CHARLES UNIVERSITY IN PRAGUE

Faculty of Law

Barbora Studihradová

General Data Protection Regulation: Challenges for the Cloud

Master's thesis

Master's thesis supervisor: JUDr. Magdaléna Svobodová, Ph.D.
Department of European Law
Date of completion (manuscript closure): 13 April 2018

Declaration

I declare that this master's thesis is a result of my independent work and that all the sources used have been duly quoted. I further declare that this master's thesis has not been used to obtain any other or the same degree.

This master thesis has 408 383 characters including spaces and footnotes.

Barbora Studihradová

In Prague on

Prohlášení

Prohlašuji, že tato diplomová práce je výsledkem mé vlastní samostatné práce a že všechny použité zdroje byly řádně citovány. Dále prohlašuji, že tato diplomová práce nebyla použita ke získání jiného nebo stejného titulu.

Vlastní text této diplomové práce má 408 383 znaků včetně mezer a poznámek pod čarou.

Barbora Studihradová

V Praze dne

Acknowledgement

First and foremost, I would like to thank my thesis supervisor, JUDr. Magdaléna Svobodová, Ph.D. for her time, patience and valuable comments during my work on this master's thesis. I would also like to express my thanks to Mgr. et Mgr. Tomáš Honzák, Director of Security and Compliance in GoodData, for his expert advice and feedback. Last but not least, I would like to thank my family and boyfriend for their unconditional love and support in the course of my studies.

Poděkování

V první řadě bych ráda poděkovala vedoucí své práce JUDr. Magdaléně Svobodové, Ph.D. za její čas, trpělivost a cenné komentáře při psaní této diplomové práce. Dále bych ráda poděkovala Mgr. et Mgr. Tomáši Honzákovi, řediteli Security and Compliance ve společnosti GoodData, za jeho odborné rady a zpětnou vazbu. V neposlední řadě děkuji své rodině a příteli za jejich bezpodmínečnou lásku a podporu při mém studiu.

Table of Contents

Introduction

The ubiquity of the Internet has opened up new horizons for the processing of personal data. It has become ever more widespread and prone to risks that were previously unheard of. May it be due to the individual's lack of control over his or her personal data, insufficient information about what, why, and how is being processed, or uncertainty regarding who is responsible. This trend was dramatically accelerated with the emergence of cloud computing at the beginning of the century, and still grows on importance as the industry continues to innovate and new and more advanced services are offered.

Despite being a commonly used word, cloud computing is often misunderstood as a concept concerning only the storage of information online. Nonetheless, cloud services can take on many forms, including such remarkable phenomena like Facebook, Instagram, YouTube, Netflix, or Dropbox, but also low-level computing resources on which they are built. The issue from the data protection perspective is that the cloud environment is extremely complex. There are many parties involved behind a provision of what we see as a single product, often acting as cloud clients for a certain service while providing another, using the data in many ways, including as a commodity. Consequently, processing of personal data in the cloud is completely opaque.

Nevertheless, cloud computing has enormous business potential. It has become a basis of Big Data, Internet of Things, and a common core of many business strategies, evolving from a paradigm allowing large cost savings by using computing resources more efficiently, into a phenomenon driving change in innovative software by making its development easier and faster. As a result, it has become widespread, not only among individuals, but also businesses processing personal data in the cloud. Cloud Industry Forum's survey revealed that cloud computing services have achieved mainstream already in 2013 among UK businesses, with 69% of them using at least one cloud-based service for business purposes.[1] Forrester predicts that in 2018 globally more than 50% of businesses will rely on at least one public cloud platform.[2] Businesses worldwide are undergoing digital transformation on increasing client demand, using cloud computing as its fuel.[3]

The EU recognized that this newly shaped data processing environment merits special attention. Already in September 2012, the European Commission issued a Communication on cloud computing, declaring policy goals focused at enabling and facilitating faster adoption of

[1] Cloud Industry Forum. Adoption of Cloud computing continues upward trend as a mainstream IT deployment option [online]. Available at: <https://www.cloudindustryforum.org/content/adoption-cloud-computing-continues-upward-trend-mainstream-it-deployment-option>. Last accessed 4 March 2018.

[2] BARTOLETTI, Dave. Predictions 2018: Cloud computing accelerates enterprise transformation everywhere [online]. 7 November 2017. Available at: <https://go.forrester.com/blogs/predictions-2018-cloud-computing-accelerates-enterprise-transformation everywhere/>. Last accessed 4 March 2018.

[3] Gartner. Gartner Says Global IT Spending to Reach $3.7 Trillion in 2018 [online]. 3 October 2017. Available at: <https://www.gartner.com/newsroom/id/3811363>. Last accessed 4 March 2018.

cloud services, to give Europe a *"chance to act to ensure being at the forefront of its further development"*[4] and benefit from the increased number of jobs and productivity. Data security and protection were repeatedly identified as the biggest concerns disrupting the use of cloud.[5] European Commission acknowledged that inadequate data protection regulation is a key area that could hinder adoption of cloud and proposed a uniform legal framework that would replace the impeding 27 national frameworks as part of its Digital Agenda Action,[6] combatting a major regulatory challenge created by the borderless nature of the cloud. The initial target was to adopt the proposed General Data Protection Regulation (hereinafter referred to as "GDPR")[7] as early as possi-possible during the year 2013.[8] This milestone was obviously not met and GDPR was in its final version adopted in May 2016 and at the time of writing of this thesis, is yet to come into force on the 25th of May, 2018.

GDPR strives to achieve an ambitious goal, to be both an enabling law for cloud computing and to guarantee a high level of protection for individuals.[9] The fundamental question that this thesis seeks to answer stems from this twofold objective. Can GDPR be in fact regarded as in the words of the Commission to be "*cloud friendly*"?[10] I approach this question from the point of view that a data protection framework must provide reasonable legal certainty and allow for its practical application, in order to be regarded as friendly. After a thorough research undertaken in the field, a hypothesis that I propose is that the GDPR includes wording and concepts that are highly impractical in cloud computing, causing considerable challenges for the industry. This thesis recognizes and analyzes some of the most fundamental ones, drawing inspiration mainly from the issues addressed by the Cloud Legal Project at Queen Mary University in London under the regime of the Directive 95/46/EC (hereinafter also referred to as "Directive"),[11] and heated discussions in the cloud computing industry.

The hypothesis is tested by confronting some of the provisions of the GDPR with how cloud computing functions, leading to conclusions whether the legal aspects can be reflected in the cloud reality. This thesis, therefore, is interdisciplinary and requires conceptual understanding of both the technical and the legal aspects.

---

[4] European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Unleashing the Potential of Cloud Computing in Europe. COM(2012) 529 final, pp. 2-3.

[5] Cloud Industry Forum, 'Adoption of Cloud computing continues upward trend', op. cit.

[6] European Commission, 'Unleashing the Potential of Cloud Computing in Europe', op. cit., p. 8.

[7] 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), OJ L 119.

[8] European Commission, 'Unleashing the Potential of Cloud Computing in Europe', op. cit., p. 8.

[9] Ibid, p. 12.

[10] Ibid.

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

The thesis is divided into four parts. Chapter 1 provides solid overview of the foundations of cloud computing, necessary for the analysis of the challenges. Firstly, it addresses the definition of it and deconstructs the myths. It further explains different service models in the cloud and why distinguishing between them is relevant in the data protection context. Lastly, it illustrates how difficult it may be to trace every single piece of information in the cloud through the explanation of virtualization and sums up risks that may arise.

Chapter 2 does the same with the foundations of the data protection law in the European Union. Firstly, it takes a look at data protection in primary and secondary law. Then it acknowledges the standing of the right to personal data protection as a fundamental right in the EU law. The final part then seeks to outline the data protection reform of which the GDPR is a part, and its connection with cloud computing.

Chapter 3 intends to outline the basics of the GDPR, relevant for the subsequent analysis in Chapter 4, which forms the core of the thesis. The author works with the guidelines issued by the WP29 and available commentaries. Where appropriate, case law of the CJEU is also reflected.

Finally, chapter 4 sets out some of the challenges of the GDPR for cloud computing and critically analyzes whether they hinder practical applicability of the GDPR or give rise to considerable legal uncertainty.

Bearing in mind that a dynamic development of the CJEU case law can be reasonably expected based on the flood of questions referred for a preliminary ruling by national courts, I am nevertheless utterly convinced that my analysis is not premature. The cloud computing industry has to adjust accordingly before the GDPR comes into force. The lack of case law is exactly why I intend to test the hypothesis in the light of the technical aspects of the cloud, attempting to recognize whether there are impractical provisions, which should have been addressed more precisely at a regulatory level.

As far as the bibliography is concerned, I largely draw from the works of the professors engaged in the Cloud Legal Project at Queen Mary University in London,[12] especially Professor Kuan W Hon. I find their research especially valuable, due to their expertise in both law and technology. Unfortunately, given the topicality of the GDPR, even their scholarly literature is largely outdated, so I approach it critically, recognizing which aspects may be applicable. Besides that, I use non-cloud specific commentaries of the GDPR, selected industry online sources, academic articles and documents issued by the European Commission or the WP29 and some relevant case law of the CJEU.

I duly note that this thesis does not attempt to cover GDPR and its relationship to cloud exhaustively, as it exceeds the possibilities of a master's thesis. Therefore, the challenges that are analyzed are carefully chosen. Although other secondary law instruments besides the GDPR that concern data protection are applicable to the cloud computing, this thesis does not attempt to address them. Neither does it strive to provide a step-by-step guide to compliance, as this would

[12] See <http://www.cloudlegal.ccls.qmul.ac.uk> for more information. Last accessed 4 April 2018.

be practically impossible, without focusing on a specific service. The links with competition law, the balance between the right to personal data protection and right to freedom of information or to conduct business, these are all issues that I find extremely interesting, but do not examine them in this thesis.

Realizing the complexity of the topic, I aim to provide solid starting point for further discussions. What are the challenges of the GDPR for the cloud, which may have been addressed better at a regulatory level, so that it would be cloud friendly?

1 Cloud computing

1.1 What is cloud computing

There is no single and all-encompassing definition of cloud computing.[13] Rather, organizations tend to create their own definitions for their own purposes. Some of them are more complex, some of them less. The more precise ones are usually preferred to ensure differentiation from other phenomena, which function similarly (such as outsourcing). However, they can at the same time be hard to comprehend for non-technical readers. So, in order to explain what cloud computing is, let me firstly define it simply as *"a way of delivering computing resources as a utility service via a network, typically the Internet"*[14].

There are several important aspects to note in this definition. Firstly, cloud computing is not a new technology or a type of technology at all, although being frequently understood as such by the general public.[15] Far more accurate way to think about it is to see it "as a service", or a model of computing.[16] The term "cloud computing" itself stems from the design of a chart traditionally used to illustrate network-based computing. The cloud then represents the Internet – or another network,[17] which connects the shared computing resources and allows cloud clients to access them.[18]

Secondly, cloud computing is not a concept that would appear as a single outcome to cloud clients but can in fact mean many different things.[19] This is because the shared computing resources may take lots of different forms. It can be an infrastructure only, a provision of storage or servers, a core hosting operating system that allows cloud clients to run their own applications on it, or an application ready to use by end-users. And even then, services intended for end-users, are not confined solely to storages that can be used online, such as Dropbox. Other widely used include social networking, such as Facebook, LinkedIn or Twitter, web-based emails, such as Gmail or Hotmail, photo-sharing websites such as Flickr, Picasa, entertainment such as YouTube, Netflix, and many other.[20] What is provided as a computing resource matters and is examined in more detail later in this chapter.

---

[13] FOGARTY, Kevin. Cloud Computing Definitions and Solutions [online]. 10 September 2009. Available at: <https://www.cio.com/article/2424886/cloud-computing/cloud-computing-definitions-and-solutions.html>. Last accessed 20 February 2018.

[14] HON, Kuan W and MILLARD, Christopher. Cloud Technologies and Services. In: *Cloud Computing Law*. United States of America: Oxford University Press, 2013, p. 3.

[15] FOGARTY, 'Cloud Computing Definitions and Solutions', op. cit.

[16] Ibid.

[17] A VPN or other.

[18] BLACK, Nicole. *Cloud computing for lawyers.* United States of America: American Bar Association, 2012, p. 2.

[19] Ibid, p. 2.

[20] GORDON, Michael and MARCHESINI, Kathryn. Examples of Cloud Computing Services [online]. 2010. Available at: <http://www.unc.edu/courses/2010spring/law/357c/001/cloudcomputing/examples.html>. Last accessed 20 February 2018.

European Parliamentary Research Service[21] defined cloud computing in its analysis of economic and policy issues of cloud computing similarly as *"a model for providing or obtaining information and communication technology (ICT) services over a network like the internet,"*[22] but simultaneously cited other definitions, including the widely accepted one[23] issued by the National Institute of Standards and Technology of the United States of America (hereinafter referred to as "NIST").[24] NIST states that cloud computing is *"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"*[25] and on top of that provides the essential characteristics, main service models and deployment models of cloud computing, which form part of the definition itself. Although such a definition may seem unnecessarily complicated, it provides a level of comprehension vital in order to understand the challenges data protection represents for cloud computing. I will now therefore proceed to further explanation.

1.2 Characteristics of cloud computing

According to NIST, cloud computing as a model comprises of five essential characteristics[26]:

[1] On-demand self-service

Cloud computing is an on-demand self-service, which means that there is no human interaction with the cloud service provider needed, when the user requests the offering. The request is processed automatically, which makes getting the resources fast and easy for the user and decreases the administrative burden on the provider, who would otherwise have to employ support staff to carry out the automated tasks. However, self-service solutions may be difficult to build and create considerable challenges for the providers, in terms of fulfilment of regulatory and compliance requirements.[27]

[2] Broad network access

---

[21] The European Parliament's in-house research department and think tank.

[22] According to Article 4 (19) of the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, cloud computing service "means a digital service that enables access to a scalable and elastic pool of shareable computing resources".

[23] ROUNTREE, Derrick and CASTRILLO, Ileana. *The Basics of Cloud Computing*. Understanding the Fundamentals of Cloud Computing in Theory and in Practice. Waltham: Syngress, p. 2.

[24] National Institute for Standards and Technology is an agency established in 1901 by the U.S. Congress, which is part of the U.S. Department of Commerce. It provides measurement standards and promotes innovation and industrial competitiveness. For more information, see e.g. <https://www.nist.gov/about-nist>. Last accessed 20 February 2018.

[25] MELL, Peter and GRANCE, Timothy. The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. Gaithersburg: National Institute of Standards and Technology, U.S. Department of Commerce, 2011. Available at: < http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. Last accessed 20 February 2018.

[26] Ibid.

[27] ROUNTREE, CASTRILLO, 'The Basics of Cloud Computing', op. cit., p. 3.

Cloud services should be easily accessible. This requirement is projected on three levels. Firstly, cloud services are accessible from any network. Cloud clients are only required to have a basic network connection, but there is no threshold when it comes to the amount of bandwidth needed to use the services.[28] Secondly, cloud services require either no client or a thin client.[29] A thin client acts simply as a terminal to the server and requires constant communication with it. It is a network computer without a hard disk drive.[30] Thick client, on the other hand, will be able to do a lot of processing on client server applications. It has its own resources. Consequently, some operating systems are generally unable to run on thin clients only, but this is not the case with cloud services. Thirdly, cloud services do not require a specific type of client device in order to be able to function properly.[31] They can be used with laptops, desktops, but also smartphones, tablets or other computing devices. With cloud computing, users should never be told which browser or device they need to use.[32]

[3] Resource pooling

Resource pooling is a classic technique commonly used outside of the IT world, which enables users to benefit from sharing resources.[33] The advantages include not only saved costs, but also increased efficacy, as less time can be spend maintaining the shared resources, compared with the situation when every user would have his or her own. With cloud computing, the provider's computing resources are pooled together to serve multiple users, based on their demand. Individual users do not have a constant need for the resources offered. In cloud computing, when the resources are not used by one user, they are assigned to another one, instead of being left idle.[34] Users generally will have no control over the exact location of the resources that are dynamically assigned to them but may be able to have knowledge of the country or data centre they are in.[35]

[4] Rapid elasticity

Rapid elasticity refers to the ability of cloud services to expand and shrink easily in terms of their capacity in proportion to the users' demand. Capabilities offered by cloud service are available at

[28] Ibid, pp 3-4.
[29] Ibid.
[30] BEAL, Vangie. The Differences between Thick and Thin Client Hardware [online]. 6 July 2006. Available at: <https://www.webopedia.com/DidYouKnow/Hardware_Software/thin_client.asp>. Last accessed 20 February 2018.
[31] ROUNTREE, CASTRILLO, 'The Basics of Cloud Computing', op. cit., p. 3.
[32] BENSON, Patrick. The Cloud Defined, Part 2 of 8: Broad Network Access [online]. 5 May 2013. Available at: <http://www.pbenson.net/2013/05/the-cloud-defined-part-2-of-8-broad-network-access/>. Last accessed 20 February 2018.
[33] BENSON, Patrick. The Cloud Defined, Part 3 of 8: Resource Pooling [online]. 6 May 2013. Available at: <http://www.pbenson.net/2013/05/the-cloud-defined-part-3-of-8-resource-pooling/>. Last accessed 20 February 2018.
[34] ROUNTREE, CASTRILLO, 'The Basics of Cloud Computing', op. cit., pp. 4-5.
[35] MELL, GRANCE, 'The NIST Definition of Cloud Computing', op. cit.

any quantity at any time, but they are not wasted, as their amount increases or decreases flexibly based on the demand.[36]

[5] Measured service
Cloud services are measured services, meaning that their usage can be quantified, measured, controlled and optimized. Users are commonly billed based on their consumption levels, the so-called pay per use system.[37]

1.2.1 Service models

What is provided as a service determines the role that cloud clients and cloud providers play in cloud computing. Based on the service model, cloud clients manage different spectrum of resources. As a result, the level of control that they exercise over the resources in general, but importantly also over the personal data possibly processed and their involvement when using the service varies significantly. The same applies to cloud providers and the amount of knowledge they possess about how the cloud client uses their service, including what data are processed.[38]

There are three standard cloud service models, originally described as part of the definition of cloud computing by NIST, which are now well-established in practice.[39] When cloud services are offered, they are usually also branded as falling into one of these categories. The standard cloud service models are:

[1] Infrastructure as a Service (usually referred to as "IaaS");
[2] Platform as a Service ("PaaS");
[3] Software as a Service ("SaaS").

