fit. Additionally, Company B still hold power in deciding how to execute the operation in order to provide an error-free cloud to Company A. From this allocation of responsibility, both companies are accountable for separate parts of the process such as security measure and management. Even if the degree and types of control vary, this does not mean that both company is not a controller in this processing procedure.[204]

In this scenario, both companies will be considered joint controllers in this processing procedure. However, with different degrees of responsibility, there can also be different degrees of liability in case of damage.

Example 6: Company A operates a social network platform in a cloud. The company has multiple establishments in various countries to manage its business. The

[201] 29WP, 'WP128' (n 157).

[202] 29WP, 'WP196' (n 12) 25; Hon, Millard and Walden, (n 19) 10, 12.

[203] Ibid (n 12) 4.

[204] Ibid (n 12) 8, 12, 26, 28; Case C-210/16 (n 168) [61]; Hon, Millard and Walden, (n 19) 11.

main establishment is in Netherlands, where all the decisions about corporate structure are made and implemented. Another establishment is in Germany where it controls the server system responsible for all customers in Germany, Austria and Belgium. Customers within that areas who want to use the platform need to conclude the service agreement with the establishment in Germany.

The responsibility of the Netherlands establishment is the function of the platform, including overall organization policy. Germany's establishment is responsible for operating the server within a specific area, including the security measures and customer service. With this distribution of control regarding processing customer data on the social network platform, both establishments function as a joint controller.

To summarize, four factors help assess the title of actors in a processing procedure.[205]

- Level of instruction: This helps determine the freedom of processor and how much control it can exert in one processing procedure.
- The monitoring of the controller: The level of monitoring by the controller can help estimate the autonomy of the processor in the processing procedure and show that how much the controller is in "full and sole control" in that procedure.
- Impression of controller to data subject: the expectation of the data subject caused by the image portrayed by the controller
- Expertise of parties: Traditional role or expertise in certain profession can be seen as one factor to determine the role of controller.[206]

2.3.4 Cloud service provider as a neutral intermediary

This case is a special scenario in which the cloud service only provides a facility to the customer. The cloud provider does not have any influence on the customer data—no access to the content, no method to modify or manage the content, etc.

Example 7: Company A runs a cloud storage service in which customers have complete control in utilizing the storage. The company only offers the storage and has the sole responsibility to keep the cloud's storage operating. Company A will have no practical way to gain access to or modify the data. All control is in the hands of the customer to manage the data and choose the security measures.

In this scenario, according to the WP29 and the case law mentioned in Section 3.2, Company A will be deemed a processor, because the aim of the customer, which is the controller in this procedure, is to have a workable cloud storage to store their information. The act of Company A in providing functional cloud storage to the customer will be seen as following the customer's instructions.

[205] 29WP, 'WP 169' (n 24) 28; 29WP, 'WP196' (n 12) 8.

[206] Information Commissioner's Officer (ICO), 'Data controllers and data processors: what the difference is and what the governance implications are' (n 150) [26-27]

The example for this expertise of parties has been clarified in the Wp169 page 28 as followed:

> "Example No. 21: Barristers
>
> A barrister represents his/her client in court, and in relation to this mission, processes personal data related to the client's case. The legal ground for making use of the necessary information is the client's mandate. However, this mandate is not focused on processing data but on representation in court, for which activity such professions have traditionally their own legal basis. Such professions are therefore to be regarded as independent 'controllers' when processing data in the course of legally representing their clients."

Some articles raise problems similar to the scenario in example 7.[207] They suggest that with this type of cloud, it is unreasonable for a cloud service provider to be deemed as a processor with significant responsibilities and liabilities. Another opinion is that the nature of the cloud computing itself has disrupted the foundation of the data protection. This foundation is based on the practice of traditional outsourcing where the location of the data is known, unlike with processing of cloud services.[208] The reason to support these arguments will be clarified below as a foundation argument in the issue called "the binary distinction problem" which has been introduced in the legal research paper by W. Kuan Hon and others.[209]

To begin with, the nature of cloud computing for example multiple location facilities, virtual infrastructures, service providers, customers and third parties made it difficult in the allocation of responsibilities among parties.[210] Moreover, there are many scenarios in cloud service that include a plurality of service providers and customers that share a joint-controllership.[211] This leads to a grey area in determining who is a controller and a processor in a cloud computing environment.

The binary distinction problem is defined as a problem where the cloud service provider sometimes serves merely as a neutral intermediary, without any control in the content of the customer but they will be deemed as a processor with much of legal obligations and labilities. This is because, the law required in all processing procedure all relevant actors need to be allocated the responsibility and liability through the entitlement of controller or processor. A cloud service provider, even with minimal connection also needs a legal status of either processor or controller. But even with the legal status of a processor seems too much burden for this type of cloud provider when compared with the minimal amount of power they retain.[212] The scenario of service provider as a utility infrastructure has not been clarified in the paper of WP169.[213]

An example of a cloud service provider as a utility infrastructure is a cloud service that offer software or hardware to the client.[214] This type of cloud provider does not have any knowledge to the content or practical access to the data and does not retain data in their system.

A second type of neutral cloud service provider is when the cloud provider only providing system's maintenances in the cloud system.[215] This means administrative functions such as checking and updating software and hardware to make sure that the cloud system is running smoothly. This includes any maintenance service that requires incidental but authorized access to data. This action is similar to hardware/software provider that sells or licenses their product and usually provides post-sale services, such as updating or maintenance. However, this software/hardware provider does not hold any liability as a processor.

[207] Hon, Millard and Walden, (n 19); Balboni (n 117) 6-7.

[208] Ronald Leenes, 'Who Controls the Cloud?' (IDP: Internet, law and politics e-journal, 2010) < https://pure.uvt.nl/ws/files/1306180/Leenes_Who_controls_the_clouds_110209_fulltext_with_url_no_permission.pdf> accessed 10 January 2018.

[209] Hon, Millard and Walden, (n 19).

[210] Leenes (n 207).

[211] Poullet and others (n 128).

[212] Hon, Millard and Walden, (n 19) 1.

[213] Ibid 14.

[214] Ibid 1, 24.

[215] Ibid 17, 24.

Third is a cloud provider that merely hosts data storage.[216] Storage is considered automatically temporary caching of data by the system to operate the system faster. Even with the storage of data, this cloud provider will not have any access to or knowledge of the data.

In all the above examples, the cloud service provider as a neutral intermediary should not be considered a processor.

For the neutral intermediary issue of the binary distinction problem, the author agrees that in the cases where the cloud service provider only functioned as utility infrastructure, maintenance function or hosting data, they should not be considered a processor. Because the responsibility and control that these neutral intermediaries have is less than what the law required them to do. They are also not a controller or joint controller, since these possess even more control and responsibility than a processor.

The term neutral intermediary should be restricted to cloud providers that have no practical access to data, knowledge of the nature of the data and do not permanently retain data. Including when the data is encrypted by the customer and cloud provider not possess any decryption key. Even if a cloud provider can access to such data, it still cannot know the nature of that data, for instance, whether it is personal data. Thus, this kind of cloud service provider should also be considered a neutral intermediary.

The author suggests that these cloud providers do not have much control in the management of data within the cloud, not to mention any influence in specific processing procedure. It does not have any power to manipulate such content, so it will be difficult to act on behalf of a customer to process the data.

To distinguish these types of neutral intermediaries, the author still agrees that the criteria used by court and WP29 are tenable. However, the criteria can also be improved by creating an exception similar to the exception of liability of intermediary service provider in the E-Commerce Directive that provides mere-conduit, hosting and caching.[217]

However, W. Kuan Hon suggested that the entire binary distinction of controller and processor should not be used in all cloud computing scenarios.[218] She also suggested a replacement with end to end accountability.[219]

[220] The author disagrees with this idea because the current interpretation system of controller and processor are justifiable in typical cloud scenarios (examples 1–6). The author supports the methods that the court and WP29 introduced, such as using factual influence, broad interpretation and plurality of controllership. These methods by the court and WP29 are still considered effective tools in determining the legal status of a player

[216] Ibid 18, 19, 24, 26.

[217] Directive 2000/31/EC, article 12, 13, and 14.

[218] Hon, Millard and Walden, (n 19) 24.

[219] Hon, Millard and Walden, (n 19) 25.

[220] Information Commissioner's Office (ICO), 'The Information Commissioner's (United Kingdom) response to the European Commission's consultation on the legal framework for the fundamental right to protection of personal data in the European Union' (n 28).