As has been noted above, "as a Service" emphasizes that cloud clients are not buying product or obtaining a license, but rather really renting chosen resources as services.[40]

In IaaS, the cloud provider offers only the most fundamental computing resources, mainly computing hardware infrastructure, such as servers, storage or networking. IaaS therefore involves, out of the three models, the lowest-level functionality and requires the highest level of technological expertise on the side of cloud clients as they manage and control most of the resources on their own.[41] With IaaS, cloud clients possess considerable control and have detailed knowledge about how and what is provided to them, as well as over the specific determination of

[36] ROUNTREE, CASTRILLO, 'The Basics of Cloud Computing', op. cit., p. 5.
[37] Ibid.
[38] STAIGER, Dominic Nicolaj. *Data protection compliance in the cloud.* Zürich, 2017. Dissertation. Universität Zürich. Prof. em. Rolf H. Weber, Chair, p. 93.
[39] They were firstly introduced by NIST, but are currently widely used without reference to NIST's definition. See e.g. HON, MILLARD, 'Cloud Technologies and Services', op. cit., p. 4, footnote 9.
[40] Ibid.
[41] Ibid.

the means of the processing. A client of IaaS may be for example a start-up company, which is unwilling to invest in its own physical infrastructure but needs one to install its operating systems on. In IaaS, cloud clients use their own platforms within the service provider's infrastructure. Services offered as IaaS include for example Google Compute Engine, Microsoft Azure and Elastic Compute Cloud (EC2) or Simple Storage Services (S3) provided by Amazon.[42]

PaaS enables cloud clients to develop their own applications on the platform provided. Computing resources offered therefore include besides hardware, also software platforms for programming, deploying and hosting applications. Cloud clients do not influence the underlying infrastructure and are not concerned with it. They focus on building their own service offerings using the already created environment, allowing them to develop new applications faster and more efficiently. They do control the code they deploy. However, they are limited to programming languages, libraries etc. that are supported by the specific provider. Other restrictions may also apply and usually will concern security or scalability. Which means that PaaS clients may have some influence on how their application accesses stored data and the data storage mechanism in general, but only within the set boundaries.[43] Examples of PaaS include Google App Engine, Red Hat OpenShift or Heroku.[44]

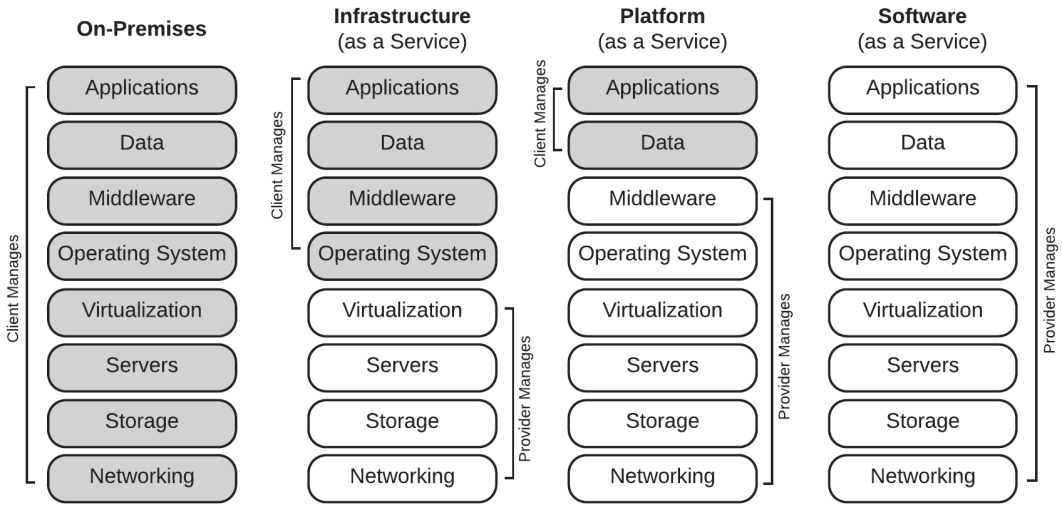
SaaS provides high-level functionality and requires the least technical knowledge.[45] When the general public imagines cloud computing, it is usually SaaS. The capability provided is an end-user application. Clients are not concerned even with the code of the application.[46] With SaaS, clients access the application software, hence the name "Software as a Service". They do not manage or control any underlying cloud infrastructure, and cannot influence capabilities of the application. Cloud clients of SaaS are the most detached from computing resources used and do not have any control over them. Therefore, they are also the most vulnerable in terms of the data protection. They can at best influence the application in terms of choosing which capabilities they wish to use in its settings, i.e. within the boundaries created by the provider. Examples of SaaS include webmail such as Gmail or Yahoo and social networking service like Instagram or Facebook.[47] Data storages, which form part of SaaS are sometimes recognized as a distinguishable subclass with the same abbreviation known as "Storage as a Service".

It is important to clarify that individual models do not separate distinct types of cloud services strictly, but rather illustrate a spectrum of cloud services based on which capabilities are provided. Boundaries between them, therefore, can be unclear and their modifications are possi-

[42] BOISVERT, Michelle and BIGELOW, Stephen J. Infrastructure as a Service (IaaS) [online]. September 2017. Available at: <https://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS>. Last accessed 20 February 2018.
[43] HON, MILLARD, 'Cloud Technologies and Services', op. cit., pp. 12-13.
[44] BIGELOW, Stephen J. Platform as a Service (PaaS) [online]. September 2017. Available at: <https://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS>. Last accessed 20 February 2018.
[45] HON, MILLARD, 'Cloud Technologies and Services', op. cit., p. 4.
[46] Ibid, p. 13.
[47] Ibid, p. 4, footnote 12.

ble.[48] In order to recognize specifics of certain new cloud-based services, other terms besides the three established ones are gradually emerging. Distinguishable categories include "BaaS" or Blockchain as a Service, "MBaaS" or Mobile Backend as a Service and many others.[49] On top of that, there has also been some advocacy of a term "XaaS"[50], known as Everything as a Service or Anything as a Service, which covers all the service models that are otherwise distinguished and reflects the vast potential cloud computing as new and more sophisticated services are constantly being developed.[51]

However, the classification into three models is useful for the analysis of challenges that data protection poses to cloud computing, since their impact and possible solutions differ significantly based on the capabilities provided as a service. I will therefore refer to SaaS, IaaS, and PaaS throughout the analysis in chapter four. The following chart prepared by the author of this thesis illustrates who manages what computing resources in different scenarios, as described in this subchapter.



1.2.2 Layers of cloud services

A cloud service often consists of several layers of cloud services, which can have distinct providers. For example, a SaaS provider does not have to have its own physical and software infrastructure but can use another provider's IaaS or PaaS as an alternative. This is the case with Dropbox,

[48] Ibid, pp. 4-5.

[49] MCLELLAN, Charles. XaaS: Why 'everything' is now a service [online]. 1 November 2017. Available at: <http://www.zdnet.com/article/xaas-why-everything-is-now-a-service/>. Last accessed 22 February 2018.

[50] See e.g. HARVEY, Kate. The Future is XaaS: What you need to know about Everything-as-a-service [online]. 7 February 2017. Available at: <https://www.chargify.com/blog/xaas-everything-as-a-service/>. Last accessed: 22 February 2018.

[51] STROUD, Forrest. Everything-as-a-Service (XaaS) [online]. Available at: <https://www.webopedia.com/TERM/E/everything-as-a-service_xaas.html?relatedterms>. Last accessed 20 February 2018.

which offers storage as SaaS to its clients. But Dropbox built the storage on an infrastructure provided by Amazon. In such layering of the service, Dropbox is both a cloud service provider and a cloud client. From the point of view of the end user, there are two cloud providers hidden behind what appears to be a single service. These providers, as will be discussed in the fourth chapter, then can be classified differently under GDPR. Both of them might be processers, or Dropbox a controller and Amazon a processor, and so on. Thus, their responsibilities may differ. Many permutations are possible. SaaS does not have to be layered at all, when everything is provided by a single cloud service provider (e.g. Gmail, Flickr, outlook.com). Or, there might be as many as three layers, when SaaS is built on PaaS based on another provider's IaaS (e.g. many apps offered by different providers for the Apple smartphone iPhone are built on a platform provided by a sub-provider Heroku, which is using an infrastructure provided by sub-sub provider Amazon[52]).

Very often, cloud clients, especially of SaaS, do not see or care who is involved in the provision of the service. However, the multiple dependencies that layering of cloud services creates have substantial effect on risks involved in terms of data protection. Who supplies and ultimately owns the physical infrastructure behind every cloud service is another question. Cloud platforms may be proprietary or open source, hosted or installed as a software. To sum up, the examples presented above are meant to illustare, how highly sophisticated and complex provision of cloud computing services can be.[53]

1.2.3 Deployment models

Deployment models first identified as part of the NIST's definition of cloud computing differentiate between services based on to whom they are accessible. In other words, they illustrate who can use the cloud service. There are four deployment models:[54]

[1] Private Cloud;
[2] Public Cloud;
[3] Community Cloud;
[4] Hybrid Cloud.

Private clouds are dedicated to the exclusive use by a single client. It does not matter who owns the infrastructure, or whether it is located on or off premises of the client. The decisive factor lies in that the infrastructure is not accessible to general public, but to one client only. Private clouds are expensive and often used by clients like banks, government agencies or businesses that seek enhanced control and security, because they deal with data requiring enhanced protection.

[52] HON, MILLARD, 'Cloud Technologies and Services', op. cit., p. 16, footnote 69. Over 7 thousand clients, who use Heroku to build their own cloud services are listed here: <https://siftery.com/heroku>. Last accessed 20 February 2018.
[53] Ibid, pp. 12-17.
[54] MELL, GRANCE, 'The NIST Definition of Cloud Computing', op. cit.

Security and protection of data in private clouds is improved by design, simply because the computing resources used are not shared with any other clients.[55]

In case of public cloud, the infrastructure is accessible to multiple clients, who share the same computing resources. It is usually owned and located on the premises of the cloud service provider. But then again, this does not matter in terms of classification of the service as a public cloud. Public cloud is in the centre of attention of data protection law, since it is the most open deployment model. It is the cheapest and most popular model, which at the same time represents the highest risks for personal data.

An infrastructure of a community cloud is accessible to a specific community of clients, which shares the same purpose or goals (e.g. security requirements or compliance considerations), such as financial services industry, insurance companies specifically etc.

Hybrid cloud is a combination of at least two of the deployment models described above. Key is that the models are clearly defined and exist separately, but they are linked together, so that the clients can benefit from the advantages of each of the models.[56]

When analyzing the challenges of the GDPR for cloud computing in the fourth chapter, I consider public clouds, as they are the most relevant in the context.

1.2.4 Virtualization

The risks that arise for data protection in the cloud are partially based on its key enabling technology, called virtualization.[57] It makes one physical hardware system act like multiple, enabling splitting its resources into separate environments that can be utilized independently. These environments are known as "virtual machines" ("VMs") or "guests" and the software that allows their creation is a "hypervisor". The physical hardware itself is a "host". Hypervisor both separates the resources and distributes them. In other words, it determines how much of the resource (in terms of computing power, operational memory, or storage) is given to specific VMs based on demand. Hypervisor can be proprietary (e.g. Microsoft Hyper-V), or open source (e.g. Xen or Oracle VM Virtual Box).[58]

Virtualization allows the resources to be used more efficiently compared to if a physical hardware was dedicated just to one user, creating the advantages of economies of scale. But multiple users ultimately use the same pool of resources provided by the host and their VMs are separated from each other only virtually by a software. This creates data protection and security compliance concerns.[59]

---

[55] BUTLER, Brandon. 3 types of private clouds: Which one's right for you? [online]. 24 November 2015. Available at: <https://www.webopedia.com/TERM/E/everything-as-a-service_xaas.html?relatedterms>. Last accessed 20 February 2018.

[56] HON, MILLARD, 'Cloud Technologies and Services', op. cit., p. 5.

[57] Ibid, p. 6.

[58] *Redhat.* Understanding virtualization [online]. Available at: <https://www.redhat.com/en/topics/virtualization>. Last accessed 20 February 2018.

[59] Note that there are also cloud service providers, who offer the possibility of a provision of a physical hardware dedicated to a single client and not all cloud computing services are based on virtualization, though it is still the norm.

There are several types of virtualization, affecting the handling of the data, including personal data. The most common type in cloud computing is a server hardware virtualization, where it is the server that is made to act like many. Methods used differ, but generally, in such a case, if the data are not stored on a persistent storage and the VM fails, there is a risk that data may be lost, since they are stored only on "virtual disk files".[60] The solution is often provided through storage virtualization, which commonly uses RAID technology to mitigate individual physical drive failure through redundancy. In storage virtualization, a file appears as a single file, but the fragments of data are in fact stored across distinct physical drives. Fragments are "mirrored", again in complex ways, allowing for varying schemes. This is relevant for both data location (as different fragments of one data file can be located in different locations) and whether such fragments fall under the definition of personal data and are as a result within the scope of the GDPR. Distributed data storages are either managed by cloud service providers and may include data of multiple clients or in some rather rare cases sophisticated clients may be able to use their own applications to manage the storage. Such an option is limited by cloud service provider's restrictions and contract arrangements. It is important to note that even within IaaS, levels of control over the data and their location and who manages what differ.

Another practical aspect that may impact data protection is the fact that although not all cloud providers do, many back up data in multiple locations, creating their replicas to ensure their availability in case of sudden failure of software or hardware. Seldom and temporarily, persistent storage (such as hard disk or memory) can be used in cloud computing, with varying policies on data purging and deletions. Besides that, data can be also held on any temporary caches, used to speed up delivery into different geographical locations.[61] This practical functioning poses a challenge with regard to the right to erasure under the GDPR, which I analyze in greater detail in chapter four.

1.3 What are the risks of cloud computing for data protection?

The risks of cloud computing for the protection of personal data stem from the very advantages it offers. One of them being the ability to focus at what is important to the client (e.g. building a new app, using an app, conducting one's own business), while relying on third parties (cloud services providers) with the management and control of the rest.[62] As a result, the availability, confidentiality, and integrity of personal data can be largely in cloud provider's hands, who might be able to easily access the personal data stored, though much depends on the service model and design of the service. Professors Hon and Millard emphasize that collocation risks also exist. Since

[60] Also called "virtual disk images".

[61] HON, Kuan W and MILLARD, Christopher. Cloud Technologies and Services. In: *Cloud Computing Law*. United States of America: Oxford University Press, 2013, p. 6-12.

[62] HON, Kuan W and MILLARD, Christopher. Control, Security, and Risk in the Cloud. In: *Cloud Computing Law*. United States of America: Oxford University Press, 2013, p. 18.

providers manage data of multiple parties, when the data seized by authorities are on the same hardware or in the same database, data of clients who are not targeted by the seizure can be affected by either being seized as well or made unavailable due to the forced suspension of the service.[63] In other words, data protection concern is that data subjects may lose control over their data in cloud computing. In practice, this is of a high concern mainly in SaaS, where users do not have any technical control over data management.[64]

Other related concerns are the risks to data integrity and their protection against unauthorized destruction, loss, or modification.[65] On the contrary, cloud services may as well be problematic in terms of reliability on the access to the data by the controller or the data subjects, in case the systems shut down. This issue is often mitigated by storage virtualization, as described above, which on the other hand allows the spread of the data in form of their replications of fragments, possibly increaseing the chances of their unauthorized use, and ineffectiveness of future deletion.

As the European Commission aptly noted, "where the World Wide Web makes information available everywhere and to anyone, cloud computing makes computing power available everywhere and to anyone"[66]. The nature of cloud computing is borderless. Personal data are able to travel across continents in no time. The clients usually do not possess sufficient visibility into who and how really processes their data or where they are located. As described above, cloud service providers engage sub-providers and other actors in the process. Cloud computing is often layered. The resulting lack of transparency is one of the issues that GDPR strives to address to bring the data subject more control. The current state of the visibility into the cloud layers on client's side is well illustrated by the recent news that in January 2018, Apple disclosed that it cooperates with Google to store end-user's data (like photos and videos, perfectly fit for direct identification) in its popular iCloud. It is uncertain when Apple started using Google's cloud, but it has to be noted that it previously relied also on Amazon Web Services and Microsoft Azure. However, there was no prior indication of the changes of sub-processors and users, who obviously are not in such cases in the position to require employment only of certain providers in the processing, did not even get a chance to make a decision to stop using Apple's services, before Google got its hands on their data.[67] In any case, what percentage of iCloud users knows that other players may be involved in the processing of their data?

[63] Ibid.

[64] Ibid, p. 25.

[65] Ibid.

[66] European Commission, 'Unleashing the Potential of Cloud Computing in Europe', op. cit., p. 2.

[67] NOVET, Jordan. Apple confirms it uses Google's cloud for iCloud [online]. 26 February 2018. Available at: <https://www.cnbc.com/2018/02/26/apple-confirms-it-uses-google-cloud-for-icloud.html>. Last accessed 1 March 2018.

2 Data protection law in the European Union

This chapter shall serve as an introduction to the EU data protection law. I will firstly explain its legal basis in the primary law and then outline the complex secondary law framework. Then I will provide a brief recourse to the origins of the right to the protection of personal data and its inclusion in the Charter of Fundamental Rights of the EU ('Charter').[68] Lastly, I will come to the reform of the data protection framework of which the GDPR is a part.

2.1 Introduction

2.1.1 Data protection in the primary law

Firstly, the Charter, which was proclaimed in Nice in 2000 originally as a political instrument only, gained legally binding force and was granted the same legal value as the Treaties by Article 6 of TFEU with the entry into force of the Lisbon Treaty in December 2009. There are two articles of the Charter which are relevant to data protection, Article 7 and Article 8. I will elaborate on their content and relationship further in this chapter.

Besides that, the entitlement to data protection as expressed in Article 8 (1) of the Charter is mirrored in Article 16 (1) TFEU which states that *"everyone has the right to the protection of personal data concerning him"*. Article 16 of TFEU is placed among the provisions having general application and thus being of major importance. Other issues regulated therein aim at tackling discrimination or provision of adequate social protection and protection of human health (Articles 8-10 TFEU).

Furthermore, Article 16 (2) TFEU provides for a general mandate of the EU in the area of data protection.[69] It *obliges* the European Parliament and the Council to *"lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data."*[70] As the article referres to rules and is worded as an obligation, the choice of legislative instrument is left upon the discretion of the legislator, allowing for an adoption of directly applicable regulation.[71]

Lynskey lists as one of the key characteristics of the EU data protection framework that its regime is 'omnibous' as opposed to 'sectoral' typical for the US.[72] However, she then notes that the boundaries may be blur. At least at the European level, the efforts not to distinguish between

[68] Charter of Fundamental Rights of the European Union, 2012 OJ C 326.

[69] HUSTINX, Peter. EU data protection law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation. In: *Collected courses of the European University Institute's Academy of European Law, 24th Session on European Union Law, 1-12 July 2013,* p. 19. [online] Available at: <https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf>. Last accessed 1 March 2018.

[70] Emphasis added.

[71] HUSTINX, 'EU data protection law', op. cit., p. 19.

[72] LYNSKEY, Orla. *The Foundations of EU Data Protection Law.* First edition. Oxford: Oxford University Press, 2015, p. 15.

the public and private actors in terms of which rules apply to them, were present in the development of data protection laws at least before the adoption of Convention 108.[73] And Article 16 (2) TFEU indeed appears to be seamlessly applicable across all areas of the EU law, this interpretation being supported by the fact that the three-pillar structure was abolished with the Lisbon Treaty. But the pillar distinction prevails in the data protection framework.[74]

Article 16 (2) TFEU states that the provision is without prejudice to Article 39 of TEU, which provides for a derogation concerning the legislative procedure for the adoption of acts in the area of common foreign and security policy. Whereas acts based on Article 16 TFEU require ordinary legislative procedure, Article 39 of TEU foresees decisions of the Council only. Both articles state that the data protection rules are subject to the control of independent authorities. In addition, specific rules may be laid down in the area of police and judicial cooperation in criminal matters if they prove necessary.[75] Lastly, there are also generous exemptions from the general regime for the public sector throughout the GDPR.[76]

2.1.2 Data protection in the secondary law

Although the Commission called for an overeaching instrument once setting out to reform the data protection framework, [77] two acts were adopted in the end. The failure to adopt a single one is seen as a major drawback of the reform.[78] The GDPR is by far not the only secondary law relevant to data protection. Not only that the secondary law continues to reflect the distincion between the pillars, but also is fragmented in other ways, creating a complex framework. I will now provide an illustration of its structure.

Firstly, the area regarding the police and judicial cooperation in criminal matters (the former third-pillar) is governed by specific instruments with regard to data protection. The main one[79] being the so-called Police Directive 2016/680 adopted as part of the data protection reform.[80] As Hustinx points out, *"the option of a Regulation also covering the area of criminal law enforcement was apparently a bridge too far for most Member States, even with the inclusion of appro-*

[73] See subchapter 2.2.1.

[74] LYNSKEY, 'The Foundations of EU Data Protection Law', op. cit., pp. 18-19.

[75] Declaration on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007, no. 21. (Declaration 21).

[76] LYNSKEY, 'The Foundations of EU Data Protection Law', op. cit., p. 20.

[77] European Commission. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach to Personal Data Protection in the European Union. COM(2010)0609 final, p. 4.

[78] See LYNSKEY, 'The Foundations of EU Data Protection Law', op. cit., p. 20 or HUSTINX, 'EU data protection law', op. cit., p. 28.

[79] See HUSTINX, 'EU data protection law', op. cit., p. 15.

[80] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119.

priate limitations and exceptions."[81] The Police Directive 2016/680 repeals its predecessor, the Council Framework Decision 2008/977/JHA[82] and already entered into force on 5 May 2016. The Member States shall transpose it into their national laws by 6 May 2018.

Secondly, as Lynskey writes, although it is uncommon for an 'omnibus' regime to differentiate between sectors,[83] under the EU data protection, some sectors are indeed besides the general regime governed by other acts. They function as *leges speciales*.[84] A good example is the so-called E-Privacy Directive 2002/58/EC,[85] which is currently undergoing review. It applies to electronic communications services and public communications networks,[86] so in many instances also to cloud computing. In case that it does not regulate certain questions, the general regime of the Directive 95/46/EC and soon that of the GDPR steps in.[87]

Thirdly, the rules applicable to the processing of personal data by EU institutions and bodies are set forth in the Regulation 45/2001.[88] This regulation implements the Directive 95/46/EC and E-Privacy Directive and therefore represents a complete set of instruments applicable in the area.[89] It also establishes the European Data Protection Supervisor as an independent body (Article 41 (1)). Its responsibilites are set out in Article 42 (2) of the Regulation 45/2001, but predominantly, it is concerned with monitoring of the application of data protection within EU institutions and investigating complaints. Besides this supervizory body, the European Commission appointed a Data Protection Officer who monitors the application of data protection within the Commission. It shall be duly noted that the Commission proposed the amendment of Regulation 45/2001 to bring it in line with the GDPR in early 2017.

2.2 Recourse to the right to the protection of personal data

2.2.1 Privacy and the origins of the right to data protection

The emergence of the right to the protection of personal data is closely connected with the development of the concept of the right to private life. At an international level, privacy was as a human right *firstly* materialized in 1948 in Article 12 of the Universal Declaration of the Human

[81] See HUSTINX, 'EU data protection law', op. cit., p. 28.
[82] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350.
[83] LYNSKEY, 'The Foundations of EU Data Protection Law', op. cit., p. 23.
[84] Ibid.
[85] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201.
[86] Article 1 E-Privacy Directive 2002/58/EC.
[87] LYNSKEY, 'The Foundations of EU Data Protection Law', op. cit., p. 23.
[88] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8.
[89] HUSTINX, 'EU data protection law', op. cit., p. 14.

Rights. A non-legally binding instrument at the time. It focused on the prohibiton of *arbitrary interference* with one's privacy, family, home or correspondence.[90]

Of immense importance was the subsequent development in the Council of Europe, which in 1953 adopted the European Convention on Human Rights ('ECHR'), much later one of the main sources of the Charter.[91] ECHR enshrined in its Article 8 the right to *respect* for private and family life, one's home and correspondence, prohibiting *interference* by a *public authority* except for where permitted by law and necessary in the interest of higher democratic objectives.

However, ECHR failed to stend the test of the increasing employment of computers in the processing then undertaken mainly for administrative purposes.[92] Besides that, it overly focused on the interference caused by public authorities.[93] The Council of Europe recognized these deficiencies and in 1968 issued a Recommendation 509 adressed to the Committee of Ministers, calling for examination of the sufficiency of the protection of the *right to privacy* under ECHR and national laws of Member States in the light of *"modern science and technology"*.[94] The study showed that the protection was inadequate. The Commitee of Ministers responded by the adoption of two resolutions, establishing principles of data protection in private and public sector, Resolution (73) 22 and Resolution (74) 29 respectively.[95] The resolutions left it upon Member States, how they will give effect to the rules therein. The response was encouraging. National data protection laws were conceived for example in Germany, Sweden, Norway or France. Austria, Portugal and Spain soon even enshrined data protection into their constitutions.[96]

Council of Europe then recognized the need to bring national data protection laws closer together, again citing *"rapid evolution of information handling techniques"* and increasing processing activities involving different Member states as reasons.[97] A Convention for the protection of individuals with regard to automatic processing of personal data, also known as 'Convention 108',[98] which addresses these issues was adopted in 1981. It was widely accepted and ratified by all member states of the Council of Europe and the Community.[99] Convention 108 obliged the Parties, to give effect to the basic principles that it contained in their national laws.[100] It aimed to secure respect of the rights and fundamental freedoms, *in particular* the right to privacy, *"with regard to automatic processing of personal data "* relating to an individual regardless of nationality or

[90] Ibid, p. 3.

[91] See Article 52 (3) Charter.

[92] Explanatory Report to Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg: 28 January 1981, European Treaty Series – No. 108, para 1.

[93] HUSTINX, 'EU data protection law', op. cit., p. 4.

[94] 'Explanatory Report Convention 108', para 4.

[95] Ibid.

[96] Ibid, para 5.

[97] Ibid, paras 10-11.

[98] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 108 (Convention 108).

[99] HUSTINX, 'EU data protection law', op. cit., p. 4.

[100] Article 4 (1), (2).

residency (Article 1). It set out the definition of personal data as *"any information relating to an identified or identifable individual"* (Article 2 a) and dealt with the quality of data, which required that the personal data were among other things *"obtained and processed fairly and lawfully", "accurate and if necessary kept up to date"* or not used in a way incompatible with the purposes for which they were stored (Article 5) and therefore regarded processing as having to observe certain rules.[101] Besides that, Convention 108 contained provisions on general prohibition of processing of *special categories of data,* such as those revealing racil origin unless appropriate safeguards were provided (Article 6), data security (Article 7) as well as tranborder data flows (Article 12). The additional safeguards under Article 8 gave the data subjects for example the rights to rectification or erasure.

These principles are until present days in the heart of the EU data protection law.[102] Influential were also the recommendations subsequently issued by the Committee of Ministers to clarify the application of the Convention in different sectors.[103]

When referring to the importance of protection of personal data for privacy, the ECtHR repeatedly used the Convention 108 as a source of standards, but as Hustinx points out, never held that *any* processing would fall within the scope of Article 8 and therefore only applied the Convention 108 within the boundaries of privacy.[104]

Convention 108 remains binding to date and underwent modernization in 2016 to enable consistency with the reforms of data protection frameworks both in EU and OECD.[105] Even though it built solid foundations of the modern data protection law, national laws were still regarded as lacking sufficient consistency. The European Commission saw that as a threat to internal market and therefore set out to regulate data protection by a Directive 95/46/EC.[106] Its objective was twofold.[107] Directive aimed at securing the *free flow of personal data* among Member States, while ensuring protection of fundamental rights and freedoms, in particular the right to privacy *with respect to data protection* (Article 1). The Directive adopted many of the principles laid out in the Convention 108 and provided a more detailed regulation. It resulted in an increased harmonization but again did not reach its desired level[108] and ultimately led to a reform of the data protection framework in the EU that is on-going since 2012.

The Directive predated EU's adoption of its own catalogue of fundamental rights. The route of the EU towards their recognition at a primary law level was not without flaws. EC Treaty

---

[101] HUSTINX, 'EU data protection law', op. cit., p. 6.

[102] Ibid, pp. 5-6.

[103] Ibid, pp. 6-7, e.g. Recommendation No. R (83) on the protection of personal data used for scientific research and statistics.

[104] Ibid, p. 7.

[105] Modernization of Convention 108 (CAHDATA). Council of Europe [online]. Available at: <https://www.coe.int/en/web/data-protection/convention108/modernisation>. Last accessed 3 March 2018.

[106] HUSTINX, 'EU data protection law', op. cit., p. 9.

[107] Ibid.

[108] Ibid.

originally made no express mention of fundamental rights. In 1950 in *Stork,* the Court held that it did not have a competence to examine whether Community measures infringed on fundamental rights guaranteed by a Constitution of a Member State.[109] After a gradual development, in 1969 the Court recognized that fundamental rights are enshrined in the general principles of the Community law and therefore protected by the Court.[110] In 1970 it held again that respect for fundamental rights formed integral part of the general principles and that their protection must be ensured. Moreover, the Court added that it was inspired by the common constitutional traditions of Member State when assessing its scope.[111] In 1974 in *Nold* it noted that its inspiration is also drawn from international treaties of which Member States are signatories.[112] This case law gained increasing support over the years and Article 6 (3) TEU then did nothing but confirmed it.[113]

However, since the Charter gained legally binding force, the EU officially recognizes also the rights, freedoms and principles set out therein (Article 6 (1) TEU) as an autonomous source of law, going beyond general principles.[114] It shall be noted that even before the Lisbon Treaty conferred on the Charter a legally binding force, the Charter was regarded as an authoritative and consequently, the Courts often referred to it.[115]

The need for the Charter was long considered in scholarly literature, which called for a catalogue that could be invoked directly in the context of the Union law. Debate also evolved around the question of the list of the rights to be included therein. Some considered that the catalogue could cover also rights that were not enshrined in the ECHR.[116] However, the reasons for inclusion of the right to the protection of personal data, untraditionally in a provision separate from privacy, remain unclear.

2.2.2 The right to protection of personal data and right to privacy in the Charter

Article 7 of the Charter concerns the right to respect for private and family life, home and communications, from which data protection originally stems.[117] It states that "[e]veryone has the right to respect for his or her private and family life, home and communications."

The right to the protection of personal data is explicitly separately granted under Article 8. It holds in three sections that: *"1. Everyone has the right to the protection of personal data concerning*

[109] Friedrich Stork & Cie v High Authority of the European Coal and Steel Community, C-1/58, EU:C:1959:4, para 26.
[110] Erich Stauder v City of Ulm – Sozialamt, C-29/69, EU:C:1969:57, para 7.
[111] Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel, C-11/70, EU:C:1970:114, para 4.
[112] J. Nold, Kohlen-und Baustoffgroßhandlung v Commission of the European Communities, C- 4/73, EU:C:1974:51, para 13.
[113] LENAERTS, Koen, VAN NUFFEL, Piet. European Union Law. Third edition. BRAY, Robert, CAMBIEN, Nathan (Eds.). London: Sweet & Maxwell, 2011. rec. 22-019.
[114] Ibid, rec. 22-016.
[115] Ibid, rec. 22-022.
[116] Ibid, rec. 22-020.
[117] KRANENBORG, Herke. Article 8. In: The EU Charter of Fundamental Rights: A Commentary. London: Hart Publishing Ltd., 2014, pp. 228 et subseq.

him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."

Article 52 (1) then provides that these rights are not absolute and shall be weighted against fundamental rights and freedoms of others under the principle of proporcionality.

The inclusion of a separate provision dealing with the right to the protection of personal data is quite unique at a higher than the state level. There is also no common tradition in granting an autonomous right to the protection of personal data among Member States.[118] In fact, their constitutional traditions largely differ in this matter.[119] The connection with Article 8 of the ECHR is also unclear. Consequently, Article 8 of the Charter and its relationship with Article 7 raises many questions.

Firstly, based on the explanation[120] on Article 7 of the Charter,[121] rights guaranteed thereunder correspond to the scope of Article 8 of ECHR. This is not surprising since the provisions mirror each other. However, the explanation on Article 8 states that Article 8 is also based on *Article 286 of the EC Treaty,*[122] *Directive 95/46/EC, Convention 108 and Article 8 of the ECHR.* [123] But these all pursue protection of privacy as their ultimate goal.

Article 52 (3) then states that the meaning and scope of a Charter right which *"corresponds to rights guaranteed by the [ECHR]"*, shall have the same *meaning and scope* as the right enshrined in the ECHR, though EU may guarantee higher degree of protection. In other words, the case law of the ECtHR under Article 8 may be relevant when applying the corresponding right under the Charter but at the same time may not be conclusive.[124] To be clear, ECHR does not expressly provide for the right to data protection, but the ECtHR has been addressing issues concerning data protection citing Article 8 of ECHR on the right to privacy in its case law.[125] It is appropriate to at least note that since *Niemietz*[126], the ECtHR saw the notion of private life as broad, aligning under its scope data protection, holding that private life includes for example some professional and business activities.[127]

From what was explained above, it follows that the right to the protection of personal data as an autonomous right was not part of the general principles. It cannot be subordinated neither

---

[118] FUSTER GONZÁLES, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* First Edition. Brussels: 2014, Springer International Publishing, 2014, p. 199.

[119] See FUSTER GONZÁLES, 'The Emergence', op. cit., p. 175 et subseq.

[120] Now replaced by Articles 16 of TFEU and 39 of TEU.

[121] For the role of explanations see LENAERTS, 'European Union Law', op. cit., rec. 22-022.

[122] Now replaced by Articles 16 of TFEU and 39 of TEU.

[123] Explanations relating to the Charter of Fundamental Rights, OJ C 303, 14.12.2007.

[124] KRANENBORG, 'Article 8', op. cit., p. 235.

[125] FUSTER GONZÁLES, Gloria and GELLERT, Raphael. The fundamental right of data protection in the European Union: in search of an uncharted right. In: *International Review of Law, Computers & Technology.* March 2012, Vol. 26, No. 1, p. 74.

[126] Niemietz v Germany App no 13710/88. ECtHR, 16 December 1992. A-251-B.

[127] Ibid, at 29.

under the common constitutional traditions nor ECHR. Therefore, it can be treated as a newly added right.[128] But is it really autonomous as its inclusion in a separate article suggests?

At least in the scholarly literature, the prevailing opinion seems to be that although the right to privacy and the right to data protection are closely connected, they cannot be seen as one and the same right and the right to data protection has a distinct quality.[129] Firstly, the substantive scope of data protection seems different than that of privacy. Often, it is considered to be broader. Whilst privacy does not necessarily include *all the information* on identified or identifiable persons, data protection does.[130] Data protection encompasses information which are not sensitive, such as car ownership and would not necessarily infringe on privacy.[131]

The right to the protection of personal data does not seem to fit the traditional notion of fundamental or human rights. It is designed to facilitate data processing that is seen as inevitable and ensure that such handling of the data is lawful.[132] While there are cases where questions at issue qualify as fundamental by their importance many protect ordinary interests. Data protection is not necessarily empowering individuals but rather restricting the behaviour of others.[133] The right to privacy protects against interference while data protection contains rules for lawful interference.[134]

The argument that data protection equals privacy stands on the assumption that data protection guarantees self-determination, i.e. control over personal information, and that the right to privacy in fact is the right to control personal information. But this assumption may be incorrect, since the notion of informational self-determination, coming from a German tradition, does not correspond with the view of the data protection in the EU. While *informationelle Selbstbestimmung* sees consent as central for lawful data processing, the EU data protection looks beyond consent.[135]

The disconnection of the two rights seems to be supported also by the choice of terminology used in the GDPR. The Directive makes reference to the right to privacy 13 times and when setting its objective, states that: *"Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to processing of personal data".*[136] No reference to the right to privacy appears in the GDPR, which also replaces the word 'privacy' with 'data protection' in its terms, e.g. changing "privacy impact assessment" to "data protection

[128] See LENAERTS, 'European Union Law', op. cit., rec. 22-020.