An end-to-end accountability that has been mentioned here can be defined according to ICO, The Information Commissioner's response to the European Commission's consultation on the legal framework for the fundamental right to protection of personal data as

"… Liability could be assigned to the organisation, or organisations, that initiate the processing, whereas anyone processing personal data at any stage of the information life cycle should be responsible for dealing with it properly and securely and be accountable for their own aspect of the processing. This could mean being accountable to whoever initiated the processing; to individuals; to regulators; or all three."

in processing procedure. Moreover, this method of factual influence contains similar features with an end-to-end accountability which has been recommended by W. Kuan Hon. To completely abolish title of controller and processor will place too much burden on all parties in the EU, since much of practice and case law has already been structured according to this system.

The author supports abolishing the legal status of controller and processor only in the scenario of neutral intermediary of a cloud service provider. With the normal scenario, where a cloud service provider does hold certain kinds of control, it should be accountable with the responsibility of a controller, joint controller or processor as usual.

To conclude, the legal status of a cloud service provider under the Directive and GDPR will still be a controller, a joint controller, a processor or a sub-processor, as explain in examples 1–7. However, the author suggests that the status should be amended for the scenario in example 7, where a cloud provider does not possess an effective control in a data and to receive a legal status of a controller or even processor will be too unjustifiable a burden. The author suggests using a legal status of a neutral intermediary with this type of cloud providers.

Chapter 3

The Assessment of the Legal Status of the Cloud Service Provider in the GDPR in the Context of Complete Protection of Data Subject.

In this chapter, the author will first define the principle of complete protection of the data subject that will be used in an assessment (3.1). Later in the chapter, the interpretation of the legal status of the cloud provider in light of the GDPR and case law will be discussed (3.2). The author will answer the question regarding whether the legal status of a cloud provider in the GDPR can provide complete protection to the data subject or not including any suggestions and recommendations for the GDPR (3.3).

3.1 WHAT IS COMPLETE PROTECTION OF THE DATA SUBJECT?

In a Google Spain,[221] the principle of complete protection of the data subject was defined in which the court clarified the legal principle that should be used to interpret the scope of data protection law.

The principle of complete protection of the data subject is a way that courts reject an application of a principle of proportionality to narrowing the scope of data protection law. The principle of proportionality was proposed by Advocate General Jääskinen with the aim to prevent an excessive legal consequence[222] and concluded that a search engine provider is not a controller.[223] However, the judge disagreed because such an application can pose a threat to the fundamental rights to privacy and to protection of personal data.[224] A search engine provider is not subject under data protection law, and the scope of data protection law can be interpreted broadly with an aim to uphold the objective of the provision to ensure an effective and complete protection of the data subject.[225] The search engine provider should be accounted for as a controller in establishing an index of a search result. [226]

> “Inasmuch as the activity of a search engine is therefore liable to affect significantly…. the fundamental rights to privacy and to the protection of personal data, the operator of the search engine… must ensure…the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved.”[227]

In brief, the approach of the court’s interpretation of principle of complete protection of the data subject is to ensure the protection of fundamental rights and freedoms of the data subject with a complete protection against infringement from a processing procedure. The court illustrated such protection by rejecting the use of the principle of proportionality to interpret the scope of the Directive in Google Spain.

[221] Case C-131/12 (n 6).
[222] Case C-131/12, ‘Opinion of AG Jääskinen’ (n 171) [21].
[223] Ibid [82] [84] [86]; 29WP, ‘WP 169’ (n 24) [59].
[224] Case C-131/12 (n 6) [34].
[225] Ibid [38] [66].
[226] Ibid [28] [29] [33] [35]; Case C-131/12, ‘Opinion of AG Jääskinen’ (n 171) [44].
[227] Ibid (n 6) [38].

3.2 THE ASSESSMENT OF THE CLOUD SERVICE PROVIDER'S LEGAL STATUS UNDER THE PRINCIPLE OF COMPLETE PROTECTION OF THE DATA SUBJECT

In this section, the assessment will begin with the example scenario of a cloud service provider that was illustrated in Chapter 2. Then, the author will link scenarios to the importance of the provision of GDPR to see whether it can provide a complete protection to the data subject or not.

3.2.1 Cloud service provider as a processor

From the example[228] in chapter 2, where Company A used Company B's SaaS to analyze its customers' data, following Company A's instructions to come up with a new marketing strategy, a cloud service provider ("Company B") will be considered as a processor in this processing procedure. This is because Company B holds no control to solely decide in the means and purposes of the processing procedure. With the legal status of a processor, Company B will possess major obligations under GDPR, as follows:

(a) The Prior Written Authorization for a Sub-processor
Article 28 (2) GDPR

This obligation will force Company B as a cloud service provider and a processor to ask for consent from Company A, a controller, before acquiring sub-processors, including any changes relevant to already existing sub-processors. Such consent must be done in a formal written authorization format. With this obligation, controller will have knowledge of all sub-processor participated in the processing procedure.

For a data subject whose personal information has been collected by Company A and processed by Company B or Company A as a data subject itself, this can be considered an improvement for better data protection. First, this will create a much stronger and clearer connection between all relevant parties who contributed to the processing procedure. In case of any damages, the data subject can pinpoint more easily who is failing to fulfill their responsibilities since the data subject will have knowledge of all relevant processors and their sub-processors in Company B. This knowledge resulted from the data subject as a controller has been informed of all participated sub-processor or it can require such information from a controller directly. Contrary to prior practice where processor can covertly and autonomously employ any sub-processors.

Second, the data subject will have more liable parties to file a claim against in case of damage. If a data subject does not succeed in demanding a remedy from the main

[228] Example 2: In a cloud context scenario, Company A comes up with a new marketing strategy and opts for Company B's SaaS, which is a marketing software operating as a cloud service. It functions by using algorithms to process data to analyze the target customers. Instead of hiring actual marketing staff from Company B, Company A signs a service agreement to upload their customer data to Company B's server. After that, Company B's server will process the data and determine what the sales promotion of Company A should be. This procedure generates the same result as using a traditional outsourcing method, but with a different medium. With a cloud service, Company A still retains all authority it has in a traditional outsourcing. Company A still determines the means and purpose for this processing procedure of its clients' data. Company B will still be recognized as a processor in this processing procedure for Company A.

processor, Company B, it will still have knowledge of other sub-processors from which it can demand such remedy. This will provide better insurance that the data subject will receive a remedy.

Third, the obligation also offers the power to the controller to object to any use of sub-processors.

Consequently, this obligation will provide much stricter and clearer legal connections between each actor who takes part in processing procedures, namely, Company A, Company B and their sub-processors. Prior to the GDPR, the law only required a processor to processed data according to the instruction of the controller without specifically mentioning any rule for the sub-processor.

Altogether, this obligation upholds the principle of complete protection to a data subject because it provides a data subject with more knowledge and control of the processing procedure which, in case of damage, such information can assist in seeking a remedy.

However, to implement such an obligation in a real scenario in a cloud service, this process may face obstacles. In the cloud's practice, the customers or controllers do not have much power to choose or negotiate which sub-processor they prefer with the cloud service provider.[229] For example, Company A may not have the power to object to or influence which sub-processor Company B will choose since it needs to depend on Company B's service.

Also, the cloud usually comes in a package bundle, which means that it is usually comprised of several layers of add-on functions provided by different cloud providers. The majority of cloud providers offer the service in a take-it-or-leave-it manner.[230] For example, Company B's cloud service was comprised of layers of sub-processors even before Company A's arrival. The already existing sub-processors means that Company B's cloud service has already made agreements with all the sub-processors who operate in its cloud. The only decision left for Company A is to either choose to agree with the term or not use Company B's service at all. If Company A is only a start-up company with minimal negotiating power, it will not have any influence on Company's B decision.[231] Only powerful customers with enough resources and bargaining power will succeed in negotiating the cloud service agreement. And thus, the lacking in the negotiation power can mitigate the effect of the complete protection to the data subject that the law is aiming for.

(b) The Same Obligation's Requirement Between Sub-processor and a Processor Article 28(4) GDPR

For this obligation, the GDPR requires all sub-processors be bound by the same controller-processor relationship. This means that all sub-processors of Company B will need to act under instruction from Company A, a controller. Additionally, the sub-processor will also be bind with other obligations provided in the GDPR.[232]

[229] W. Kuan Hon, 'Killing Cloud Quickly, with GDPR?' (SCL, 2 February 2016) < https://www.scl.org/articles/3583-killing-cloud-quickly-with-gdpr > accessed 4 February 2018.

[230] Ibid.