[129] KRANENBORG, 'Article 8', op. cit., p. 229.

[130] KOKOTT, Juliane and SOBOTTA, Christoph. The distinction between privacy and data protection. In: *International Data Privacy Law,* 2013, Vol. 3, No. 4, p. 225.

[131] VAN DER SLOOT, Bart. Legal Fundamentalism: Is Data Protection Really a Fundamental Right? In: *Data Protection and Privacy: (In)visibilities and Infrastructures.* LEENES, Ronald, VAN BRAKEL, Rosamunde, GUTWIRTH, Serge and DE HERT, Paul, (Eds.) Switzerland: Springer International Publishing, 2017, p. 5.

[132] Ibid, p. 28.

[133] FUSTER GONZÁLES and GELLERT, 'In search of an uncharted right', op. cit., p. 80.

[134] VAN DER SLOOT, 'Legal Fundamentalism', op. cit., p. 22.

[135] KRANENBORG, 'Article 8', op. cit., p. 229.

[136] Article 1 of the Directive.

assessment". Also, the objective follows this pattern and referrs to the *"rules relating to the protection of natural persons with regard to the processing of personal data"*[137], *"[the] right to the protection of personal data"*[138] and *"free movement of personal data"*[139].

In summary, right to data protection seems to have different nature from privacy, its autonomous standing seems to be supported by its inclusion in a separate article in a Charter and recently, the changed terminology in the GDPR. However, the case law of CJEU is still covered in veil of uncertainty when it comes to recognizing the different nature of the two rights. More guidance is needed mainly regarding the scope and limits of the right to personal data protection with regard to growing importance of the field in the digital age.

I will now briefly look at the development of the reasoning of the CJEU to support my argument that there is a deeply rooted 'privacy thinking'[140] with regard to data protection in the case law and that this approach is being slowly abandoned.

Before the Charter gained legally binding force, the case law was affected by the joined reading of privacy and data protection. In *Österreichischer Rundfunk*[141], several Austrian public undertakings, Österreichischer Rundfunk included, refused to communicate some personal data of their employees to the Austrian Court of Auditors. The Court did not take the argument that this situation did not fall into the scope of the Directive 95/46/EC, since the control served public interest and did not obstruct the free movement of workers in the EU and held that its applicability cannot depend on whether there was a sufficient link with the exercise of the free movement, regardless of the directive being an internal market instrument.[142] In this particular case, the Court analysed extensively if the issue at stake interfered with *private life* and if so, whether that was justified under *Article 8 ECHR* (the Charter was not even mentioned). In other words, it interpreted the Directive in the light of the right to respect for private life,[143] drawing no distinction between privacy and data protection.[144]

It was not until 2008 that the Court referred to Article 8 of the Charter in its judgment directly for the first time when observing that the article expressly proclaims the right to the protection of personal data in *Promusicae v Telefónica de Espana.*[145] However, the rhetoric remained similar as in previous decisions, since CJEU only mentioned Article 8 and then dealt with the issue at stake as with a conflict between the right to respect for private life and rights to the

[137] Article 1 (1), GDPR.

[138] Article 1 (2), GDPR.

[139] Article 1 (3), GDPR.

[140] FUSTER GONZÁLES and GELLERT, 'In search of an uncharted right', p. 79.

[141] Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk, joined cases C-465/00 and C-138/01 and C-139/01, EU:C:2003:294.

[142] Ibid, at 42.

[143] Ibid, at 68.

[144] Ibid, at 72.

[145] Productores de Música de España (Promusicae) v Telefónica de España SAU, C-275/06, EU:C:2008:54, at 64.

protection of property and right to an effective remedy, treating data protection and privacy as equal.[146]

The reluctance of the CJEU to provide an analysis based *solely* or at least predominantly on Article 8 remained a trend in its case law. In *Rijkeboer* CJEU referred to the purpose of the Directive 95/46/EC, framing it under the protection of privacy of individuals.[147] In *Schecke,*[148] the Court saw the fundamental right to the protection of personal data as closely connected with the right to respect for private life,[149] which implied, although not clearly, keeping of a distance from the previous views.

In *Deutsche Telekom,*[150] the Court declared the Directive 95/46/EC to be designed to ensure observance of the right to the protection of personal data.[151] Later, it interpreted the Directive 95/46/EC in the light of data protection in *Schrems*[152] in *Google Spain*[153] and again in *Coty* case.[154] However, without providing any thorough argumentation as to its scope and nature, as both Hustinx and Lynskey point out. CJEU therefore remains struggling with defining the role of the Article 8 with suffiecient clarity,[155] much needed in connection with the harmonising efforts of the data protection reform in the EU.

2.3 Reforming data protection law in the European Union

Data protection was among the most discussed issues in the EU in recent years. New innovations and technologies placed great pressure on legislators to implement appropriate data protection framework. The principle EU data protection secondary law instrument preceding the GDPR, Directive 95/46/EC was proposed in the early 1990's, adopted in 1995 and came into effect in October 1998. Back then, the Internet was still in its infancy. The impact of the digitalization of the single market could not have been forseen. Viviane Reding[156] called what has happened since the adoption of the Directive 95/46/EC a "data revolution"[157]. Previously unimaginable ways of online data processing emerged, bringing lack of control over data protection. During the years, technologies used by few become widespread in the daily lives of all of us. The Directive

[146] Ibid, at 65.

[147] College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer, C-553/07, EU:C:2009:293.

[148] Volker und Markus Schecke and Eifert v Land Hessen, joined cases C-92/09 and C-93/09, EU:C:2010:662.

[149] Ibid, at 47.

[150] Deutsche Telekom AG v Bundesrepublik Deutschland, C-543/09, EU:C:2011:279.

[151] Ibid, at 50.

[152] Maximillian Schrems v Data Protection Commissioner, C-362/14, EU:C:2015:650.

[153] Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, EU:C:2014:317.

[154] Coty Germany GmbH v Stadtsparkasse Magdeburg, C-580/13, EU:C:2015:485, at 30.

[155] LYNSKEY, 'The Foundations of EU Data Protection Law', op. cit., p. 270 and HUSTINX, 'EU data protection law', op. cit., p. 31.

[156] Vice-President of the European Commission; EU Commissioner responsible for Justice, Fundamental Rights and Citizenship at that time.

[157] REDING, Viviane. The upcoming data protection reform for the European Union. *International Data Privacy Law.* 2011, Vol. 1, No. 13, p. 3.

95/46/EC was not designed to cope with complexities that the digital age brought. Innovations like cloud computing fell into regulatory grey area,[158] increasingly having to deal with inappropriate data protection laws, lacking sufficient harmonization and its administrative implications.

Number of problems that the Directive 95/46/EC entailed were recognized ever since the first review report[159] published by the Commission in May 2003. The Commission however noted that there was too little experience with the Directive to allow for a reform. But a Work Programme was launched and mainly WP29 played an important role in highlighting the issues in the following years.[160] In March 2007, in its second report, the Commission took the view that it was still early for a thorough review.[161]

Nevertheless, the three main concerns that created a challenge for the data protection framework where identified by the Commission as the new capabilities of modern technologies, globalized data flows and incerased access to data by law enforcement authorities for reasons such as public security, threatening adherenece to principles like necessity and proporcionality.[162] Consequently, the European Commission launched in 2009 a public consultation to determine, whether data protection law in fact really needed to be systematically reformed to cope with the new challenges.[163] The outcome unsurprisingly showed that the current data protection framework was largely outdated.[164] The ambitous aim was identified as to pass a reform that will *"stand the test of the time"*[165]. In other words, will cope with the challenge of rapid technological innovation and not need to be substantially revised in the upcoming years again.

The European Commission presented its original proposal of the GDPR in January 2012[166] as part of a broader data protection reform package (having as the second main element the Police Directive), with the aim to adopt the Regulation as soon as possible at the end of the parliamentary term in 2014 at the latest.[167] The new data protection instruments focused on ensuring *effectiveness* in *"a world where data processing become ubiquitous"*[168], increased *consistency* as a rec-

[158] VIDOVIC ŠKRINJAR, Marina. EU Data Protection Reform: Challenges for Cloud Computing. In: *Croatian Yearbook of European law & Policy.* 2016, Vol. 12, No. 12, p. 172.
[159] Article 33 of the Directive 95/46/EC requires the Commission to report on the implementation of the directive and monitor whether amendments are needed.
[160] HUSTINX, 'EU data protection law', op. cit., p. 25.
[161] Ibid.
[162] READING, 'The upcoming data protection reform', op. cit., p. 3.
[163] HUSTINX, 'EU data protection law', op. cit., p. 25.
[164] SERVENT RIPOLL, Ariadna. Protecting or Processing? Recasting EU Data Protection Norms. In: *Privacy, Data Protection and Cybersecurity in Europe.* Springer International Publishing, 2017, p. 119.
[165] READING, 'The upcoming data protection reform', op. cit., p. 5.
[166] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final.
[167] SERVENT RIPOLL, 'Protecting or Processing?', op. cit., p. 119.
[168] HUSTINX, 'EU data protection law', op. cit., p. 26.

tion to insufficient harmonization and *comprehensiveness*,[169] aiming at decreasing fragmentation of the secondary law as allowed by the Lisbon Treaty, which then failed to materialize.[170]

Hand in hand with the proposal, the European Commission also adopted a communication titled "Unleashing the Potential of Cloud Computing in Europe"[171] as part of its Digital Single Market Strategy, making it clear that the GDPR shall be an enabling law, dealing with data protection legislation as one of the main barriers for the spread of cloud computing in the EU.[172] As the main points to be implemented into the new law from the point of view of the cloud were recognized harmonization, increased transparency, determination of the territorial scope and international data transfers.[173] Though not legally binding, the Commission expressly welcomed[174] the opinion on cloud computing issued by the WP29,[175] where it elaborated on the cloud computing specifics in more detail, citing lack of control over personal data and transparency as the core issues and proposed recommendations on how to apply the Directive in the cloud. Many of the recommendations therein were reflected in the text of the GDPR.

The proposal of the Commission was first passed on to the European Parliament and the Council with the aim to reach a unified position. However, the negotiations took much longer than expected. As is usually the case, the original proposal was more ambitious than the text that was adopted in the end. Negotiations discussions were based around fundamental tensions between liberty and protection (or inaccuratly, security), brought in by the left-wing parties. The Committee appointed to scrutinize the GDPR proposal was LIBE (Committee on Civil Liberties, Justice and Home Affairs), whose rapporteur was at the time Jan Phillip Albrecht (Germany), well-known for his strong support of data protection. The economic logic was brought into the discussion by the centralist and right-wing parties that saw the proposal as too idealistic.[176] Nevertheless, the proposal was exposed to 3999 amendments suggested by the Commitee, of which 207 were approved by the Parliament at the first reading.[177] The extent of the negotiations is well illustrated by the comparison with the Directive, whose proposal saw 363 suggested amendments.[178] Though it shall be also noted that when the Directive was being negotiated, there were only 12 Member States (15 from January 1995). Viviane Reading said about the compromise that was reached that *"[i]t equips regulators with strong enforcement powers and it allows companies to exploit the full potential of the digital economy".*[179] In 2013, the Snowden scandal accelareted the

[169] Ibid, p. 27.
[170] Ibid, p. 25.
[171] European Commission, 'Unleashing the Potential of Cloud Computing in Europe', op. cit.
[172] Ibid, p. 8.
[173] Ibid.
[174] Ibid, p. 9.
[175] WP29 Opinion 05/2012 on cloud computing (WP196), adopted on 1 July 2012.
[176] SERVENT RIPOLL, 'Protecting or Processing?', op. cit., p. 121.
[177] Ibid, p. 120.
[178] For very illustrative graphs see <http://blog.kuan0.com/2015/01/data-protection-directive-vs-draft-data.html>. Last accessed 1 March 2018.
[179] SERVENT RIPOLL, 'Protecting or Processing?', op. cit., pp. 120-122.

discussions. The proposal was voted on in the European Parliament in March 2014 and received a great support in the end (621 votes for, 10 against, 22 did not vote).[180]

The tough trialogue between the European Commission, European Parliament and the Council followed. It did not start until June 2015 and lasted throughout the year. Concerns of the Member States showed considerations of how some of the high standards and strict rules of the new Regulation will affect businesses. The controversies mostly circled around the scope of the Regulation and the level of harmonisation.[181] Another large concern was the so-called *"on-stop-shop",* which would see an extensive oversight of the compliance by the European Data Protection Board.[182] Major role in the negotiations played also the ICT lobby, determined to limit GDPR and ensure that it would not hinder the rapid development of the industry. In one of the key features of the GDPR, its penalties for non-compliance that it targeted, the lobbysts were largely unsuccessful. They saw only a decrease from 5% to 4% of the worldwide turnover.[183] Last but not least, another actor that considerably influenced the final version of the GDPR was CJEU, which in the course of the negatiations invalidated the Data Retention Directive 2006/24/EC[184] in the *Digital Rights Ireland*[185] case, discussed how data protection law applied to internet search engines in *Google Spain* and lastly among other things also invalidated the Safe Harbour, an adequacy decision concerning transfers of personal data between the EU and US.[186] The GDPR was in the end adopted literally after years of negotiations in April 2016 and is set to enter into force on the 25th May 2018.

The GDPR does not specifically deal with cloud computing but strives to be technologically neutral and therefore shall apply regardless of the technologies used in the processing. Since it is designed to apply to any technology or innovation, the practical implications differ based on their nature. I will analyze the main consequences specific for the cloud computing in the fourth chapter, but first look at the building stones of the GDPR.

The Directive 95/46/EC regime represented a solid foundation for the reform, since most of its principles remained valid even in the internet era.[187] As will become apparent, *"in spite of all innovation – there is also a lot of continuity"*[188] in the GDPR.

---

[180] Ibid.
[181] Ibid.
[182] Ibid.
[183] STAIGER, 'Data protection compliance in the cloud', op. cit., p. 152.
[184] Directive 2006/24/EC of the European Parliament and the of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 2016 OJ L 105/54.
[185] Digital Rights Ireland, Joined Cases C-293/12 and C-594/12, EU:C:2014:238.
[186] VIDOVIC ŠKRINJAR, Marina. 'EU Data Protection Reform', op. cit., pp. 174-175.
[187] REDING, 'The upcoming data protection reform', op. cit., p. 4.
[188] HUSTINX, 'EU data protection law', op. cit., p. 28.

3 General Data Protection Regulation

The GDPR is an outcome of a gradual evolution of the european data protection framework that has taken place since the turn of the century. Many elementary concepts remain untouched or are only subtly changed for the sake of a more detailed regulation. The GDPR is not a violent revolution, though being sometimes presented as such in the media. Therefore, substantial part of the case law on the principles and definitions remains valid.

The innovations of the new regime can be characterized as putting increased emphasis on limitation of processing of personal data where this is not strictly necessary, technological neutrality, employment of the best practices in terms of implementation of technical and organizational measures, and enhanced transparency and control over the data by the data subjects. GDPR pushes controllers and processors to take data protection into account from the very start of their operations, and through the whole process.[189] It stresses their responsibility, which is newly allocated differently and threatens incompliance by an extensive catalogue of fines.

The GDPR has 99 Articles compared to 34 in the Directive. Yet, the Regulation shall simplify the regime and reduce costs from the controller's point of view, at least through the implementation of a one-stop-shop principle, which implies that businesses may have to deal only with a single supervisory authority when doing business in the EU. GDPR has a potential to further harmonize data protection in the EU and thus enhance legal certainty for both data controllers and processors. Its direct applicability shall secure this goal. Nevertheless, it leaves some leeway for Member States.[190] Therefore, harmonisation shall be strengthened, but not strictly fully achieved.[191] In any case, the GDPR clearly cannot be overriden by a contradicting national law. Face to face with the Regulation, such rules would be inapplicable.

Much depends also on how *consistent and homogenous* the application of the GDPR will be in practice.[192] Recital 10 holds that the data protection of individuals shall be *"equivalent in all Member States"*. To that end, Rüger suggests that the GDPR needs to be interpreted independently from national implementations of the Directive and prior decisions of national courts.[193] The wording of the provisions and the Recitals are suggested as a starting point.[194] Second in relevance shall be guidelines and other statements provided by the supervisory authorities[195] and WP29, as far as they may be deemed valid in the light of the changes and are not repealed. WP29

[189] Ibid, pp. 28-29.
[190] There are more than 50 opened options for the national legislator. Perhaps the most discussed is the employment context (Article 88, GDPR). For their assessment see SCHUMACHER, Pascal. In: *New European General Data Protection Regulation.* A Practitioner's guide. Ensuring Compliant Corporate Practice. First edition. RÜCKER, Daniel, KUGLER, Tobias (Eds.), rec. 206-230.
[191] RÜCKER, In: 'New European General Data Protection Regulation', op. cit., rec. 9-10.
[192] Recital 10, GDPR.
[193] RÜCKER, In: 'New European General Data Protection Regulation', op. cit., rec. 30-31.
[194] Ibid, rec. 33.
[195] Article 51 (2), GDPR.

shall be upon the GDPR's entry into force replaced by the European Data Protection Board ('Board'), which will takeover its agenda and whose role is strengthened compared to its predecessor.[196] However, a more prominent role will of course have the new case law of the CJEU in the future. At the moment, to a lesser extent than the guidelines of the WP29, statements of the Commission, European Data Protection Supervisor or other European institutions may be considered as well.[197] I take Rüger's suggestions into account and go beyond them with citations of case law where applicable.

3.1 Scope of application

3.1.1 Material scope

Material scope of application of the GDPR is set out in its Article 2 in four sections. First, the general rule is provided and then exceptions to it. The interaction with E-commerce directive 2000/31/EC[198] is also considered.[199] The general rule copies word by word the provision contained in Article 3 (1) of the Directive[200] and so provides that the GDPR applies to the: *"[p]rocessing of personal data wholly or partly by automated means* and to the processing of personal data *other than by automated means of personal data which form part of a filing system or are intended to form part of a filling system."*[201]

In other words, given that the processing is undertaken wholly or partly using automated means, the applicability of the GDPR is triggered if *any* such processing occurs. In particular, it does not matter what technology is used as GDPR strives to be technologically neutral.[202]

On the other hand, when the processing is done manually, it falls under the scope of the GDPR *only if* the data are (or at least are intended to be) organized in a file, i.e. according to certain criteria. Manual processing done without any structure, classification or rules, is not subject to the GDPR.[203]

Exemptions pursuant to Articles 2 (2) and 3 entail that even if the processing is such that it fits the general rule described above, the GDPR does not apply if the processing:

---

[196] For tasks of the EDPB see Article 70 (1), GDPR and RÜCKER, In: 'New European General Data Protection Regulation', op. cit., rec. 35-38.