[231] W Kuan Hon and others, 'Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation' (Queen Mary Legal Studies Research Paper172/2014, 2014) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2405971> accessed 2 February 2018.

[232] W. Kuan Hon, 'Dark clouds? Are Regulations Being Applied to Cloud Computing in a Way that Stimulates Innovation, Asks Kuan Hon' (International Institute of Communication (ICC), January 2016) <

The benefit is a decreasing supervisor burden for a data subject, whether it is a controller within this procedure or not, because all sub-processors will be contractually bound by the same obligation as the main processor. So whatever obligations Company A as a data subject and controller agrees with Company B as a processor will also automatically bind Company B's sub-processors. The main priority for Company A is to choose credible processors who provide efficient safeguards in the processing procedures. In the event that a data subject is not a controller in this procedure, it needs to choose a credible controller in order to be confident that its data will be carefully supervised and protected.

Moreover, the data subject will have the same benefit as mentioned in (a), that this obligation will create much stronger and clearer connections to all sub-processors used in a cloud service. In case any damage occurs, this legal binding can be used to file a claim directly against liable sub-processors. Company A or the data subject can directly file a claim against a sub-processor without having to first check the contractual agreement between Company B and that sub-processor. The GDPR requires all sub-processors to be bound with the same obligations with a processor so there is no need for Company A and the data subject to check a service agreement between Company B and its sub-processor. Consequently, the data subject and cloud's customer will have an easier and faster channel to seek a remedy. And these accumulations will result in a better and more complete protection to the data subject, where it can execute its right in a more convenient way. However, in exchange for this, the customer and data subject may have to pay a higher price for the cloud service since the processor and its sub-processor will be responsible for more obligation and liability.[233]

Superficially, this is a good example of upholding the principle of complete protection for the data subject, but in practice, this will not provide as much advantage as it seems. Sub-processors in this scenario can be infrastructure providers hired by Company B, such as data center operators or internet connectivity service providers. These third-party sub-processors such as connectivity providers can only gain access to non-secure encrypted data or encrypted data in an unintelligible form. And when the data is intelligible, there is no need to bind the sub-processor under the same obligation and liability with a processor who actually handles the personal data.[234] Also, most third-party sub-processors would not agree to sign the contract and carry such a burden of obligation. This leads to a similar result with (a) where only a large company with bargaining power can comply: it can force the processor and sub-processor to be bound with a mirroring contract.

The hardest part, other than forcing all sub-processors to be bound in a contractual agreement, is to bind them with the same level of obligation as the main processor.[235] This is simply because some sub-processors do not bear the same amount of maneuvers as the main processor and do not think that they deserve such strict obligation: consider the nature of any business that wants to escape from any possibility of liability as much

http://www.iicom.org/intermedia/intermedia-past-issues/intermedia-january-2016/dark-clouds> accessed 6 February 2018.

[233] W Kuan Hon, 'Data Protection: Controllers, Processors, Contracts, Liability – the ICO draft Guidance' (SCL, 10 June 2017) < https://www.scl.org/articles/10017-data-protection-controllers-processors-contracts-liability-the-ico-draft-guidance > accessed 13 February 2018.

[234] Ibid.

[235] Hon, 'Killing Cloud Quickly, with GDPR?' (n 228).

as it can. And this will force them to craftily find a legal loophole to avoid such obligation and will overall deteriorate the complete protection of the data subject.

For example, Company B outsourced to five other sub-processors who oversee internet connectivity issues in Company B's cloud service. They are only responsible for internet connectivity and do not have any access to Company A's data. They will not want to bear any responsibility related to Company A since in their view, they possess no connection with Company A. However, in the case where Company A dominates a market, it can order all sub-processors to agree, and it may present enough incentive for all sub-processors to be bound with Company A in order to create its business's profile or freeload on Company A's reputation in a market.

However, apart from the impracticality, if this obligation can be implemented, the tradeoff for decreasing overseeing the burden of a data subject will be a much higher price for the cloud service. Since the processor and its sub-processor will be responsible for more obligation and liability, it surely will do anything to regain its benefit.[236]

(c) The Clarification of the Processing Procedure
Article 28 (3) GDPR

This article will require the data subject/controller, namely, Company A, to provide an extensive amount of information which can be confidential information of a company or individual. For example, Company A will also need to formulate and highlight its plan, plus strategies of the company that can be valuable for competition in the market. With this provision, Company A is forced to hand over its confidential information to use Company B's cloud service.[237]

The advantage of this obligation is that it can be served as legal evidence in case of any problem related to the usage of such personal data. For example, if the data subject is a third party, it can easily know whether its personal data, which has been collected by Company A, has been used as agreed-upon or not because in the contract between Company A, a controller and Company B, a processor will explicitly list all details of processing procedures, such as the duration, nature, purpose of procedure and so forth. The data subject can easily determine whether any detail differs from what Company A has promised.

To provide complete protection to the data subject through this obligation, there is a need to establish a cautious procedure to regulate such a contract. Because the contract will contain much more personal data than a normal cloud's service contract, it needs to be protected from unauthorized disclosure to unnecessary parties. For example, when the contract is agreed upon, both Company A and B need to keep the contract confidential; only relevant parties, such as legal departments, etc., can have access to such documents.

The author understands that this provision is contradictory to the idea of protecting personal data because it forces the data subject or cloud customer to disclose such personal data to other parties or even third parties.[238]

To put this in practice will have a huge impact on the nature of cloud service, which may not be favored by both providers and users. Customers usually choose a cloud service because of its self-service nature -- its ability to manage their own data without third parties interfering. A customer will agree to a click-wrap agreement and right away start

[236] Hon, 'Data Protection: Controllers, Processors, Contracts, Liability – the ICO draft Guidance' (n 232).
[237] Hon, 'Killing Cloud Quickly, with GDPR?' (n 228).
[238] Ibid.

operating his or her own cloud without much requirement or detail in the processing procedure. But this provision will require the opposite of the cloud nature, in that customers must disclose all of their strategies and plans, including their personal data, to the service provider, which is contrary to the data protection principle.[239]

To implement this provision, a cloud provider must reformulate its service agreement, which it usually offers on its website, to sustain all the requirement details and establish security measures to keep such data safe. This could influence the cloud provider to raise its service fee.

(d) The Informing Duty of a Processor
Article 28 (3) GDPR

This obligation is an absolute responsibility of the cloud service provider and is generally named as the "policing processor." [240] This will force Company B as a cloud service provider and a processor to perform a legal advising task to Company A. The advice must be given in case Company A's instructions could possibly infringe on the GDPR or Member State data protection law.

To a data subject and a controller, this obligation is beneficial because it provides another entity to oversee the legality of the processing procedure apart from the controller itself. And since a processor who holds such a legal advising task is a cloud service provider who has an insight and knowledge in cloud service, this will make the advice even more useful and suitable to the circumstances. The advice will equip a data subject to better protect its personal data and ensure the complete protection of the data subject.

Nevertheless, in practice with a large number of cloud customers, it will be impossible to give legal advice to all customers, including the requirement to immediately inform the controller. For example, Company B, which offers SaaS services to Company A, may have a thousand customers, which would make it impossible to specifically tailor the advice to each customer.

One can argue that this can be done by using more manpower to monitor all customers or by investing in high-quality monitoring software. However, this will heighten the risk of a cloud service provider conducting a general monitoring of their client's data without a legal basis. If Company B opts to use a general monitoring practice to gain insight and knowledge in each cloud, including Company A, in order to customize its advice, such action is prohibited.

However, to avoid infringing upon the law, the processor may try to give general advice that does not specifically relate to a processing procedure or helpfully aid a data subject. For example, Company B may give advice for all customers, including Company A, to regularly change their cloud's password or not to store valuable data without prior encryption. The advice is provided in a very general scope and does not constitute any better protection of personal data in the cloud system. To make matters worse, there can be a case where the cloud service provider requests remuneration in exchange for more precise and specific advice, which will only put more financial burden on the cloud's customer or data subject.

[239] Ibid.

[240] W. Kuan Hon, 'Open Season on Service Providers? The General Data Protection Regulation Cometh.' (SCL, 8 April 2015) < https://www.scl.org/articles/3430-open-season-on-service-providers-the-general-data-protection-regulation-cometh> accessed 10 February 2018.

(e) The Implementation of Appropriate Security Measures
Article 32 (1) GDPR

The obligation requires Company B as a processor to install an appropriate security measure to ensure the security of a cloud system. The measure needs to harmonize with each processing procedure of Company B's cloud system.

All cloud services will install, more or less, a security measure in their cloud -- but the special part of this obligation is where a security measure must be appropriated with each processing procedure that occurs within the cloud. For example, Company B may offer the encryption feature to Company A because it processes personal data that can adversely affect the data subject in case of unauthorized disclosure. However, for another customer who does not process personal data, such an encryption feature may not be necessary. This obligation will help equip each processing procedure to withstand any misconduct or threat. It will help ensure the security of the cloud to all data subjects and cloud customers and help guarantee that their cloud service is supplied with sufficient safeguards and is able to provide complete protection to the data subject.

Nonetheless, the customization of a security measure to each cloud's customers can be impractical due to the number of customers in the service.[241] With the nature of the standardized cloud itself, which is usually offered in ready-to-use and take-it-or-leave-it fashion, all measures will already be readily provided before the customer starts the processing procedure. To provide a customized security measure to each processing procedure, the cloud provider first needs to know the nature of such procedures. However, to obtain such knowledge will go against the self-service nature of cloud provider, which normally does not have any knowledge of the customers' processing procedures. Sometimes the cloud provider needs to change the structure of its services in order to access the customers' data or at least gain sufficient knowledge of the nature of such data in order to customize an appropriate security measure to such cloud. This can lead toward the disclosure of the customers' personal data, which contradicts the objective of the data protection principle.

The problem can be solved by offering all services with the maximum level of security.[242] This may, however, result in wasting a lot of manpower and other resources for certain processing procedures that don't need such an intense level of security. For example, other customers of Company B's cloud may use its cloud to store only non-personal data, and to apply encryption features, a firewall system or a double verification system to such a procedure seems unnecessary.

(f) The Liability of a Controller and a Processor
Article 82 GDPR

In the pre-GDPR structure, the processor does not have a direct liability. The creation of the GDPR adds a new area, where the processor could get sued directly for the entire damage.[243]

This is useful for the customer and data subject because they can file one claim for the entire damage instead of filing multiple claims to separate processors, sub-

[241] Hon, 'Killing Cloud Quickly, with GDPR?' (n 228).

[242] W. Kuan Hon, 'GDPR: Killing Cloud Quickly?' (iapp, 17 March 2017) < https://iapp.org/news/a/gdpr-killing-cloud-quickly/> aceesed 10 February 2018.

[243] Hon, 'Open Season on Service Providers? The General Data Protection Regulation Cometh.' (n 239).

processors or other relevant actors.[244] Moreover, the right to sue for the entire damage will guarantee more chances for the data subject to get full compensation for their damages.[245] Such developments will provide a data subject with a more convenient way to seek a remedy in the event of any damages.

The GDPR also did not limit the damage to only financial matters; this can be interpreted widely and cover all damage that has occurred, whether financially related or not.[246] Data subjects or any person who suffers damages will benefit from this broad interpretation and have a chance to get a remedy for all damages.

However, the cloud provider will surely try to escape from or limit their liability. A cloud provider will try to add a limitation clause in the service agreement to protect themselves from being liable for any damages. For example, it can limit categories of data that can be uploaded into the cloud to protect sensitive personal data, it can restrict certain purposes for processing that possess a high risk of threat, or it can exempt itself from certain responsibility. In this case, the cloud customer and data subject need to carefully assess the service agreement before signing up or else risk finding themselves in a disadvantaged position where the service provider is exempt from all important responsibility.

3.2.2 Cloud service provider as a controller

In these examples[247], the cloud provider will be accounted for a controller or a joint-controller. The reasons for this are that both Companies share certain controls in a different areas of processing procedure where they can independently decide on the

[244] W. Kuan Hon, 'Could Cloud Vendors Dump Big Customers to Avoid Shared liability Once GDPR is Enacted?' (Computing, November 2017) <https://webcache.googleusercontent.com/search?q=cache:oVztIosHXnEJ:https://www.computing.co.uk/ctg/news/3020801/could-cloud-vendors-dump-big-customers-to-avoid-shared-liability-once-gdpr-is-enacted+&cd=1&hl=en&ct=clnk&gl=nl&client=safari> accessed 10 February 2018

[245] Hon, 'Open Season on Service Providers? The General Data Protection Regulation Cometh.' (n 239).

[246] Hon, 'Could Cloud Vendors Dump Big Customers to Avoid Shared liability Once GDPR is Enacted?' (n 243).

[247] Example 3: Using the same scenario as above, Company A is a department store while Company B is an outsourcing company or a cloud service provider, but in this case, Company B used the client data of Company A and processed it for its own advertising purposes, such as sending email ads. This action extends beyond the scope of Company A's instruction and is irrelevant to the means and purposes of Company A. Additionally, Company A does not acknowledge or consent to such action. This leaves Company B in autonomous control over this set of data and establishes a new processing procedure of its own. The new purpose of this process will be the analysis of A's client detail for the advertisement of Company B. Moreover, Company B also decided on the means. In this scenario, even though the data set is the same as examples 1 and 2, Company B's email advertisements are a separate processing procedure. Therefore, Company B is a controller that holds absolute power in managing the data and processing procedure.

Example 5: Company A wants to install a new security system to store its data. Company A decided to use the cloud service of Company B, where it offers a virtual infrastructure equipped with security measures. Company A solely decided which data will be stored within the cloud while Company B can autonomously decide on the security measure and the operation of the cloud. For example, Company B can analyze the data and decide to encrypt certain parts of the data, and it can also choose to create a mirror server and conduct system testing. From this allocation of responsibility, both companies are accountable for separate parts of the process, such as security measures and management. This entitles both Company A and B as joint-controllers in this processing procedure.

means and purpose within the same processing procedure. With legal status as a controller or a joint-controller, the obligations will be provided by the GDPR as follows:

(a) The Implementation of an Appropriate Security Measure
Article 32 (1) GDPR

This obligation falls in the perspective of the processor, which has already been mentioned in 4.2.1(e). For a controller, it requires a similar implementation. Controllers in Company A and B need to install a credible and effective security measure to ensure the protection of personal data in the processing procedure.

This will guarantee double protection for the data subject and its personal data from both controller and processor. The law is required to not only install a security system but also a system that is appropriate to the processing procedures. The controller must consider the characteristics of the processing procedure before applying any safeguards. And because the controller in cloud service is a primary actor who executes the processing procedure, that means it will have the best insight and knowledge of such a procedure.

In this scenario, Company A and B are both controllers, which will give a different result from what was illustrated in 4.2.1(e), when Company B as a cloud provider and processor cannot practically and effectively implement the very same obligation. The result is different when a cloud service provider has a legal status as a controller or a joint-controller because this means that in one way or another, it possesses enough room to maneuver within that processing procedure, including having enough knowledge in that specific processing procedure to be able to decide which security measure is appropriate.

This obligation is much more practical from the perspective of a controller. This is because the controller has actual control and knowledge of its own processing procedures in a cloud, unlike a cloud provider and a processor. In cloud service, the controller is the one who manages the processing procedure and thus enables it to customize its own security system. In addition, the amount of processing procedures it controls will surely be fewer than those of a cloud service provider, which commercially functions as a cloud provider. The number of clouds is another factor that renders this obligation impractical in the perspective of a cloud provider with the legal status of a processor. This obligation on the controller presents an opposite practical result when it is placed on a processor. The author considered this as an improvement, where it supports the principle of complete protection of the data subject by providing personal data in effective and appropriate security measures.

(b) The Data Protection by Design and Default
Article 25 GDPR

The data protection by default and design can be separated into two parts. The "by design" part provides the encouragement to apply the principle of data protection from the first step of the processing procedure. The implementation should be in both technical and organizational measures, with the aim to safeguard the personal data.[248] For example, Company A should establish an internal organizational policy embedded with a data

[248] European Commission, 'What does data protection 'by design' and 'by default' mean?' (European Commission) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en#references> accessed 16 April 2018.

protection principle prior to the processing procedure and not initiate such a policy after damage has occurred.

The second part is "by default," which means that the processing procedure should process the data with the highest level of data protection measures. For example, when gathering personal information, the collection should be limited to only what is necessary to reach its purpose. For example, Company B's cloud security setting should include all access to the cloud with a password verification method instead of offering it as an option for a cloud customer.

This obligation provides a similar effect as an obligation to implement appropriate security measures within the cloud service. With such a principle, the structure of processing procedures will cooperate with data protection measures and will not be treated as a remedy after the damage has occurred. The processing procedure in the cloud will provide better and additional complete protections to the data subject. As controllers, both Company A and B can comply with this obligation by including the principle of data protection by default and by design in their organizational policies, such as collecting personal data as necessary and encrypting sensitive and personal data to which only authorized personnel can have access. Also, they will not store data longer than is necessary.