[197] RÜCKER, In: 'New European General Data Protection Regulation', op. cit., rec. 40.

[198] 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 ('Directive on electronic commerce'), OJ L 178.

[199] Article 2 (1) – (4), GDPR.

[200] As well as the corresponding national legislation in the Czech Republic (i.e. §3 (2) and (4) of the Act no. 101/2000 Coll., on the Protection of Personal Data and on Amendment to Some Acts; English translation available at <https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_ktg=1107>. Last accessed 14 February 2018.

[201] Emphasis added, Article 2 (1), GDPR.

[202] Recital 15, GDPR. In line with the Directive.

[203] Such processing may be subject to other laws, such as Civil Codes, or other Acts dealing with confidentiality issues etc. See NULÍČEK, Michal, DONÁT, Josef, NONNEMANN, František, LICHNOVSKÝ, Bohuslav a TOMÍŠEK, Jan. GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář. Praha: Wolters Kluwer ČR, 2017, p. 66.

[1] is undertaken "in the course of an activity falling outside of the scope of the Union law";[204]
[2] or "by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the 'TEU'";[205]
[3] or "by a natural person in the course of a purely personal or household activity";[206]
[4] or "by competent authorities in the course of dealing with criminal offences and their prevention, as well as threats to security";[207]
[5] or is undertaken by the Union institutions, bodies, offices and agencies.[208]

The third exemption listed above deserves to be analyzed in more detail, since it is a controversial issue in the digital era.[209] One of the arguments for its introduction in the 1990s was that processing in the course of household activity did not pose risk to data protection.[210] But processing undertaken online, even if for personal purposes only, is of course not entirely harmless. With the ubiquity of the Internet, issues emerged with regard to what can be defined as a personal and household activity in the modern days, where boundaries between private and public blur.

Under the Directive, CJEU first provided guidance in *Lindqvist,*[211] where it dealt with the case of *publication of personal data on a website*. Mrs Lindqvist, who worked in a parish of a Swedish Protestant Church, set up a personal website where she was publishing information about her co-workers. The information sometimes included first names, jobs held, telephone numbers and in many cases also hobbies and other personal information described in a humorous way. Mrs Lindqvist had not informed her colleagues about the website, obtained their consent or informed the data protection authorities about her activities. She took the website down as soon as she found out that some of her colleagues had issues with the information being published. But, nevertheless, was found guilty of an offence and fined for unlawful processing. CJEU subsequently held that the processing she had undertaken fell within the scope of the Directive and corresponding national legislation and could not be treated under household exemption,[212] especially *since the data on a website were accessible to an indefinite number of people.*[213]

[204] Article 2 (2) (a), GDPR.
[205] Article 2 (2) (b), GDPR.
[206] Article 2 (2) (c), GDPR.
[207] Article 2 (2) (d), GDPR.
[208] Article 2 (3), GDPR.
[209] Article 2 (2) (c), GDPR.
[210] MITROU, Lilian. The General Data Protection Regulation. A Law for the Digital Age? In: *EU Internet Law.* Regulation and Enforcement. SYNODINOU, Tatiana-Eleni, JOUGLEUX, Philippe, MARKOU, Christina, PRASTITOU, Thalia (Eds.), Springer International Publishing, 2017, p. 25.
[211] Criminal proceedings against Bodil Lindqvist, C-101/01, EU:C:2003:596.
[212] Ibid, paras 12-28.
[213] Ibid, para 47.

Most recently, in *Ryneš,*[214] CJEU addressed the scope in which data protection law applies to the use of *CCTV cameras,* sheding some more light on when the exemption applies with regard to new technology. Mr Ryneš installed a camera system on his home following several attacks by unknown persons on him and his family, stating as the only reason of taking such a measure protection of his property. The camera recorded the entrance to his home, public footpath, and the entrance to the opposite house. The recordings were only visual and stored on a hard disk drive. If it reached its capacity, the new recordings would be saved over the old ones. It was only Mr Ryneš who had access to the data and the recordings could not be watched live. After the installation, when another attack took place, Mr Ryneš handed the recording to the police and attackers were identified as a result. Following the criminal proceedings, Office for Personal Data Protection confirmed upon the request of one of the suspects that the surveillance was unlawful. Mr Ryneš challenged the decision first in Prague City Court, and then appealed on point of law before the Supreme Administrative Court, which referred for a preliminary ruling to the CJEU.[215] The question was whether the operation of the camera system in question could be classified as processing in the course of 'purely personal and household activity'. The Court held it could not.[216] Notwithstanding the context of the case, the camera monitored a public space and stored personal data obtained. The Court explained that *processing is covered by the exemption only where it is carried out in the purely household 'setting of the person that is processing the data'.*[217] The Court also emphasized that the Directive was intended to ensure high level of protection of personal data[218] and that it was settled case law that any derogations in relation to protection of personal data as a fundamental right must 'apply only in so far as is strictly necessary'.[219] Besides that *'purely'* in the wording of the provision itself, implies that the processing has to lack any connection to commercial or other professional activities whatsoever.[220] Examples of processing which will amount to household exemption were said to include writing down information in a personal diary or storing them for correspondence.[221]

As Woods suggests, *Lindqvist,* which was not cited by the Court in *Ryneš,* might have been omitted because of lack of detailed argumentation provided therein. However, the cases should not be seen in isolation, but rather treated as consistent case law covering the scope of application of the household exemption.[222] *The household exemption therefore should be construed narrowly.*[223]

---

[214] František Ryneš v. Úřad pro ochranu osobních údajů, C-212/13, EU:C:2014:2428.

[215] Ibid, paras 13-18.

[216] Ibid, para 36.

[217] Ibid, para 32.

[218] Ibid, para 27.

[219] Ibid, para 28. The Court referring to IPI, C-473/12, EU:C:2013:715, para 39, and Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, para 52.

[220] 'Ryneš', op. cit., para 30.

[221] Ibid, para 32.

[222] WOODS, Lorna. Bringing Data Protection Home? The CJEU rules on data protection law and home CCTV [online]. In: <www.eulawanalysis.blogspot.cz>. Available at: <http://eulawanalysis.blogspot.cz/2014/12/bringing-data-protection-home-cjeu.html>. Last accessed 2 March 2018.

Many called for clearer definition of the household exemption under the GDPR. The original proposal submitted by the European Commission reffered to *"exclusively"* personal and household activities instead of "purely". Another proposed change concerned a phrase *"without any gainful interest"* but was also dropped and the wording remained identical to the one in the Directive. As a result, the settled case law touched on above is applicable under the GDPR, though its further development may be expected in the near future.

Other guidance, which may be helpful with regard to SaaS social networking services, was provided by the WP29[224] and statements in Recital 18 of the GDPR. In line with *Lidqvist* and its requirement of closed number of people who can access the data, SaaS social networking services and other similar online activities where the processing is undertaken by natural persons for personal purposes, are going to fall within the scope of the exemption, *given the person shares personal data only with the users with whom he or she is connected* through the social network (has them for example as 'friends' on Facebook). But if a person shares personal data with all the users of that network, such processing shall not be regarded as purely personal and the user of the network will not be protected by the personal and household exemption.[225] Caution therefore needs to be exercised when information is shared in public groups on Facebook or majority of profiles on Instagram, a social network build on a business model that requires open profiles for its effectiveness.

Importantly for cloud computing, according to Recital 18, GDPR will in any case apply to the providers who provide the means of processing of personal data for purely household activities undertaken by natural persons,[226] regardless if they are processors or controllers in the particular case. In other words, GDPR will apply to cloud service providers of SaaS, such as storage services, e.g. Dropbox Personal or social networking, e.g. Facebook or Instagram, regardless of how the activities of their users are regarded. Mitrou notes the above-mentioned attempts to shape the household exemption, emphasizes their failure and claims that the challenge of sufficiently protecting the rights of the individuals whose personal data are in the hands of users of social networks, while not threatening openness of information and communication, should have been striked better.[227]

To sum up, issues which may arise with regard to cloud computing concern mainly social networking and SaaS targeted at end-users. The ultimate aspect to consider is when assessing household exemption face to face online services is whether the data can be accessed by an indefinite number of people.[228]

---

[223] 'Ryneš', op. cit., para 29.

[224] WP29 Opinion 5/2009 on online social networking (WP163), adopted on 12 June 2009.

[225] DONÁT, Josef, TOMÍŠEK, Jan. *Právo v síti. Průvodce právem na internetu.* 1. vyd. Praha, C.H. Beck, 2016, p. 47.

[226] Recital 18, GDPR.

[227] MITROU, 'A Law for the Digital Age?', op. cit., p. 28.

[228] 'Lindqvist', op. cit., para 47.

The last matter that Article 2 on material scope addresses is the interaction of the GDPR with the E-commerce directive.[229] GDPR states that its application shall be without prejudice to the E-Commerce directive, in particular of the exclusion of liability rules of the internet service providers, as laid down in Articles 12 to 15 therein.[230]

Nevertheless, to be able to draw any conclusions about the material scope of the GDPR, we need to look at the interpretation of the two key terms, processing and personal data.

3.1.2 Processing

Processing means any operation or a set of them, performed on the personal data or their set, whether or not by automated means.[231] A 'set of operations' may refer to operations undertaken simultaneously, in stages, by one actor, or multiple.[232]

Since the GDPR is technologically neutral,[233] the list of operations that are expressly considered processing pursuant to Article 4 (2) is designed as non-exhaustive and includes the most common operations such as collection of data, their storage, alteration, erasure, destruction, disclosure, or dissemination. But practically any manipulation with the data can fall within the scope of the term,[234] including short-term operations even with small amounts of data.[235] The definition of processing under the GDPR is wide and does not bring changes compared to the previous regime.[236] Automated processing entails the use of *computers, smartphones, web cameras, drones, so-called wearable devices (e.g. Fitbit), and other devices*.[237] From a technical perspective, it is also indecisive whether the data are actually downloaded into a system and stored or merely showed on a screen, for the processing to fall under the GDPR.[238]

In *Google Spain,*[239] CJEU emphasized that operations must also be regarded as processing under the Directive even if they *"[…] exclusively concern material that has already been published in unaltered form in the media"*[240]. Publication does not render data non-personal.[241] The Court also

---

[229] 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 ('Directive on electronic commerce'), OJ L 178.
[230] Article 2 (4), GDPR.
[231] Article 4 (2), GDPR.
[232] WP29 Opinion 1/2010 on the concepts of "controller" and "processor" (WP169), adopted on 16 February 2010, p. 18.
[233] Recital 15, GDPR.
[234] RÜCKER, In: 'New European General Data Protection Regulation', op. cit., rec. 52.
[235] VOIGT, Paul, VON DEM BUSSCHE, Axel. *The EU General Data Protection Regulation (GDPR).* A Practical Guide. Springer International Publishing, 2017, p. 10.
[236] RÜCKER, In: 'New European General Data Protection Regulation', op. cit., rec. 51-53.
[237] Examples drawn from VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 10.
[238] Ibid.
[239] 'Google Spain',op. cit., para 28.
[240] Ibid.
[241] See Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy. Satamedia, C-73/07, EU:C:2008:727, paras 48-49.

noted that the processing operations undertaken by an online search engine include collecting, retrieving, indexing, storing, or disclosing the information in the search results.[242]

Nevertheless, although I just illustrated that the scope of the term processing is rather broad, it may be argued that there are highly exceptional instances in which even if the data are handled in some way, an operation may not fall within its scope. To be considered processing, the operation has to have a certain *purpose.*[243] Therefore, entirely purposeless operations arguably may not be considered processing under the GDPR.[244]

3.1.3 Personal data

GDPR protects only the information that fall under the definition of *personal data.* This term has been construed very broadly even under the Directive.[245] GDPR seemingly expands it, mainly by newly expressly stating that online identifiers (e.g. cookies, IP address) or location data also serve as possible identifiers of a person.[246] However, as we will see, given the construction of the term in the case law of CJEU, the definition in the GDPR cannot be seen as a clear expansion of the meaning of the term.[247] GDPR lays down a definition of personal data as follows: *"personal data means any information relating to an identified or identifiable natural person ('data subject')"*[248].

A natural person is *identifiable,* if he or she can be *directly or indirectly* identified using an identifier.[249] An *identifier* is a piece of information which makes it possible that at least one of the factors specific to an identity of a particular natural person, such as their physical, genetic, social or other identity, can be sufficiently closely linked to that person.[250] The GDPR provides a non-exhaustive list of identifiers. These are a name, an identification number, location data and an online identifier.[251]

In its opinion on the concept of personal data,[252] WP29 analyzed the definition of personal data based on four elements that it marked out as main building blocks. I will refer to them for guidance, use WP29's reasoning, and reference case law of the CJEU.

[1] Any information.

The use of the word *any* itself implies that the term needs to be construed broadly.[253] It does not matter whether it is an objective fact (e.g. date of birth) or a subjective evaluation (e.g. a person is

[242] 'Google Spain',op. cit., para 28.
[243] Article 4 (7), GDPR.
[244] NULÍČEK et al., 'GDPR', op. cit., pp. 85-86.
[245] Article 2 (a), Directive see also 'Rijkeboer', op. cit., para 59.
[246] Article 4 (1), GDPR.
[247] NULÍČEK et al., 'GDPR', op. cit., p. 77.
[248] Article 4 (1), GDPR.
[249] Ibid.
[250] Ibid.
[251] Ibid.
[252] WP29 Opinion 4/2007 on the concept of personal data (WP136), adopted on 20 June 2007.
[253] Ibid, p. 6.

reliable as a borrower) to be considered personal data. Furthermore, such information does not even have to be true. In that case, data protection law takes that into consideration and provides appropriate remedies such as the right to rectification.[254] Also, information can be available in whatever format to constitute personal data, including a binary code in a computer memory, a sound, or an image.[255] Moreover, if the processing is done at least partly by automated means, it is not necessary that the data are in a structured file, e.g. an email usually contains personal data.[256]

As far as the content of personal data is concerned, the extent of the impact of the processing on the rights of the data subject differs. A special category of information that is especially significant is recognized under the GDPR. Though the term is not used by the Regulation, they are commonly referred to in practice as *sensitive personal data*[257] and enjoy enhanced protection[258] – such information are data revealing *racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade and union membership;* data concerning *health, sex life or sexual orientation* and *genetic and biometric data*[259] processed for the purpose of identification (Article 9(1)). Another separate category that also attracts a higher level of protection, under different conditions, is personal data relating to criminal convictions and offences.[260]

[2] Information relating to.

Information will generally *relate to* a natural person, if it is *about that person*. If it is *about an object,* a process or events, it can relate to a natural person indirectly, based on the context and specifics of the case. According to WP29, value of a house as an information about an object can be considered personal data relating to its owner, if it is used to determine the high of tax payments owned by that individual.[261] Along those lines, if the information is about an object, it shall relate to an individual if its *purpose* is to evaluate or treat the person in a specific way or if its use is likely to have an impact on the rights of an individual.[262] Furthermore, an information may be considered to be related to a natural person, if its use *results* in an impact on the person's rights and freedoms, even if as a side-effect. WP29 provides an example of monitoring of taxi positions to optimize efficiency of the service, which may nevertheless also impact the drivers.[263]

[254] Note that personal data shall be accurate according to the principle of accuracy (Article 5 (1) (d) GDPR). Inaccuracy of processing personal data entails consequences.
[255] WP 29, 'On personal data', op. cit., p. 7.
[256] Ibid, p. 8.
[257] NULÍČEK et al., 'GDPR', op. cit., p. 162.
[258] Article 9, GDPR.
[259] Genetic and biometric data were not explicitly included in a category requiring enhanced protection under Directive. In the GDPR, they are defined in Article 4 (13), (14), GDPR.
[260] Article 10, GDPR.
[261] WP 29, 'On personal data', op. cit., pp. 9-11.
[262] Ibid.
[263] Ibid, p. 11.

What information can be considered personal data and under what circumstances, is constantly being addressed by CJEU. Most recently, in *Peter Nowak*[264] the Court dealt with a question referred to it by the Irish Supreme Court, whether *an answer given by a candidate that is contained in an exam script* constitutes his or her personal data and whether *the comments that an examiner writes* alongside these answers, can be considered personal data of the candidate. On the facts of the case, Mr Nowak was a trainee accountant. He failed a professional examination four times and challenged the results of his last attempt. His complaint was denied, so he submitted a request to access the examination script on the grounds that he had the right to access *his personal data processed.* However, the examination board refused that request as well, claiming that examination script does not contain such information. Mr Nowak challenged that decision. Ultimately, the Supreme Court referred a question concerning whether the information in question are personal data to CJEU.[265] The Court held that *both of the answers and the comments shall be consid-considered personal data* of the candidate, *since they reflected knowledge and competence in a given field* of a particular natural person *and were used for the purpose of evaluation* of the candidate, having profound impact on his or her rights and thus were considered 'relating to' an identifiable natural person.[266] The right to rectification and access, in this sense, could be used to review whether the results were attributed to a correct individual, but could of course not be used to change an answer.[267] The judgment can have interesting side implications in the future,[268] since under the GDPR, no fees can be charged for the exercise of the right to access personal data. Currently, in many instances, exam boards do charge for such a service.[269]

Earlier in *Schecke*, CJEU held that a requirement of publication of informotion relating to the beneficiaries od European agricultural funds (their names and amount of aids they received) is a disproportianate measure concerning their personal data.[270] Personal data relating to natural persons can therefore include information about the professional or business activities of natural persons.[271]

[3] Identified and directly or indirectly identifiable natural person.

A person is identified if he or she is distinguished from a group of people using one or several pieces of information.[272] An identifiable person is such that has not been identified but can be.

---

[264] Peter Nowak v Data Protection Commissioner, Case C-434/16, EU:C:2017:994.

[265] Ibid, para 18-26.

[266] Ibid, para 32, 36-39.

[267] Ibid, para 56-57.