(c) The Data Protection Impact Assessment[249]
Article 35 (1) GDPR

Before starting a processing processor, one must conduct a DPIAs in any procedure that poses a high risk to personal data or uses new technology. In order to assess the level of threat that can occur, safeguards or preventions must be established to mitigate any possible damage.

Conducting a DPIAs will help controllers identify and address risks that would otherwise not have been detected. This may help controllers avoid breaches of the GDPR that might otherwise have occurred. Overall, such a practice will provide more thorough protection to personal data and help mitigate any threat before it occurs. For example, if Company A decides to use cloud service to process personal data for the first time, it is more prudent to conduct a DPIAs to evaluate all possible threats and establish a safeguard. On the other hand, Company B as a cloud provider will process data from Company A, which contains sensitive information that can pose a high risk to a data

[249] A data impact assessment herein referred as a "DPIAs"

"A DPIA is required whenever processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA is required at least in the following cases:
a systematic and extensive evaluation of the personal aspects of an individual, including profiling; processing of sensitive data on a large scale; systematic monitoring of public areas on a large scale.
An example where DPIAs will be required are A bank screening its customers against a credit reference database; a hospital about to implement a new health information database with patients' health data; a bus operator about to implement on-board cameras to monitor drivers' and passengers' behavior."
For official guidelines on how to conduct an impact assessment, WP29 has issued an official guideline in WP248 (17/EN WP248) which provide further clarity on the requirements around Impact Assessments < http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236>

European Commission, 'When is a Data Protection Impact Assessment (DPIA) required?' (European Commission) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en#references> accessed 16 April 2018.

subject. Company B may opt for a DPIA before offering its service to Company A to see an overall image and better prepare itself for possible damages.

To conduct a DPIAs, a cloud provider needs to know the details in their customer data in order to estimate whether there is a risk or not. In normal situations where a cloud provider is a processor, this step can be hard to fulfil since a cloud provider does not have any knowledge of its customers' procedures. Nonetheless, in this scenario, when a cloud provider is a controller or a joint-controller, the results differ. As a controller, a cloud provider has control of such a procedure and is able to obtain knowledge in processing procedures that make it possible to conduct a DPIAs.

Despite the benefit that a DPIAs can offer to a data subject, the assessment will exhaust many resources and use a lot of time since the examination will have to be done in all aspects. This can lead to an increase in price for a cloud service. Also, the provision required to conduct DPIAs prior to the processing procedure means that the customer cannot start processing until the DPIAs have been done. This obligation will impede customers who choose to use cloud service because of its ready-to-use anywhere and anytime feature.

(d) The Notification of Data Breach[250]
Article 33 GDPR

This obligation requires a controller to inform the data subject of when the data breach occurs within a 72-hour timeframe. Moreover, if such a breach can cause an adverse effect in the rights and freedoms of a natural person, the controller also must notify the supervisory authorities.

This obligation will provide a data subject with a right to know if any damage occurs regarding their personal data. In most cases, a cloud service would not be willing to share such information because it could adversely affect the service's reputation. This obligation, then, will offer the chance for a data subject to protect or mitigate any adverse effect that occurs, such as a transfer of their data to be stored in another location, a change in their login password, or an encryption of their data in the cloud.

According to the law, a breach that the controller must inform the authorities of would include unlawful access that only relates to the integrity and confidentiality of data. However, in WP250, the instructions differ and include a breach in availability as one of the breaches that need to be relayed to the authorities.[251] This can create confusion for the

"A data breach occurs when the data for which your company/organisation is responsible suffers a security incident resulting in a breach of confidentiality, availability or integrity. If that occurs, and it is likely that the breach poses a risk to an individual's rights and freedoms, your company/organisation has to notify the supervisory authority without undue delay, and at the latest within 72 hours after having become aware of the breach. If your company/organisation is a data processor it must notify every data breach to the data controller.

If the data breach poses a high risk to those individuals affected, then they should all also be informed, unless there are effective technical and organisational protection measures that have been put in place, or other measures that ensure that the risk is no longer likely to materialise.

As an organisation, it is vital to implement appropriate technical and organisational measures to avoid possible data breaches." <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en>

[251] Article 29 Data Protection Working Party 17/EN WP 250, Guideline on Personal Data Breach under Regulation 2016/679, 7.

cloud provider that tries to comply with these measures; hence, there is a need for harmonization in this matter.[252]

The provision requires the cloud provider to notify authorities of a breach after becoming “aware” of the incident. In WP250, “aware” means having a certain degree of certainty that such a breach has occurred and will lead to a potential risk of personal data being accessed.[253] The problem is that it is based on the presumption that the cloud provider has the means and the power to be sure that there has been a security breach within the system in such a short period. The timeframe of 72 hours is considered as a challenge since in practice it usually takes at least a few weeks just to identify the breach and assess its potential effect.[254] In the cloud, a cloud provider may not notice such a breach since it usually rents out its facilities without monitoring such usage.

Sometimes, the potential effect of a breach is uncertain, but non-compliance for breach notification can result in a significant fine, so this can lead to “just in case” notifications to avoid non-compliance liability. This is considered the best solution for all cloud providers: to notify data protection authorities even if they are not entirely sure whether a breach has occurred.[255] This way, a controller can partially comply with the obligation even if it means flooding the data protection authorities with “just in case” notifications.[256] However, this can cause a problem whereby the authorities must spend many resources to manage “just in case” types of notifications instead of solving those breaches that involve real and/or potential risks, including increasing widespread reputational harm as a consequence of a breach even if there is minimal actual potential adverse effect. With such type of notification and widespread reputational harm will not do any good in uphold the principle of complete protection of the data subject. It will just create unreliable distress for the data subject and impair the efficiency of data protection authorities.

3.3 CONCLUDING REMARKS AND SUGGESTION

To conclude, the author finds that the legal status that appears in the GDPR will be interpreted in a broad scope as it did in the Directive era. With such interpretation, this will cover much of the cloud provider’s activity to mainly fall into the status of processor or controller. It can also be considered as a sub-processor or a joint controller in a processing procedure. This means that most cloud providers will be entitled to take on a legal status and follow with legal obligations and liabilities in order to provide an effective and sufficient protection to the processing procedure of personal data.

This is considered a benefit to the data subject because relevant parties in processing procedures will be legally binding and can be liable in case of any damages that occur. Moreover, the GDPR has introduced many obligations for the processor which

[252] W. Kuan Hon, ‘What’s Wrong with WP29 guidelines on Personal Breach Notification Under GDPR?’ (iapp, 28 November 2017) <https://iapp.org/news/a/whats-wrong-with-wp250-guidelines-on-personal-breach-notification-under-gdpr/> accessed 1 February 2018.

[253] 29WP, ‘WP250’ (n 250).

[254] Detlev Gabel, and tim Hickman, ‘Obligations of controllers – Unlocking the EU General Data Protection Regulation’ (White&Case, 13 September 2017) <https://www.whitecase.com/publications/article/chapter-10-obligations-controllers-unlocking-eu-general-data-protection > accessed on 28 April 2018.

[255] Hon, ‘What’s Wrong with WP29 guidelines on Personal Breach Notification Under GDPR?’ (n 251).

[256] Ibid.

has not appeared in the Directive before; this will also ensure that all parties can be held accountable in the event of any misconduct. Together, this will help uphold the principle of complete protection of the data subject.

However, one problem impedes the effectiveness of the principle of complete protection of the data subject: the impracticality of the provision in the context of cloud service. Much of the provision that has been clarified above cannot be fully implemented in the cloud service due to the incompatibility between the nature of the cloud service and the foundation model of GDPR. The model of GDPR is based on a traditional outsourcing model where the exact location and tangible entity that processes the data in a one-by-one outsourcing system is known. On the other hand, cloud service is a virtual infrastructure with multiple add-on services, which makes it harder to pinpoint exact locations or entities that process the data, including the ability to provide service to multiple customers simultaneously.

The author proposes that there should be an amendment in the provision to be more technology-neutral since the GDPR is still unsuitable in cloud service scenarios. When much of the obligation cannot be effectively implemented, to escape from such heavy liability the cloud provider usually transfers such a burden to the customer in the form of higher service fees. An example of this would be when higher service fees are charged to install maximum levels of security measures to all customers when it is not necessary to all processing procedures. Otherwise, the cloud service will resort to inefficient measures simply to comply with the GDPR, such as the “just in case” notification.

In my opinion, the aim of the Regulation is to uphold the protection of personal data but with the uniqueness of the cloud service’s structure, this could lead to the opposite result. The application of the Regulation in certain provisions obliges the cloud provider to disclose more detail regarding the customer’s personal data, which is supposed to be kept private. For example, the obligation to clarify the detail of the processing procedure can cause the Regulation to resort to other means that do not lessen the level of privacy of personal data, which can serve as one proof of evidence that the Regulation is not neutral in technology.

Chapter 4

Conclusion

From the assessments, the author can answer the research question as follows;

1. A cloud service provider could acquire three possible legal statuses; a processor, controller and joint controller. Moreover, the author also suggests adding the legal status of a neutral intermediary to a cloud service scenario.

2. For the principle of complete protection to data subjects, the author found that when the cloud service provider possesses a legal status of a controller or a joint controller, it can provide an effective and better complete protection to data subjects. On the other hands, when a cloud service provider has a legal status of a processor, it cannot sufficiently uphold the principle of complete protection of data subjects.

Apart from that the author has other considerations as follows;

1. The interpretation method of the legal status that basing on the provision, WP29 and case law is still tenable and provide efficient interpretation to cover the complicated business's scenarios. The interpretation should always take in account both contractual and factual influence.

2. The author concluded that the GDPR is not technology neutral and thus, resulted in the legal status of a cloud service provider cannot sufficiently provide complete protection for data subjects. The insufficient protection results from multiple factors, namely, the outdated outsourcing model that the GDPR is basing on, the unawareness in the uniqueness of the nature of cloud computing and the imbalance in negotiation power of actors in the business. Due to the nature of the cloud service, which is different from a traditional computing method, the good intention of the law to uphold the complete protection of data subjects faces many obstacles in the implementation phase.

3. In the scenario that cloud service provider is a processor, most of the obligation and deteriorate the principle of complete protection of data subjects. The decreasing of complete protection is due to the insufficient control and knowledge in a processing procedure and the unawareness in the uniqueness of cloud infrastructure such that illustrated in the assessment of article 28(2) GDPR[257]. The obligation can only be fulfilled when data subjects occupy enough resources and bargaining power and more technology neutral provision. Lacking in these two factors can diminish the outcome of the complete protection to the data subject that the law is aiming for. This similar result also takes place in other obligations toward a cloud service provider

[257] the prior written authorization for a sub-processor

with legal status as a processor. For example, article 28(4) GDPR[258], article 28(3) GDPR[259], article 32(1) GDPR[260] and article 82 GDPR[261].

4. The principle of complete protection will be sustained when a cloud service provider has a legal status as a controller or a joint controller since it will enjoy more control and knowledge in that particular processing procedure. Consequently, many obligations which prove ineffective when cloud service provider serves as a processor can be effectively applied. For instance, article 32(1) GDPR[262], article 25 GDPR[263], article 35(1) GDPR[264] and article 33 GDPR[265]. These obligations can be applied to the cloud service's scenarios and thus, will not treat a data protection measure as a remedy after damages have occurred.

5. The notion of binary distinction of the legal status, , when a cloud provider falls into a neutral intermediary who function passively as utility infrastructure, hosting platform or maintenance administrator. Only these kinds of cloud providers should be exempt from existing legal statuses of a processor, sub-processor, controller, or even a joint controller. The author recommends that this kind of cloud provider should be referred to as a neutral intermediary.

6. The author recommends that there is a need to amend the GDPR to be more technology-neutral to harmonize with the more innovative technology that we will see in the future. Also, to be more flexible with the neutral intermediary, the GDPR can adapt the exemption for a neutral intermediary which was also provided in an E-Commerce directive to be used in the GDPR.

7. Lastly, for further research, it will be useful to consider case law and literature that occurs and is published after the GDPR has been enforced, as the author conducted this research prior to the enforcement of the GDPR. So, there are certain limitations to the practical issue which have not yet occurred, and much of the information needs to be based on literature in the time of the Directive.

[258] The same obligation's requirement between sub-processor and a processor.
[259] The informing duty of a processor.
[260] The implementation of appropriate security measure.
[261] The liability of a controller
[262] The implementation of an appropriate security measure.
[263] The principle of data protection by default and design.
[264] The DPIAs.
[265] The notification of data breach.

Bibliography

Legislation and Related Texts

European Legislation

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

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market

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)

Opinion

Article 29 Data Protection Working Party 01935/06/EN WP128, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 November 2006

Article 29 Data Protection Working Party 00264/10/EN WP 169, Opinion 1/2010 on the concepts of controller and processor", 16 February 2010

Article 29 Data Protection Working Party 0836-02/10/EN WP179, Opinion 8/2010 on applicable law, 16 December 2010

Article 29 Data Protection Working Party 03/12/EN WP196, Opinion 05/2012 on Cloud Computing, 1 July 2012

Article 29 Data Protection Working Party 16/EN WP 238, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, 13 April 2016.

Article 29 Data Protection Working Party 17/EN WP 248 rev.01, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, 4 April 2017

Article 29 Data Protection Working Party 17/EN WP250, Guideline on Personal Data Breach under Regulation, 3 October 2017

Case Law

European Court of Justice

Case C-131/12 Google Spain SL. v. Agencia Española de Protección de Datos (AEPD) (ECJ 13 May 2014)

Case C-131/12 Google Spain SL. v. Agencia Española de Protección de Datos (AEPD) (ECJ 25 June 2013), Opinion of AG Jääskinen

Case C-210/16 Wirtschaftsakademie Schleswig v Holstein (ECJ 24 October 2017), Opinion of AG Bot

Case C-25/17 Jehovan todistajat v. uskonnollinen yhdyskunta (ECJ 1 February 2018), Opinion of AG Mengozzi

Bibliography

Books

Bowen A. J., 'Legal Issues in Cloud Computing' in James Broberg, Andrezej Goscinski and Rajkumar Buyya (eds), Cloud Computing Principles and Paradigm (John Wiley & Sons Inc. 2011)

European Union Agency for Fundamental Rights, 'Handbook on European Data Protection Law' (Publication office of the European Union, 2014)

Furht B., 'Cloud Computing fundamental' in Borko Furht and Armando Escalante (eds), Handbook of Cloud Computing (Springer 2010)

Halper F., and others, 'Hybrid Cloud for Dummies' (John Wiley & Sons Inc. 2012)

Jin H., and others, 'Cloud Computing Technologies and Applications' in Borko Furht and Armando Escalante (eds), Handbook of Cloud Computing (Springer 2010)

Kuner C., 'European Data Protection Law Corporate Compliance and Regulation' (2nd edn, Oxford University Press, 2007)

Millard C., 'Cloud Computing Law' (OUP 2013)

Morrow S., 'Data Security in the Cloud' in James Broberg, Andrezej Goscinski and Rajkumar Buyya (eds), Cloud Computing Principles and Paradigm (John Wiley & Sons Inc. 2011)

Blokdijk G., and Menken I., 'Cloud Computing- The Complete Cornerstone Guide to Cloud Computing Best Practice' (EMEREO PTY Limited 2009)

Voorsluys W., Broberg J., and Buyya R., ‘Introduction to Cloud Computing’ in James Broberg, Andrezej Goscinski and Rajkumar Buyya (eds), Cloud Computing Principles and Paradigm (John Wiley & Sons Inc. 2011)

Zhu J., ‘Cloud Computing Technologies and Applications’ in Borko Furht and Armando Escalante (eds), Handbook of Cloud Computing (Springer 2010).