[268] ORME, Joe. ECJ determines that exam scripts and examiner comments are personal data [online]. 21 December 2017. Available at: <https://www.lexology.com/library/detail.aspx?g=41928c90-2435-403d-9c04-e04d8b051e28>. Last accessed 1 April 2018.

[269] E.g. British Council makes results of its test available only in form of a score. If a candidate feels that his or her result is incorrect, they can request an enquiry on results, subject to a fee. See: <https://bit.ly/2vh3sz5>. Last accessed 1 April 2018.

[270] 'Schecke', op. cit., para 59.

[271] For discussion on contradicting case law of the Czech Constitutional Court – Nález Ústavního soudu ze dne 9. Března 2004, sp.zn. Pl. ÚS 38/02, see NULÍČEK et al., 'GDPR', op. cit., p. 81.

[272] RÜCKER, In: 'New European General Data Protection Regulation', op. cit., rec. 83.

Either directly, based only on information available to a person who identifies the data subject without the need to cooperate with others, or indirectly, if additional information is needed from another person.[273]

A natural person might be directly identifiable if a name as an identifier is available. However, identifiers cannot be divided into categories routinely. For example, if knowing a name will even be sufficient for identification depends on the context. Some family names are so common that they do not allow for identification. Nevertheless, they can be able to distinguish a person in some circumstances, for example from a group of people in his or her class at school, but not in the context of the whole city. Another example provided by the WP29 concerns *digital images displaying persons.* If they contain clearly visible faces, they would allow for identification and be considered personal data. However, if there are scenes on the photo, portraying individuals from a distance they usually will not be considered personal data, unless the existence of such an image implies a relationship between the individuals.[274] Therefore, circumstances of an individual case have to be always taken into account.

In case that additional information of some sort is needed, such information can be publicly available, in possession of a third party,[275] or in possession of the processor or the controller themselves. In case of indirect identifiability, the question is who has to be able to identify the person. The threshold is that the *means* available have to be *reasonably likely to be used* to acquire the additional information needed in order to determine identifiability.[276] It has been discussed under the regime of the Directive, whether criteria to establish reasonable likeliness should be considered relative or absolute. If the criteria were absolute, piece of information would fall under the definition of personal data if *anyone* would be able to possibly connect the data to a particular person. The GDPR itself does not expressly provide a clear answer.[277] CJEU held in *Breyer* that the information in question constituted personal data *in relation to* a provider,[278] suggesting that the efforts needed for someone to identify a person based on additional information are disproportionate. Nulíček and collective argue that the information shall then be considered personal data for anyone who holds it, given that person shall presume that identification is not only hypothetical.[279] They argue that this interpretation is obvious, and an opposite conclusion would hinder effective protection of personal data.[280]

In terms of the determination of the means that can be used and whether they are reasonably likely to be used for identification, anonymisation, and pseudonymisation techniques of the

[273] NULÍČEK et al., 'GDPR', op. cit., p. 79.

[274] WP29 Opinion 02/2012 on facial recognition in online and mobile services (WP192), adopted on 22 March 2012, p. 5.

[275] Confirmed in Patrick Breyer v Bundesrepublik Deutschland, C-582/14, EU:C:2016:779, see paras 44 and 49.

[276] Recital 26, GDPR and WP 29, 'On personal data', op. cit., pp. 13-15.

[277] RÜCKER, In: 'New European General Data Protection Regulation', op. cit., rec. 90-91.

[278] 'Breyer', op. cit., para 49.

[279] NULÍČEK et al., 'GDPR', op. cit., p. 80.

[280] Ibid.

data and related risks of re-identification play an important role in cloud computing. I will discuss them in detail in chapter 4.

[4] Natural persons.
In order to be considered personal data, [281] the information has to relate to a *living* human being regardless of his or her nationality or residency.[282] Such persons are called data subjects.[283] Information about the deceased or relating to legal entities are not protected under the GDPR, though Member States are allowed to provide for data processing rules that would apply to them.[284] Moreover, information about the deceased person can be sometimes personal data in relation to heirs or persons living with the deceased before his death. An example concerns hereditary illness or a transmissible disease.[285]

As far as legal persons are concerned, the CJEU held in *Schecke* that they can claim protection under Articles 7 and 8 of the Charter, if the *official title of the legal person identifies a natural person.* In that case, the title of the partnership revealed who were the partners.[286] WP29 also noted on that account that information related to legal persons do not fall within the scope of the Directive *in principle,* but may under certain circumstances, when they may identify an individual.[287]

3.1.4 Territorial scope

Unlike the previous provision on material scope, the determination of the territorial scope has undergone substantial changes compared to the regime under the Directive and strives to react to the reality of the digital age. Territorial scope of the GDPR is designed to be extremely broad, attempting to enhance protection of data subjects' rights, and as such has been subject to heated discussions. Under the GDPR, as far as its territorial scope is concerned, there are three instances, in which it applies.

[1] An establishment in the Union.[288]
GDPR applies to the processing of personal data undertaken in the context of activities of an establishment (of a controller or a processor) in the Union. Unlike under the Directive, in these circumstances, it does not matter, whether the processing itself takes place in the EU or not. If it

[281] Recital 27, GDPR.
[282] WP 29, 'On personal data', op. cit., p. 21.
[283] Article 4 (1), GDPR.
[284] Recital 27, GDPR.
[285] VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 11.
[286] 'Schecke', op. cit., para 53.
[287] 'WP 29, 'On personal data', op. cit., p. 23.
[288] Article 3 (1), GDPR.

is carried out in the context of an establishment of a processor or a controller in the EU, GDPR applies.[289]

Both 'the connection to the activities of an establishment' and the term 'establishment' itself, need to be construed broadly in line with the case law of CJEU. Most recently in *Weltimmo,*[290] CJEU considered the construction of these terms, when assessing applicability of national law and the reach of the national data protection authority under the Directive. Weltimmo, a company with its registered office in Slovakia, runs a website dealing with properties in Hungary. The processing that took place concerned the personal data of the advertisers. The advertisements were free of charge during the first month, but incurred a fee payable starting from the second month. A lot of advertisers enjoyed the first month of free service, and then requested deletion of their advertisements as well as personal data. Weltimmo did not do that and required payment for the advertising. When advertisers refused to pay, Weltimmo proceeded to debt collection agencies. Advertisers filed complaint with the Hungarian data protection authority. Weltimmo claimed that the case should have been handed over to the Slovakian data protection authority. However, its Hungarian counterpart argued it had jurisdiction and imposed a substantial fine on Weltimmo. The company brought an action before 'Budapest administrative and labor court', which upheld the view of the Hungarian data protection authority on the point of its jurisdiction, pointing out deficiency in terms of the finding of facts. Weltimmo appealed. The Court first pointed out some of the information submitted by the Hungarian data protection authority. Weltimmo did not carry out any activity in Slovakia. The website was developed exclusively for the Hungarian market and all in Hungarian language. Furthermore, Weltimmo opened *a bank account in Hungary and had a letter box in Hungary,* from which the post was regularly resent to it.[291] Servers used by Weltimmo were said to be either in Austria, Slovakia, or Germany.[292] In short, the question then was, where was Weltimmo established and therefore whether its processing was 'in the context of activities of an establishment'. The Court emphasized that the concept needed to be construed broadly to ensure adequate protection of the right to personal data protection as a fundamental right, referring to Google Spain,[293] and stating that the territorial scope of the Directive is prescribed broadly.[294] 'Establishment' implied 'real and effective exercise of activity' based on stable arrangements. Legal form, including a formal presence of branch, was indecisive.[295] *Establishment* needs to be seen as a flexible concept. The effective exercise of an activity through stable arrangements have to be analyzed on a case-by-case basis, taking into account the specific of a particular activity, especially if the activity is carried out over the

[289] Ibid.

[290] Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, EU:C:2015:639.

[291] Ibid, para 16.

[292] Ibid, para 18.

[293] Ibid, para 25.

[294] Ibid, para 27.

[295] Ibid, para 28. Note that establishment in several Member States meant the obligation to comply with national laws applicable in each of the Member States under the Directive.

internet only. A presence of one representative in the Member State can be enough. Weltimmo had one in Hungary. The activity carried out can be minimal, if it is based on stable arrangements.[296] Consequently, CJEU held that Weltimmo was established in Hungary as well as in Slovakia and then proceeded to the interpretation of the processing carried out 'in the context of activities of an establishment'. Referring to Google Spain[297] again, the Court explained that the processing does not have to be undertaken 'by' the establishment itself, and that the concept is rather broader. The economic activity was an advertising of Hungarian properties on a website *in Hungarian language,* using *a Hungarian bank account* and the processing undertaken was uploading personal data on that website. There was no doubt it was done 'in the context of activities of an establishment' in Hungary and Hungarian law applied as a result.[298]

Some of the aspects of *Weltimmo* are expressly dealt with in Recital 22, which in summary requires an assessment based on real and effective exercise of an activity, stable arrangments and deems missing establishment of a branch in the EU as irrelevant. At the same time, the GDPR defines the concept of a main establishment,[299] taking into account that there may be multiple. However, it does not have to be in the EU.[300]

[2] Personal data of data subjects who are in the Union.[301]
With regard to the territorial scope, GDPR also applies to the processing of personal data of data subjects who *are in the EU*, by a controller or processor, which is *not* established in the EU, if the processing activities are related to:

> [a] the offering of goods or services to such data subjects in the EU;
> or
> [b] the monitoring of their behavior as far as their behavior takes places within the EU.

What constitutes *offering of goods or services* to data subjects who are in the EU needs to be determined according to factors of a specific case. First, it has to be assessed whether it is apparent that the controller or processor *envisages* offering goods or services in the EU. For example, the use of a language or a currency of a Member State can prove such an intention.[302] One the other hand, *mere accessibility of a website* in a Member State or the use of a language that is used also in the State where the processor or controller is established, are generally insufficient.[303] Other factors to consider may be derived from case law on consumer contracts and include mentioning

[296] Ibid, paras 29-31, 33.
[297] 'Google Spain', op. cit., para 48.
[298] 'Weltimmo', op. cit., paras 32 and 37-39.
[299] Article 4 (16), GDPR, plays role with respect to the determination of a lead authority.
[300] SCHUMACHER, In: 'New European General Data Protection Regulation', op. cit., rec. 190.
[301] Article 3 (2), GDPR.
[302] Recital 23, GDPR.
[303] Ibid.

phone numbers with an international code, use of a domain '.eu' or a domain of the Member State or mention of an clientele from various Member States.[304] In any instance, it is irrelevant, whether a payment is required for such goods or services or not.[305]

This regime is newly introduced by the GDPR and strives to ensure adequate protection of EU-consumers as well as fair conditions for businesses competing for customers in the EU.[306] Under the Directive, the approach to take into account on which customers the services are directed was outlined in *Google Spain,* where the Court noted that the processing is deemed carried out in the activities of an establishment of the controller in the EU, even when a subsidiary of the operator in the EU promotes the services towards *the inhabitants* of EU Member State.[307]

Monitoring of the behavior of data subjects who are in the EU, given that behavior takes place within the EU, is relevant mainly in the context of the internet (e.g. through social plugin 'like' buttons, cookies etc.).[308] The threshold is whether a natural person is tracked online, including profiling of a natural person.[309]

When are the data subjects considered to be *in the EU*? The wording of the provision seems rather ambiguous. In the original proposal of the GDPR submitted by the Commission, the processing concerned data subjects *residing in the Union*.[310] The lack of reference to nationality or residence may imply the intention of the legislator that GDPR shall simply apply to any data subjects, who are, even if for a limited period of time, physically located within the EU.[311] GDPR will therefore apply if, for example, when the offering of a service is *intentionally targeted* at clients who are in the EU. These clients do not have to be EU citizens or stay in the EU for a substantial period of time. Whenever will a US citizen travel to a Member State, his or her personal data shall be treated and protected under GDPR. Even if he or she uses an online service, provided by a US company, but logging in through the version of the service envisaged by the provider, to be used within EU. On the contrary, European citizens might not enjoy the protection under GDPR, if they travel to a third-country.[312]

[3] Application by virtue of public international law.

---

[304] Peter Pammer v Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmbH v Oliver Heller, joint cases C-585/08 and C-144/09, EU:C:2010:740, para 93.
[305] Article 3 (2) (a), GDPR.
[306] SCHUMACHER, In: 'New European General Data Protection Regulation', op. cit., rec. 194.
[307] 'Google Spain', op. cit., para 60.
[308] SCHUMACHER, In: 'New European General Data Protection Regulation', op. cit., rec. 201-202.
[309] Recital 24, GDPR.
[310] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final. Article 3 (2).
[311] NULÍČEK et al., 'GDPR', op. cit., p. 72.
[312] Ibid.

Lastly, GDPR applies to the processing of personal data by a controller that is not established in the EU, but in a place where the law of a Member State applies due to public international law. This is going to be the case if the processing takes place in Member State's diplomatic mission or a consular post.[313]

3.1.5 Personal scope

As regards personal scope of the GDPR, it applies to anyone that is *processing* or *controlling the processing* undertaken on personal data. The law distinguishes between a controller and a processor, whose rights and responsibilities vary. Their relationship changes substantially with the GDPR, but the defintions remain as established under the Directive.[314]

A controller is any "natural or legal person or a public authority or an agency or a body, which alone or with others, determines: [1] the purposes and [2] the means of the processing of personal data."[315]

It is the controller who has the main responsibility for the compliance under the GDPR.[316] A controller can undertake the processing of personal data on its own (e.g. through its employees), but it can as well instead authorize a processor to do all or part of the processing on its behalf.[317] Just as a controller, a processor can either be a natural person or a legal person, public authority, agency, or body. There always has to be a controller, if the processing of personal data takes place. Whether there is also a processor depends on the decision made by a controller (unless the processer is determined by law[318]). In any case, the processor has to be external,[319] an entity other than a controller, and process personal data on controller's behalf.[320]

Stipulation of who determines the purposes and means may be provided by law of the EU or a Member State. In such a case, who is a controller might be provided by law.[321] In all the other instances, who is a controller needs to be assessed on a case-by case basis by parties involved and as I will show in the next chapter, is not an easy exercise in cloud computing.

The assessment has to take into regard the *specific data and particular distinguishable operations.* The same person can act as a processor in certain processing operations, and at the same time as a controller in other.[322] 'On behalf' in the definition of a processor means that the processor is *mandated and instructed* by a controller. If it processes the data outside of the scope of the instructions with regard to the purpose of the processing, it will become a controller with regard

[313] Recital 25, GDPR.
[314] RÜCKER, In: 'New European General Data Protection Regulation', op. cit., rec. 117.
[315] Article 4 (7), GDPR.
[316] RÜCKER, In: 'New European General Data Protection Regulation', op. cit., rec. 120.
[317] Article 4 (8), GDPR.
[318] Article 28 (3), GDPR.
[319] WP29, 'On the concepts of "controller" and "processor"', op. cit.
[320] Article 4 (7), GDPR.
[321] Ibid.
[322] WP29, 'On the concepts of "controller" and "processor"', op. cit., p. 25.

to such operations,[323] however, this does not apply with regard to the means. Thus, an emphasis is put on 'instructions' under the GDPR and the concept is criticized in a cloud computing context as we will see.

In a simplified way, a controller is the one who initiates the processing, decides to carry out activities and needs to process personal data in their context.[324] He possesses the *main decision-making power,* determining which data are processed, why, and how.[325] Decisive for a person to qualify as a controller is the 'why' of the processing – its anticipated outcome (e.g. marketing, provision of services, protection of property etc.). The decision concerning the purpose shall be *reserved to the controller.* In other words, whoever determines the purpose, is always a controller.[326] Under the Directive, the possibility of cases where more than one controller would occur was mentioned in a definition of a controller itself, but other than that, the allocation of responsibilities in such situations was not provided for,[327] which was problematic. GDPR strives to tackle this issue and obliges the so-called joint-controllers to transparently determine their responsibilities and obligations towards the data subjects in form of an agreement, while stipulating in detail further requirement.[328]

The level of detail needed in determining the *means* is a more difficult question. The influence a person has to have over the choice of the means of processing can vary in different contexts. Means include, according to the opinion of the WP29, both *technical and organizational questions* and the decision concerning them may be delegated to a certain extent. But the 'essential elements' concerning lawfulness of the processing shall be recognized based on the context of a particular case and over these the controller should have absolute decision-making power.[329] Consequently, if a processor determines less important aspects of the means of the processing, in a way that is reasonable with regard to the purposes of the processing, this would not change his role and trigger control. The effect could be at worst violation of contractual obligations.[330] But then again, this depends on the specifics of an individual case and what constitutes essential elemenets regarding the means of the processing remains unclear. WP29 provides examples, allowing processors to choose a hardware or software to be used, which are not regarded as essential elemenets of the processing and putting in contrast the question of how long the data should be processed, which it sees as essential and therefore reserved to the controller.[331]

---

[323] Article 28 (10), GDPR.
[324] NULÍČEK et al., 'GDPR', op. cit., page 89.
[325] VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 19.
[326] WP29, 'On the concepts of "controller" and "processor"', op. cit., p. 13.
[327] Article 2 (d), Directive.
[328] If these are not determined by law – Article 26, GDPR.
[329] WP29, 'On the concepts of "controller" and "processor"', op. cit., p. 14.
[330] Ibid.
[331] Ibid.

Processing can as well be multi-layered. A processor can engage a sub-processor, who has to, nevertheless, also abide by the instructions given by the controller. Such structures occur increasingly in cloud computing environment and I consider them in the fourth chapter.

3.2 Lawful processing

3.2.1 Principles relating to the processing of personal data

Fundamental principles of the data processing are set out in Article 5 of the GDPR and realized further by various other provisions. However, as any legal principles, they shall serve the purpose of guidance in interpretation of the Regulation as a whole and deserve special attention.[332] Compared to the regime under the Directive, heavy emphasis is newly put on transparency,[333] which has not been previously expressly included in the list of principles.[334]

Newly introduced is a principle of accountability, standing separately from the list of others in the second paragraph of Article 5, holding a prominent role, serving the purpose of enforceability of other principles.[335] In terms of the GDPR, accountability means that the controller shall *"be responsible for, and able to demonstrate compliance."* The Directive only required that the controller ensured compliance.[336] The GDPR therefore requires in many cases proactivity on the controller's side,[337] encouraging implementation of effective safeguards for the protection of personal data[338] and comprehensive documentation of compliance.[339]

The principle of lawfulness, fairness and transparency requires that personal data shall be processed lawfully, fairly, and in a manner transparent *to the data subject*.[340] Guidance is given by Recital 40, which equates lawfulness with the fact that legal basis for the processing has to be present. The term *fairness* does not seem to have an independent meaning under the GDPR, since Recitals 60 a 71 read it jointly with transparency. This also seems to be confirmed by Recital 38 of the Directive, which requires giving the data subject a chance to learn about the processing for the processing to be considered fair. However, this does not mean that the notion of fairness may not gain clearer counters and independent standing once GDPR is applied. Transparency is realized mainly through the right of the data subjects to be informed, set out in detail in Articles 12-14 together with the requirements for the communication with the data subjects.

---

[332] VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 87.
[333] NULÍČEK et al., 'GDPR', op. cit., p. 105.
[334] Article 6, Directive.
[335] DIENST, In: 'New European General Data Protection Regulation', op. cit., rec. 351.
[336] Article 6 (2) Directive.
[337] NULÍČEK et al., 'GDPR', op. cit., p. 119.
[338] WP29 Opinion 3/2010 on the principle of accountability (WP 173), adopted on 13 July 2010, p. 3.
[339] DIENST, In: 'New European General Data Protection Regulation', op. cit., rec. 356.
[340] Article 5 (1) (a), GDPR.

The principle of purpose limitation has two elements.[341] Firstly, the personal data shall be *collected* only for *specified, explicit and legitimate purposes.* Secondly, further processing after the collection is possible only if done in a manner compatible with those initial purposes.[342] The wording is almost the same as the one in the Directive,[343] which previously led to significant divergences in national implementations and application of different tests of incompatibility, specificity, and explicitness by national courts.[344] GDPR does not attempt to define any of the notions and what will be considered sufficiently specific shall be assessed based on the particularities of the case.[345] WP29 recommends that more detail shall be provided, where large number of data subjects is involved, or where the purpose is uncommon for the type of the processing operations employed.[346] The bottom line is that the purpose needs to be specific enough, so that it enables evaluation of its compliance with the GDPR.[347] Furthermore, it shall be noted that WP29 stated that delimitations like marketing purposes or IT security are usually not specific enough.[348] In terms of *explicitness,* the GDPR requires informing the data subjects about the purposes in Articles 13 and 14 and therefore has to comply with all the requirements on communication pursuant to Article 12. Lastly, WP29 suggests that the notion of *legitimacy* requires the purpose to be in accordance with the law *in its broadest sense* (i.e. jurisprudence, municipal decrees, or even Codes of Conduct).[349]

The second element concerns further processing, i.e. any processing after the collection of the data, most often storage of the data, which can be undertaken only in case of compatibility.[350] Firstly, there are exemptions from the compatibility test. Archiving in the public interest, scientific, historical research or statistical purposes are presumed compatible.[351] The compatibility test is also not required if the data subject gives consent or further processing is based on an EU or a Member State law which constitutes a necessary and proportionate measure that safeguards one of the objectives enumerated in Article 23.[352] In all other cases, *compatibility test* has to be conducted. Compatibility will be rather obvious if there is no change in purposes.[353] If there is a change in purposes, GDPR provides a non-exhaustive list of criteria that shall be taken into account. These

---

[341] DIENST, In: 'New European General Data Protection Regulation', op. cit., rec. 261.
[342] Article 5 (1) (b), GDPR. Archiving purposes in the public interest, scientic and historical research purposes or statistical purposes shall be considered compatible with initial purposes (Article 5 (1) (b)) or conditions of Article 6 (4) are met.
[343] Article 6 (1) (b), Directive.
[344] WP29 Opinion 03/2013 on purpose limitation (WP 203), adopted on 2 April 2013, pp. 5-10.
[345] Ibid, p. 16.
[346] Ibid, p. 20.
[347] Ibid, p. 16.
[348] Ibid.
[349] Ibid, p. 20.
[350] DIENST, In: 'New European General Data Protection Regulation', op. cit., rec. 283.
[351] Article 5 (1) (b), GDPR. Note that whether statistics and research in a commercial interest is covered is not a settled question. See DIENST, In: 'New European General Data Protection Regulation', op. cit., rec. 286-290.
[352] Article 6 (4), GDPR.
[353] WP29, 'On purpose limitation', p. 22.

include whether there is any *link* between the original and new purpose, what is the specific *context, nature* of the personal data processed, possible *impact* on the data subjects and the existence of *safeguards,* such as encryption and pseudonymisation.[354]

Closely connected to the purpose limitation is the principle of data minimisation, which requires that the personal data processed are *adequate, relevant and limited to what is necessary in relation to the purpose* of the processing.[355] Compared to the Directive which required the processing "not to be excessive" in relation to the purposes,[356] the GDPR presents a stricter requirement.[357] Recital 39 specifies that necessity requires that the data are processed only if the purpose of processing could not be *reasonably fulfilled by other means.* This notion requires further specification, either by the Board or CJEU in the future.[358] For compliance with data minimisation, important role play the concepts of data protection by design and by default and anonymisation and pseudonymisation, which I consider in the chapter on cloud computing challenges.

Storage limitation[359] obliges controllers to keep the personal data in a form, which permits identification only as long as is necessary for the purposes of the processing.[360] Recital 39 further states that time limits for erasure or for periodic review shall be established for compliance with this principle. Exceptions are provided for the data stored for archiving purposes in the public interest, scientific or historical research or statistical purposes,[361] subject to appropriate safeguards pursuant to Article 89 (1).

The principle of accuracy requires that the personal data processed are accurate and if necessary, *kept up to date*.[362] Inaccurate data must either be erased or rectified without delay. What constitutes inaccuracy is not entirely clear. The WP29 likens it to divergence from reality.[363] Along those lines, information that is based on subjective evaluation can hardly be objectively classified as factually correct.[364] It is not only in these cases when inaccuracy may be hard to determine. In case of storage as a processing operation, its purpose can be relevant, for example if old data are stored to provide a timeline of development.[365] Updating the data may also conflict with legal contractual documentation and archiving obligations.[366] Lastly, the GDPR does not

[354] Article 6 (4) (e), GDPR.
[355] Article 5 (1) (c), GDPR.
[356] Article 6 (1) (c), Directive.
[357] DIENST, In: 'New European General Data Protection Regulation', op. cit., rec. 316.
[358] Ibid, rec. 319.
[359] Article 5 (1) (e), GDPR.
[360] An exemption to this principle forms the storage solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
[361] Article 5 (1) (e), GDPR.
[362] Article 5 (1) (d), GDPR.
[363] DIENST, In: 'New European General Data Protection Regulation', op. cit., rec. 326.
[364] Ibid.
[365] Ibid, rec. 327.
[366] Ibid, rec. 332.

clearly require the controllers to periodically scan for inaccuracies and it is uncertain whether situations may arise when it would be deemed adequate.[367]

The principle of integrity and confidentiality is another principle, which was not expressly articulated in the Directive's list of principles. It requires that appropriate security is ensured in the course of the processing.[368] This obligation is detailed in Article 32, though leaves some leeway for diverse interpretation, since what is appropriate may be highly subjective. Acknowledgement of sector-specific standards is crucial in these terms.

In conclusion, it shall be pointed out that Article 83 (5) (a) allows for imposition of fines based solely on incompliance with the principles, without requiring breach of more specific provisions. Although the real impact of this provision in practice can hardly be predicted, the position of the principles seems to be strengthened by the GDPR.

3.2.2 Legal grounds for processing

For the processing of personal data to be lawful, at least one of the following legal grounds must apply:

[1] the data subject has given *consent;*
[2] there is contractual necessity;
[3] the processing is *necessary for compliance with a legal obligation* to which the controller is a subject*;*
[4] the processing is *necessary in order to protect vital interests* of the data subject or others;
[5] the processing is necessary for the performance of a task carried out in the public interest;
[6] the processing is *necessary for the purposes of the legitimate interests* pursued by the controller or a third party.[369]

The legal grounds are enumerated exhaustively, and the list is almost identical with the one in the Directive. But then again, that listing resulted in quite divergent national implementaions. For example, in the Czech law the consent was priviledged.[370] The same applied in France or Portugal. On the contrary, for example in Belgium, Denmark, or Finland, all the legal grounds were of equal footing.[371] The GDPR considers all the legal grounds for the processing as alternative and therefore equal.[372] Moreover, the requirements for consent are much stricter than under the Directive, thus the controllers will in practice always seek first, whether other legal

[367] Ibid, rec. 330-331.
[368] Article 5 (1) (f), GDPR.
[369] Article 6 (1) (a) – (f), GDPR.
[370] NULÍČEK et al., 'GDPR', op. cit., p. 124.
[371] European Commission. Commission Staff Working Paper. Impact Assessment. Brussels, 25. 1. 2012, SEC (2012) 72 final, Annex 2, p. 26.
[372] DIENST, In: 'New European General Data Protection Regulation', op. cit., rec. 362.

grounds under Article 6 apply to their processing.[373] I will now briefly consider the ones that are most relevant in the cloud computing context.

Consent is subject to stringent requirements. Main elements of a valid consent are set out in Article 4 (11), which defines it as *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".*

The requirement of a *statement or clear affirmative action* is newly added in the GDPR. This criterion excludes silence, pre-ticked boxes, inactivity, or any other passive behaviour from being considered sufficient.[374] Many SaaS cloud services will have to react accordingly. Valid consent needs to be *withdrawable* at any time, in a manner as easy as the one used when giving consent.[375] In terms of *unambiguity,* there should be no doubt that there was an intention to consent.[376] WP29 suggests that for the sake of unambiguity in the online context, the use of service and the user experience may *have to be* interrupted, so that the data subject truly actively consents and appeals to the service providers to find innovative ways how to tackle the problem, where the users simply "click" and do not read the content.[377]

Freely given means that the data subject must have a real, genuine choice. WP29 holds that consent is invalid, if it entails such negative consequences that the data subject is forced to consent. Consequently, it *shall not* be included in non-negotiable standard terms and conditions.[378] The same situation is likely to occur if there is clear imbalance of power.[379] What it means for B2C relationships or services in which large cloud service providers like Google or Amazon take part, where imbalance of powers is usually quite obvious, remains to be seen. Strict interpretation would render consent useless for many scenarios.[380]

Article 7 (4) sets a requirement of *unconditionality* for a consent to be considered freely given. This includes tying a provision of a service to consent to the processing of personal data that is *not strictly necessary* for the performance of the contract. Consequently, for example SaaS services cannot give a potential user a choice between consenting and not being able to use an app. WP29 makes it clear that there cannot be any detriment following the absence of consent. If lack of consent entailed further costs or decreased functionality, it may be considered invalid.[381]

---

[373] NULÍČEK et al., 'GDPR', op. cit., p. 124.
[374] DIENST, In: 'New European General Data Protection Regulation', op. cit., rec. 435.
[375] Article 7 (3), GDPR. WP29 states that withdrawal should not have any detrimental impact on the use of a service by the data subject and be free of charge. See WP29 Guidelines on Consent under Regulation 2016/679 (WP259), adopted on 28 November 2017, p. 21.
[376] Ibid, p. 16.
[377] Ibid, pp. 17-18.
[378] Ibid, p. 6.
[379] Recital 43, GDPR.
[380] DIENST, In: 'New European General Data Protection Regulation', op. cit., rec. 446.
[381] WP29, 'On consent', op. cit., p. 10 and Recital 42, GDPR.

Moreover, if the processing is undertaken for multiple purposes, the data subject shall be free to choose to consent just to one or some of them.[382] This condition of *granularity* is closely linked to the element of *specificity,* which requires that the consent is given for a specific purpose or purposes[383] and is clearly distinguishable from other matters, if included in a more complex written declaration.[384] Of utmost importance is also adherence to the principle of transparency, requiring consent to be presented in an *intelligible and accessible form, using clear and plain language.*[385] The consent will be *informed,* if sufficient information is provided *prior* to the processing. Recital 42 sets out their minimum content similarly to the right to be informed under Articles 13 and 14.

In some cases, the consent needs to be *explicit.* Such threshold is higher than the one of *clear affirmative action* applicable to "regular consents" and WP29 understands it as having the same meaning as express.[386] Explicit consent is required under Article 9 in case of processing of special categories of data, under certain circumstance when the data are transferred to third countries (Article 49) and in case of automated individual decision making (Article 22). WP29 suggests how explicit consent might be given and the examples include a written and signed statement or filling in an electronic form. Two-stage confirmation of consenting might as well be desirable.[387] Separate regulation under Article 8 applies to a child's consent in relation to information society services.

All in all, as just shown, relying on consent may be impractical. It can be easily withdrawn, the requirements for its validity are stringent and it might be difficult to sufficiently demonstrate that all its elements were adhered to. Thus, consent shall only be used in cases, where it is impossible to base the processing on other legal grounds.[388]

GDPR allows a *contract* to serve as a legal basis for the processing in two instances:
[1] if the processing is necessary for the *performance of a contract* already entered into and of which a data subject is a party, or
[2] in order to take steps *prior to entering into a contract, at the request* of the data subject.[389]

Performance of a contract shall be understood as covering any processing needed for the fulfilment of the obligations under the contract and taking place in the context of a contract.[390] WP29 states that what is necessary for the performance of a contract needs to be interpreted *strictly,* the link

[382] Recital 32, GDPR, this concept is known as granular consent.
[383] Article 6 (1) (a), GDPR.
[384] Article 7 (2), GDPR.
[385] Ibid.
[386] WP29 Opinion 15/2011 on the definition of consent (WP187), adopted 13 July 2011, p. 25.
[387] WP29, 'On consent', op. cit., p. 19.
[388] NULÍČEK et al., 'GDPR', op. cit., pp. 155-156.
[389] Article 6 (1) (b), GDPR.
[390] Recital 44, GDPR.

between the performance and processing must be objective.[391] Typically customer profiling would be beyond what is necessary, but reminders connected to the provision of a service may be justifiable.[392] As regards the taking steps for entry into the contract, the processing can only take place *upon request* of the data subject, addressed either to the controller or a third party authorized to arrange for the contract. Typical requests would demand more information about products and services, such as a price list.[393]

Another legal ground which may prove widely applicable in cloud computing is the *legitimate interest* pursued by the controller or a third party. If the controller wishes to base its processing on a legitimate interest, a complex balancing test needs to take place. WP29 breaks it down into three steps:

[1] consideration whether the interest pursued is *legitimate;*
[2] evaluation of the *necessity* of the processing;
[3] *weighting of the interests* of the controller and the interests of the data subject.[394]

The GDPR does not define the term legitimate interest, WP29 states that it is not a synonym with the purpose of the processing and concerns wider intentions of the controller, including any advantages that will result from the processing.[395] These must be generally acceptable under any applicable law to be legitimate.[396] Legitimacy of the interests needs to be assessed in the context of a particular activity, but includes a wide range of reasons, from not so pressing to compelling ones.

Some examples are provided for by the Recitals. Recital 47 lists as one of them direct marketing purposes, however, it is too soon to analyze under what circumstances this will be acceptable. Easier to accept are examples such as prevention of fraud,[397] ensuring network or service security in an online environment, including prevention of unauthorized access,[398] or typically right to freedom of expression and information.[399]

The balancing test which is requiring consideration of the rights and freedoms of the data subject currently differs significantly between Member States.[400] WP29 outlined the common positions in its opinion,[401] and put briefly, suggests to take into account the nature and source of

[391] WP29, 'On consent', op. cit., p. 9.
[392] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), adopted on 9 April 2014, p. 18.
[393] Ibid, p. 18.
[394] Ibid, p. 23.
[395] Ibid, p. 24.
[396] Ibid, p. 25.
[397] Recital 47, GDPR.
[398] Recital 49, GDPR.
[399] NULÍČEK et al., 'GDPR', op. cit., p. 134.
[400] DIENST, In: 'New European General Data Protection Regulation', op. cit., rec. 407.
[401] WP29, 'On the notion of legitimate interests', op. cit.

the legitimate interests as well as the impact on the data subjects. Above all, the risk of any possible negative consequences shall be carefully assessed, including likelihood of its occurance as well as the severity of the consequences.[402] These will usually be based predominantly on the nature of the personal data (i.e. if these are sensitive data) as well as the processing operation (e.g. if the information is publicly disclosed).[403] During the balancing test, the controller should take into account also any reasonable expectations of the data subject.[404] The controller may also implement further safeguards to strengthen appropriate balancing of the interests.[405] Children merit special protection[406] and specifics in other situations where there is imbalance of powers may also need to be considered.[407]

In addition to the requirements set out above, other more stringent conditions set out in Articles 9 and 10 apply to the processing of sensitive data and personal data relating to criminal convictions, which I will not explain further at this place, since I do not consider them essential for fundamental understanding of the GDPR.

3.3 Rights of the data subjects

GDPR generally strengthens the rights existing under the Directive and includes new ones, emerging as a reaction to case law and policy review. I will now briefly consider legal basis of rights to erasure, data portability, information obligations and transparency requirements on communication with the data subjects, which I analyze in the cloud computing context in the fourth chapter.

3.3.1 Transparency

The GDPR requires that any provision of information or communication with the data subjects in relation to their rights and data breaches is governed by the principle of transparency. This obligation is realized by Article 12, which provides quite detailed minimum requirements, apparently aiming to enforce the best practices, which are applicable regardless of the stage of the processing, technology used, or legal basis for it.[408] The communication or provision of the information must always:

[1] be concise, transparent, intelligible and easily accessible (Article 12 (1)),

---

[402] See DIENST, In: 'New European General Data Protection Regulation', op. cit., rec. 413-419.
[403] DIENST, In: 'New European General Data Protection Regulation', op. cit., rec. 407.
[404] Recital 47, GDPR.
[405] DIENST, In: 'New European General Data Protection Regulation', op. cit., rec. 407.
[405] WP29, 'On the notion of legitimate interests', op. cit., pp. 42-43.
[406] Article 6 (1) (f), GDPR.
[407] DIENST, In: 'New European General Data Protection Regulation', op. cit., rec. 407.
[407] WP29, 'On the notion of legitimate interests', op. cit., p. 40.
[408] WP29 Guidelines on transparency under Regulation 2016/679 (WP260), adopted, but still to be finalized, p. 6.