Article and Paper

Alsenoy V. B., ‘Allocating responsibility among controllers, processors, and “everything in between”: the definition of actors and roles in Directive 95/46/EC’ (2012) 28 Computer Law & Security Review 25-43 <https://ac.els-cdn.com/S0267364911001828/1-s2.0-S0267364911001828-main.pdf?_tid=dab0ab39-e5b0-45a5-bbd9-f7e5a15bdd32&acdnat=1526905339_050d4c9e3ac56ae8d4c05835c32347e1>

Avram G. M., ‘Advantages and challenges of adopting cloud computing from an enterprise perspective’ (2014) 12 529-534 <https://www.sciencedirect.com/science/article/pii/S221201731300710X> accessed 10 January 2018

Cave J. and others, ‘Regulating the Cloud: More, Less or Different Regulation and Competing Agendas’ (2012) TRPC <https://ssrn.com/abstract=2031695> accessed 18 November 2017

Ciriani S., ‘The Economic Impact of the European Reform of Data Protection’ (2015) 97 Digiworld Economic Journal 41 < http://ssrn.com/abstract=2674010>

Eeck V. P., and Truyens M., ‘Privacy and social networks’ (2010) 26 Computer Law & Security Review 535-546 <https://ac.els-cdn.com/S0267364910001093/1-s2.0-S0267364910001093-main.pdf?_tid=204ffa74-ab8b-46e5-92ee-209db59d4adc&acdnat=1526910933_7893972cb0105b2b933a96dda5d1ac99>

Grossman L. R., ‘The Case for Cloud Computing’ (2009) 11(2) IEEE 23-27 <https://pdfs.semanticscholar.org/fd95/05897a97b2f82a73148dc87ce3067a33c6ab.pdf> accessed 10 January 2018

Hayes B., ‘Cloud computing’ (2008) 51(7) ACM 9-11 <https://cacm.acm.org/magazines/2008/7/5368-cloud-computing/fulltext> accessed 10 January 2018

Kuan W. H., Millard C. and Walden I., ‘Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2’ (2011) 2 (1) IDPL 3 <https://ssrn.com/abstract=1794130> accessed 17 October 2017

Kulkarni G., Sutar R., and Gambhir J., ‘Cloud Computing-Storage as Service’ (2012) 2(1) IJERA 945-950

<https://pdfs.semanticscholar.org/8ad9/bab2356b6f397645d2dd4b2c7ae35485cd13.pdf > accessed 10 January 2018

Millard C. and Kuan W. H., ‘Cloud Computing vs Traditional Outsourcing—Key Differences’ (2012) 23(4) Computers & Law <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2200592> accessed 10 January 2018

Moerel L., ‘Back to basics: when does EU data protection law apply?’ (2011) 1(2) IDPL 92–110 <https://doi.org/10.1093/idpl/ipq009> accessed 10 October 2017.

Oprysk L., ‘The Forthcoming General Data Protection Regulation in the EU’ (2016) 24 Juridica International 23-31 <https://ssrn.com/abstract=3019917>

Vick W. D., ‘Interdisciplinarity and the Discipline of Law’ (2004) 31(2) Journal of Law and Society 177-178. <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-6478.2004.00286.x>

Voss G. W., ‘One Year and Loads of Data Later, Where Are We? An Update on the Proposed European Union General Data Protection Regulation’ (2013) 16(10) Internet Law Journal 14-24 < http://ssrn.com/abstract=2567622>

Voss G. W., ‘Looking at European Union Data Protection Law Reform through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later’ (2014) 17(9) Internet Law Journal 12-24 < http://ssrn.com/abstract=2567624 >

Online Article, Papers, and Blogs

Ali I. S., Yusoff M. Z., Ayub A. Z., ‘Legal Research of Doctrinal and Non-Doctrinal’ (Researchgate, January 2017), <https://www.researchgate.net/profile/Salim_Ali8/publication/316895684_Legal_Research_of_Doctrinal_and_Non-Doctrinal/links/5917225a4585152e19a102a3/Legal-Research-of-Doctrinal-and-Non-Doctrinal.pdf> accessed 30 October 2017.

Akintunde S., ‘An Analysis of The General Data Protection Regulation (EU) 2016/679’ (2007) <https://ssrn.com/abstract=2966210 ii>

Alsenoy V. B., ‘Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation’ (JIPITEC 2016) <http://www.jipitec.eu/issues/jipitec-7-3-2016/4506/van_alsenoy_liability_under_eu_data_protection_law_jiptec_7_3_2016_271.pdf>

Armbrust M., and others, ‘Above the Clouds: A Berkeley View of Cloud Computing’ (UC Berkeley Reliable Adaptive Distributed Systems Laboratory White Paper, 10 February 2009) < https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf> accessed 10 January 2018

Balboni P., ‘Data Protection and Data Security Issues Related to Cloud Computing in the EU’ (Tilburg University Legal Studies Working Paper Series No. 022/2010, 2010) <https://ssrn.com/abstract=1661437> accessed 10 January 2018

Badger L., and others, ‘NIST SP 800-146, Cloud Computing Synopsis and Recommendations’ (NIST, 2012) <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf> accessed 10 January 2018.

Buyya R., Pandey S., and Vecchiola C., ‘Cloudbus Toolkit for Market-Oriented Cloud Computing’ (2009) <http://www.cloudbus.org/papers/Cloudbus-Keynote2009.pdf> accessed 10 January 2018

Columbus L., ‘Forrester's 10 Cloud Computing Predictions For 2018’ (Forbes, 7 November 2017) <https://www.forbes.com/sites/louiscolumbus/2017/11/07/forresters-10-cloud-computing-predictions-for-2018/#2017784a4ae1> accessed 10 January 2018

Christian A., ‘The Advantages of Using Cloud Computing’ (@CloudExpo Journal, 14 April 2014) <http://cloudcomputing.sys-con.com/node/1792026> accessed 10 January 2018

Clark S., ‘Cloud computing in 2018: what the future holds’ (The Stack, 14 December 2017) <https://thestack.com/cloud/2017/12/14/cloud-computing-in-2018-what-the-future-holds/> accessed 10 January 2018

Cloud Industry Forum, ‘Cloud UK: Paper Four Cloud Adoption and Trends for 2012’ (2012) <https://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwim3Z_b9d_YAhWJLFAKHaA7DcgQFggzMAE&url=https%3A%2F%2Fwww.cloudindustryforum.org%2Ffile%2F121%2Fdownload%3Ftoken%3D1nfl3_ue&usg=AOvVaw06-af00NshQ9U4b6okOCbc> accessed 10 January 2018

Demary V., ‘The Platformization of Digital Markets: Comments on the public consultation of the European Commission on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy’ (Econster, 21 December 2015) <https://www.econstor.eu/bitstream/10419/126091/1/845730703.pdf> accessed 20 November 2017.

ENISA, ‘Cloud Security Guide for SMEs’ (ENISA, 2015) <https://www.enisa.europa.eu/publicatio ns/cloud-security-guide-for-smes> accessed 10 January 2018

European Commission, ‘Shaping the Digital Single Market’ (European Commission, 25 March 2015) <https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market#The%20Strategy> accessed 20 November 2017.

European Commission, ‘What does data protection ‘by design’ and ‘by default’ mean?’ (European Commission) <https://ec.europa.eu/info/law/law-topic/data-

protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en#references> accessed 16 April 2018

European Commission, 'When is a Data Protection Impact Assessment (DPIA) required?' (European Commission) < https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en#references> accessed 16 April 2018

European Commission, 'What is a data breach and what do we have to do in case of a data breach?' (European Commission) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en> accessed on 16 April 2018

Freedman B., 'Cloud services – guidelines for service level agreements European'(Lexology, 16 October 2014) <https://www.lexology.com/library/detail.aspx?g=7202771e-3161-401b-aa87-1d550999bdb3> accessed 19 November 2017.

Gabel D., and Hickman T., 'Obligations of controllers – Unlocking the EU General Data Protection Regulation' (White&Case, 13 September 2017) <https://www.whitecase.com/publications/article/chapter-10-obligations-controllers-unlocking-eu-general-data-protection > accessed on 28 April 2018

Hess K., 'Why You Need Infrastructure as a Service (IaaS)' (The Frugal Networker, 7 January 2012) <https://frugalnetworker.com/2012/01/07/why-you-need-infrastructure-as-a-service-iaas/> accessed 10 January 2018

Heywood D., 'Obligations on Data Processors Under the GDPR' (Lexology, June 2016) < https ://www.lexolog y.com/library/detail.aspx?g=61ffb705-d822-47b0-8d4e-f923471bf67d > accessed 18 November 2017.

Hutchinson T., Duncan N., 'Defining and Describing What We Do: Doctrinal Legal Research' (Deakin Law Review, 2017) <https://ojs.deakin.edu.au/index.php/dlr/article/view/70>)> accessed 30 October 2017.

Huth A., and Cebula J., 'The basics of cloud computing' (US-CERT, 2011) <https: //www.us-cert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf> accessed 10 January 2018

Information Commissioner's Officer, 'Data controllers and data processors: what the difference is and what the governance implications are' (ICO, 2014) <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf> accessed 10 January 2018

Jansen W. and Grance T., 'NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing. (NIST, 2011) <http://nvlpubs.nist.gov/nistpubs/ Legacy/SP/nistspecialpublication800-144.pdf> accessed 10 January 2018

Koenigsbauer K., 'Announcing Office 365 for Government: A US Government Community Cloud' (Silicon, 30 May 2012) < http://www.silicon.co.uk/workspace/microsoft-office-365-government-80702?print=pdf> accessed 10 January 2018

Koomey J., '4 reasons why cloud computing is efficient' (REUTERS, 25 July 2011) <http://www.reuters.com/article/2011/07/25/idUS59089929820110725> accessed 10 January 2018

Kuan W. H., 'Open Season on Service Providers? The General Data Protection Regulation Cometh.' (SCL, 8 April 2015) < https://www.scl.org/articles/3430-open-season-on-service-providers-the-general-data-protection-regulation-cometh> accessed 10 February 2018

Kuan W. H., and others, 'Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation' (Queen Mary Legal Studies Research Paper172/2014, 2014) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2405971> accessed 2 February 2018

Kuan W. H., 'Dark clouds? Are Regulations Being Applied to Cloud Computing in a Way that Stimulates Innovation, Asks Kuan Hon' (International Institute of Communication (ICC), January 2016) < http://www.iicom.org/intermedia/intermedia-past-issues/intermedia-january-2016/dark-clouds> accessed 6 February 2018

Kuan W. H., 'Killing Cloud Quickly, with GDPR?' (SCL, 2 February 2016) < https://www.scl.org/articles/3583-killing-cloud-quickly-with-gdpr > accessed 4 February 2018

Kuan W. H., 'GDPR: Killing Cloud Quickly?' (iapp, 17 March 2017) < https://iapp.org/news/a/gdpr-killing-cloud-quickly/> aceesed 10 February 2018

Kuan W. H., 'Data Protection: Controllers, Processors, Contracts, Liability – the ICO draft Guidance' (SCL, 10 June 2017) < https://www.scl.org/articles/10017-data-protection-controllers-processors-contracts-liability-the-ico-draft-guidance > accessed 13 February 2018

Kuan W. H, 'Could Cloud Vendors Dump Big Customers to Avoid Shared liability Once GDPR is Enacted?' (Computing, November 2017) <https://webcache.googleusercontent.com/search?q=cache:oVztIosHXnEJ:https://www.computing.co.uk/ctg/news/3020801/could-cloud-vendors-dump-big-customers-to-avoid-shared-liability-once-gdpr-is-enacted+&cd=1&hl=en&ct=clnk&gl=nl&client=safari> accessed 10 February 2018

Kuan W. H, 'What's Wrong with WP29 guidelines on Personal Breach Notification Under GDPR?' (iapp, 28 November 2017) <https://iapp.org/news/a/whats-wrong-with-wp250-guidelines-on-personal-breach-notification-under-gdpr/> accessed 1 February 2018

Kuner C., ‘European data protection law: Corporate compliance and regulation’ (Oxford University Press, April 2008) http://global.oup.com/booksites/content/9780199283859/updates/170420083 accessed on 10 January 2018

Leenes R., ‘Who Controls the Cloud?’ (IDP: Internet, law and politics e-journal , 2010) < https://pure.uvt.nl/ws/files/1306180/Leenes_Who_controls_the_clouds_110209_fulltext_with_url_no_permission.pdf> accessed 10 January 2018.

Leung L., ‘ Cloud Customers Report Capital Cost Savings’ (Data Center Knowledge, 26 January 2010) < http://www.datacenterknowledge.com/archives/2010/01/26/cloud-customers-report-capital-cost-savings> accessed 10 January 2018

Marston S., and others, ‘Cloud Computing – The Bussiness Perspective’ (2011) <https://pdfs.semanticscholar.org/2531/00590bbd1b3fb2653ee2ba7983992f247796.pdf > accessed 10 January 2018

Mell P., Grance T., ‘NIST SP 800-145, The NIST Definition of Cloud Computing’ (NIST, 2011) <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublicatio n800-145.pdf> accessed 10 January 2018.

Meridith L., ‘Software as a Service (SaaS) Definition and Solutions’ (CIO, 15 May 2007) < https://www.cio.com/article/2439006/web-services/software-as-a-service--saas--definition-and-solutions.html> accessed 10 January 2018

Miller M., ‘Cloud Computing Pros and Cons for End Users’ (informIT, 13 February 2009) <http://www.informit.com/articles/article.aspx?p=1324280> accessed 10 January 2018

Poullet Y., and others, ‘Cloud Computing and its Implication on Data Protection’ (CRID, 5 March 2010)
< http://www.crid.be/pdf/public/6471.pdf.> accessed 10 January 2018

Roehrig P., ‘New Market Pressures Will Drive Next-Generation IT Services Outsourcing’ (Forrester, 9 October 2009). <https://www.sciencedirect.com/science/article/pii/S221201731300710X> accessed 10 January 2018

Rowe R. B., ‘Will Outsourcing IT Security Lead to a Higher Social Level of Security?’ (Research Triangle Institute International, 2007) <http://weis2007.econinfosec.org/papers/47.pdf> accessed 10 January 2018

Sehlhorst S., ‘The Economics of Software as a Service (SaaS) vs. Software as a Product’ (Pragmatic Marketing, 25 November 2008) <https://www.pragmaticmarketing.com/resour ces/articles/the-economics-of-software-as-a-service-saas-vs-software-as-a-product> accessed 10 January 2018

Sether A., ‘Cloud Computing Benefits’ (SSRN, 19 May 2016) <https://papers.ssrn.com/sol3/paper s.cfm?abstract_id=2781593> accessed 10 January 2018

Software and Information Industry Association, ‘Strategic Backgrounder: Software as a Service’ (12 May 2010) <https://www.slideshare.net/Shelly38/software-as-a-service-strategic-backgrounder> accessed 10 January 2018

Sotto J. L., Treacy C. B., and McLellan L. M., 'Privacy and Data Security Risks in Cloud Computing' (Electronic Commerce & Law Report, 3 February 2010) <https://www.hunton.com/files/Publication/4845e31f-63d8-4f9a-9a36-a074e4170225/Presentation/PublicationAttachment/6f52b2fd-2973-48cc-9f23-c941f1e19358/Privacy-Data_Security_Risks_in_Cloud_Computing_2.10.pdf> accessed 8 May 2018.

Spivey J., and others. ‘Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives. ISACA Information Security White Paper’ (ISACA, 2009) <http://www.klcconsulting.net/security_resources/cloud/Cloud_Computing_Security_&_Governance-ISACA.pdf> accessed 10 January 2018

Strickland J., ‘How cloud computing works’ (howstuffworks, 8 April 2008) <https://computer.howstuffworks.com/cloud-computing/cloud-computing.htm > accessed 10 January 2018

Taskova M., ‘Cloud Service Provider and Their use of Personal Data’ (Lexology, June 2016) <https://www.lexology.com/library/detail.aspx?g=0dd03d8e-0916-4d95-8a96-2cdae9613fe6> accessed 18 November 2017.

The European Network and Information Security Agency (ENISA), ‘Cloud computing: Benefits, risks and recommendations for information security’ (December 2012) <https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security> accessed 18 November 2017.

Urquhard J., ‘FBI Seizures Highlight Law as Cloud Impediment’ (CNET, 16 April 2009) <http://news.cnet.com/8301-19413_3-10220786-240.html> accessed 10 January 2018

Youseff L., Butrico M., and. Silva D. D., ‘Toward a Unified Ontology of Cloud Computing’ (8 May 2015) <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.176.3634&rep=r ep1&type=pdf> accessed 10 January 2018

Websites

http://www.google.com/apps/intl/en/business/index.html.

http://www.salesforce.com/crm/

http://code.google.com/appengine/.

http://www.microsoft.com/windowsazure/.

http://aws.amazon.com/ec2

http://www.gogrid.com/index.v2.php.

http://aws.amazon.com/s3.

http://www.rackspacecloud.com/

http://www.cisco.com

https://www.lexology.com

https://www.ssrn.com/en/

https://academic.oup.com/ijlit.

http://ejlt.org.

http://jolt.law.harvard.edu.

List of Abbreviations

DPA – Data Protection Authority

DPD – Data protection Directive 95/46/EC

DPIAs – Data Impact Assessments

EC – European Commission

ECHR – European Convention of Human Rights and Fundamental Freedoms

ENISA– The European Union Agency for Network and Information Security

EU – European Union

GDPR – General Data Protection Regulation

IT – Information Technology

IaaS – Infrastructure-as-a-Service

NIST – Nation Institution of Standard and Technology

ODNI – The Office of the Director of National Intelligence

PaaS – Platform-as-a-Service

SaaS – Software-as-a-Service

SLAs – Service Level Agreements

ULAs – User Licensing Agreements

US – United State

WP29 – The Article 29 Data Protection Working Party