[2] use clear and plain language (Article 12 (1)),
[3] be generally provided in writing (Article 12 (1)),
[4] be free of charge (Article 12 (5)),
[5] be realized in a timely manner (Article 12 (3)).

The threshold is high. The controller should take into account that the information provided needs to be comprehensive, but at the same time readily understandable by the average data subject concerned. Consequently, the provision of information or communication should not impose a burden on the data subject by being too excessive.[409] In addition, in an online environment, it needs to be apparent where the information is to be found.[410] Furthermore, if the processing is targeted at children, the form of the communication needs to be adjusted to their level of understanding.[411]

WP29 explains that the requirement to use 'clear and plain language' means that the information should be provided in *"as simple a manner as possible"* and in a language that is *"concrete and definitive"*.[412] Therefore, the use of any ambivalent terms (such as may, some, often etc.), overly technical or legal terminology, should be avoided. By default, the information needs to be provided in writing or in an electronic form, especially if the personal data are processed electronically.[413] Only on the data subject's request can it be given orally.[414] WP29 sees as a crucial aspect that the method used reflects the whole context of the processing.[415]

Since the controller is generally obliged to facilitate the exercise of the data subject's rights, mechanisms implemented for the communication should allow for various ways of how the data subjects can lodge requests and as soon as they make a choice, the controller should respond using the same means.[416]

Furthermore, the information and any communication must be provided *free of charge,* unless the requests are *manifestly unfounded or excessive*.[417] In that case, it is at the controller's discretion[418] to choose to charge a reasonable fee or refuse to act on the request.[419] However, it is the controller who then bears the burden of proof that such measures were appropriate. Recital 63 states that repetitive requests may be excessive, but not if lodged in *"reasonable intervals"*. The provision shall be construed restrictively.[420]

---

[409] Ibid, p. 7.
[410] Ibid, p. 8.
[411] Recital 58, GDPR.
[412] WP29, 'Guidelines on transparency', op. cit., p. 9.
[413] Recital 59, GDPR.
[414] Article 12 (1), GDPR. E.g. because he or she is visually impared. WP29, 'Guidelines on transparency', p. 11.
[415] Ibid.
[416] Article 12 (2), (4), GDPR.
[417] Article 12 (5), GDPR.
[418] VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 148.
[419] Article 12 (5), GDPR.
[420] VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 148.

The controller cannot refuse to act upon the lodged request, unless the data subject cannot be sufficiently identified.[421] The GDPR emphasizes the need of identity verification in case of requests, again not previously addressed by the Directive. The controller is obliged to use all reasonable measures to verify the identity of the requesting data subject.[422] In the online context, the measures already in place include email verification or a code sent in a text message. GDPR also specifies that if the data controller does not possess enough information for the identification, the controller may request additional information.[423]

Importantly, any response to the data subjects' requests should be provided in a timely manner. Unlike the Directive, GDPR sets time limitations. It requires the controller to *inform* the data subject *about actions taken* without undue delay and in any event within one month of the receipt of the request.[424] WP29 recommends that the controllers specify their usual response time.[425] If the controller finds out that taking into account the complexity and number of requests, more time is necessarily needed, the time limitation can be extended by two months.[426] However, the controller needs to inform the data subject about the extension within one month of the receipt of the request at the latest anyway and it seems that in such a case, it is no longer possible not to take any action.[427]

In case of refusal to take any action, the controller shall inform the data subject also about the possibility to file complaint with a supervisory authority and seek judicial remedy.[428] Paal argues that information about the general existence of the remedies, without specifying the competent authority, is satisfactory.[429] However, WP29 seems to have a different opinion, requiring the controller to inform the data subject on how to determine competency.[430]

3.3.2 Right to provision of information

GDPR compared to the Directive substantially expands the list of the information that controllers have to provide to data subjects. It regulates this question based on whether the personal data are collected from the data subjects directly or not in two separate Articles.[431]

Firstly, in any case, the controller has to provide all the essential information about the processing, such as the identity of the controller, contact details, purpose of the processing, legal grounds for processing (and specific legitimate interests pursued, if applicable), recipients or *their*

[421] Article 12 (2), GDPR.
[422] Recital 64, GDPR.
[423] Article 12 (6), GDPR.
[424] Article 12 (3), GDPR.
[425] WP29, 'Guidelines on transparency', op. cit., p. 14.
[426] Article 12 (3), GDPR.
[427] Article 12 (3) read together with (4), GDPR.
[428] Article 12 (4), GDPR.
[429] PAAL, In: Datenschutz-Grundverordnung. Beck'sche Kompakt-Kommentare. Mu̇nchen 2017. PAAL, Boris P., PAULY, Daniel A. (Eds.), Article 12, rec. 60.
[430] WP29, 'Guidelines on transparency', op. cit., pp. 34-35.
[431] Articles 13 and 14, GDPR.

categories and if applicable also intended transfers to a third country, together with the information if it is based on an adequacy decision or another safeguard.[432] Further information to be communicated are the period for which the data will be stored or how it will be determined, which right does the data subject have under the GDPR, including the steps that the data subject needa to take to exercise them and explanation of their differences,[433] the existence of automated decision-making including profiling and its consequences,[434] or intended further processing for a purpose other than for which the data were collected.[435] WP29 clearly states that *"there is no difference between the status of the information provided under sub-article 1 and 2 […], [a]ll the information across these sub-articles is of equal importance and must be provided to the data subject."*[436] In any case, the takeaway for the data subject should always be a solid understanding of the scope and the consequences of the processing.[437]

In case of direct receipt from the data subject, the controller has to inform also whether the provision of information is a statutory or contractual requirement and consequences of failure to do so.[438] In case the data are received from a third party, the controller shall inform the data subject also from which source they originated and if they were received from publicly accessible sources.[439] Recital 61 allows for the provision of a general information for example if the data come from a publicly accesible online source.

In terms of when the information is to be communicated, in case of direct collection, it must be *at the time when personal data are obtained*.[440] If the data are received from third persons, the information has to be provided *within a reasonable time after the data are obtained*. What is considered 'reasonable' is to be determined on a case-by-case basis, with regard to circumstances of the processing, but the ceiling is a one-month time.[441] If the data are to be used for the communication with the data subject, it has to be at the time of the first communication at the latest and if disclosure to another recipient is envisaged, at the time of the disclosure at the latest.[442]

The controller is never obliged to provide the information, if the data subject already has it.[443] This will be the case with annexes to a contract, but not where the information itself is provided by a legal act.[444] Also, if the personal data have not been obtained directly from the data

[432] Articles 13 (1) and 14 (1), GDPR.
[433] WP29, 'Guidelines on transparency', op. cit., p. 34.
[434] Article 13 (2), Article 14 (2), GDPR.
[435] Article 13 (3), Article 14 (4), GDPR.
[436] WP29, 'Guidelines on transparency', op. cit., p. 12.
[437] Ibid, p. 8.
[438] Article 13 (2) (e), GDPR.
[439] Article 14 (2) (f), GDPR.
[440] Article 13 (1), GDPR.
[441] Article 14 (3) (a), GDPR.
[442] Article 14 (3) (b), (c), GDPR.
[443] Article 13 (4), Article 14 (5) (a), GDPR.
[444] NULÍČEK et al., 'GDPR', op. cit., p. 195.

subject, the controller is exempt from the obligation to inform, if it proves impossible or would involve a disproportionate effort.[445]

3.3.3 Right to erasure

Right to erasure is one of the most discussed rights under the GDPR and encompasses the so-called "*right to be forgotten",*[446] which emerged under the regime of the Directive in the case law of CJEU through interpretation of the right to rectification, erasure or blocking under Article 12 of the Directive and the right to object under Article 14 of the Directive.

In *Google Spain*, CJEU accepted that these provisions extended to the data subject's right to require the operator of a search engine to remove from the list of results a link to information lawfully published on a website by a third party, which contained true information relating to the data subject, if they appeared *"inadequate, irrelevant or no longer relevant"*[447]. CJEU further explained that even if the processing was initially lawful, it may later become excessive, especially if the information are not kept up to date and are no longer necessary for the purpose of the processing.[448] The Court did not explicitly state that such right exists but rather construed the existing rights in a broad manner, amounting to a form of 'the right to be forgotten'.[449] CJEU demonstrated a balancing test, where it stated that the data subject's rights to data protection and privacy, as fundamental rights, override, *as a rule,* the economic interests of the operator of the search engine, as well as the interest of the public in freedom of information.[450] This would not be the case – for example – if the data subject played an important role in public life.[451] In this particular case, Mr Gonzales's interests on the removal of outdated information about his social security debts, which were long resolved,[452] overrode Google's economic interests as well as the interest in freedom of information.[453]

In the GDPR, the essential features of the *right to be forgotten* were codified, but it goes beyond *Google Spain* and construes the right to erasure with the right to be forgotten *stricto sensu* as its consequence, in more detail.

Right to erasure, as stipulated in Article 17 of the GDPR, gives the data subject right to request erasure of personal data, provided that:

> [1] the personal data concern him or her;

---

[445] Article 14 (5) (b), GDPR.
[446] GDPR itself puts 'right to be forgotten' in brackets in the title of the right to erasure.
[447] 'Google Spain', op. cit., para 93.
[448] Ibid, para 94.
[449] PEERS, Steve. The CJEU's Google Spain judgment: failing to balance privacy and freedom of expression [online]. 13 May 2014. Available at: <http://eulawanalysis.blogspot.cz/2014/05/the-cjeus-google-spain-judgment-failing.html>. Last accessed 3 March 2018.
[450] 'Google Spain', op. cit., para 97.
[451] Ibid.
[452] Para 15.
[453] Para 98.

[2] any of the enumerated grounds apply;
[3] none of the exemptions apply.

The controller is then *obliged to erase* the personal data. The data subject has to prove his or her right to erasure, referring to one of the following *grounds*:[454] the personal data are no longer necessary for the purpose for which they were collected; the data subject withdraws consent and there are no other legal grounds for processing; the data subject objects to the processing and there are no overriding legitimate grounds, given that they are needed;[455] the processing is unlawful; the personal data have to be erased under legal obligation imposed by EU or a Member State law; the personal data have been collected in relation to the offer of information society services to children under Article 8 (1) of the GDPR. It shall be noted that in most of these cases, the controller is obliged to erase the data under GDPR regardless if requested under the principles of data protection set out in Article 5.[456]

The right to erasure *does not apply if* the processing is necessary for:[457] exercising the right of freedom of expression and information; for compliance with a legal obligation under EU or Member State law; for reasons of public interest in the area of public health; for archiving purposes in the public interest, scientific or historic research purposes, as far as erasure would likely render impossible or seriously impair the achievement of the objectives of the processing; for the establishment or exercise or defense of legal claims.

As regards the balance with the right to freedom of expression and information, the exemption will apply mostly to journalism. In *Satamedia,* CJEU perceived as a journalist a company, which sent out text messages about tax information, taking a rather broad view. But on the contrary the Court did not regard Google as a search engine as a journalist in *Google Spain*. Based on common construction of the term, bloggers expressing themselves in social media shall also be regarded as journalists, although they are not professionals.[458] Another applicable case law of CJEU in this context states that the accessibility of personal data in public registers is in the public interest and that information therefore cannot be removed upon request.[459]

If the controller refuses to erase the personal data based on one of the exemptions above, it needs to inform the data subject that the data will not be erased and that he or she can take further actions under Articles 77 and 79. The law requires this information to be provided within one month after the request was lodged.[460]

---

[454] Article 17 (1) (a-f), GDPR.
[455] Erasure has to be automatic under Article 21 (2), GDPR.
[456] NULÍČEK et al., 'GDPR', op. cit., p. 210.
[457] Article 17 (3) (a-e), GDPR.
[458] PEERS, Steve. 'The Right to be Forgotten': The future EU legislation takes shape [online]. 23 September 2014. Available at: <http://eulawanalysis.blogspot.cz/search?q=right+to+erasure>. Last accessed 3 March 2018.
[459] Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni, C-398/15, EU:C:2017:197.
[460] Article 12, GDPR.

The scope of the obligation to erase is influenced by the requirement that *if the controller made the data public,* it shall take reasonable steps to *inform controllers* who are processing the same personal data, that the data subject requested erasure of any links to, copies or replications of the personal data.[461] It is unclear what constitutes *reasonable steps*. The Regulation states that available technology as well as costs, shall be taken into account. There have been discussions whether the criteria are subjective or objective, which to date remain unresolved. [462] In terms of how the controller informs others, using inappropriate means can attract 'Streisand effect',[463] whereby the unintended consequence may be drawing further attention to the information in question. In any case, on the proper reading of the Regulation, the controller who is dealing with the request for erasure is not obliged to ensure erasure by other controllers, but merely to inform them, as other controllers may as well have their own legitimate grounds for the processing.[464]

Pursuant to Article 19, the controller is also subject to *notification obligation* regarding any rectification, erasure or restriction of processing. Such actions shall be communicated to each recipient of the personal data, unless it either *proves impossible* or *involves disproportionate effort.* Furthermore, if the data subject requests so, the controller needs to inform him about those recipients that were notified. The purpose of the notification obligation is to enable effective enforcement of the rights in question.[465] Notification may be impossible for example when the identity of the recipients is no longer known to the controller, disproportionate effort when the personal data were published and there is a large number of recipients, though this always needs to be assessed on a case-by-case basis.[466] Although Article 19 does not explicitly refer to the right to be forgotten, it may be seen as a form of notification obligation, which is also regulated under Article 17 (2).[467]

3.3.4 Right to data portability

Article 20 of the GDPR introduces to the data protection law a new right to data portability, very much discussed in a cloud computing context. The purpose of this right is to empower data subjects by giving them more control over their personal data as well as foster competition between the controllers by facilitating switching from one service to another.[468]
The right to data portability enables the data subject to request:

[1] receipt of a subset of personal data, without necessarily transferring it to another controller (e.g. to store them on a private device);

---

[461] Article 17 (2), GDPR.
[462] VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 163.
[463] For more information see: <https://en.wikipedia.org/wiki/Streisand_effect>.
[464] NULÍČEK et al., 'GDPR', op. cit., p. 214.
[465] PAAL. In: 'Datenschutz-Grundverordnung', op. cit., Article 19, rec. 3.
[466] VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 167.
[467] Ibid, p. 168.
[468] WP29 Guidelines on the right to data portability (WP242 rev.01), as last revised and adopted on 5 April 2017, pp. 3-4.

[2] transmission of personal data to another controller.

Data portability applies only if the processing operations are based on either the data subject's consent or, on a contract, to which the data subject is a party and the processing is at the same time *carried out by automated means*. Moreover, the data portability involves only the personal data concerning the requesting data subject, which he or she *has provided* to the controller.[469] Now, WP29 clarified that the data falling under the notion of 'provided by' shall include personal data provided *knowingly and actively* (e.g. account data), but also data *resulting from the observation* of the data subject's activity and thus provided indirectly.[470] These may include activity logs, history of website search or raw data derived from a smart device tracking the data subject's heartbeat. On the other hand, the data that are inferred from the personal data provided are not covered by the right to data portability. These include data created by profiling or user categorisation.[471]

Controllers are expected to use formats that are *structured, commonly used, and machine-readable.* These formats can be coined as interoperable, supporting easy re-use of the personal data.[472] However, the receiving controllers are not required to support the particular format used by the transmitting controller. WP29 encourages establishment of common set of standards and formats in individual sectors.[473]

The right to data portability can only be exercised provided the rights and freedoms of others are not adversely affected.[474] This provision concerns situations when a certain subset of personal data includes not only the data of the data subject that requests receipt or transmission, but also of another natural person. WP29 explains that if a new controller uses the personal data of non-requesting persons for the same purpose as the original controller, the rights and freedoms of third parties are unlikely to be adversely affected.[475] The opposite situation occurs when the receiving controller defines new purposes. In that case, the controller needs to make sure that the processing is lawful, and third parties are not prevented from exercising their rights under the GDPR.[476] But WP29 also makes it quite clear that the controller shall put in considerable effort and seek to accommodate the data subject's request. Implementation of mechanisms that will recognize other data subjects involved and whether they are willing to consent to facilitate the transmission is recommended.[477] The same applies, if the requested subset of personal data involves intellectual property or trade secrets. Although they have to be considered, their existence

[469] Article 20 (1), GDPR.
[470] WP29, 'On the right to data portability', op. cit., pp. 10-11.
[471] Ibid.
[472] Article 20 (1) and Recital 68, GDPR.
[473] WP29, 'On the right to data portability', op. cit., pp. 17-18.
[474] Article 20 (4), GDPR.
[475] WP29, 'On the right to data portability', op. cit., pp. 11-12.
[476] Ibid.
[477] Ibid.

should not imply refusal to transmit all the information.[478] The controller shall endeavor to find a way to transmit the personal data in a form that does not infringe on these rights.

The controller is expected to implement appropriate means for the provision of the personal data. Firstly, there should not be any *hindrance*.[479] In other words, obstacles that would slow down reuse of personal data.[480] These include any fees, technical or legal barriers. When *technically feasible,* the data subject has the right to have the personal data transmitted directly between the controllers.[481] Technical feasibility shall be assessed on a case-by-case basis. It is important to bear in mind that the personal data still have to be transmitted in a secured way.[482] Recital 68 specifies that technical feasibility does not require controllers to design technically *compatible* systems. As WP29 explained, the new data controller must ensure compliance with the GDPR and particularly its principles, before the receipt of the personal data. Mainly, the new controller has to state the purpose of the processing and abide by data minimisation, i.e. accept only the personal data necessary for the purpose of the processing.[483]

Article 20 (3) stipulates that exercise of the right to data portability shall be without prejudice to the right to erasure, or any other right under GDPR.[484] Any obligations between the data subject and the transmitting controller remain in force. In other words, the controller can still process the personal data and the data subject use its services.[485]

As is the case with other rights under the GDPR, the controller is obliged to inform the data subjects about the existence of the right to data portability, sufficiently explain its impact and distinguish it from other rights.[486] An answer to a request must be provided without undue delay, within a month of the receipt of the request at the latest, a period which can be extended by two months, provided that the data subject is informed about the reasons of the delay within the original time frame.[487]

3.4 Other selected aspects of the GDPR

In this subchapter, I will consider the remaining provisions of the GDPR, which are relevant for the analysis of the challenges it poses for cloud computing.

[478] Ibid.
[479] Article 20 (1), GDPR.
[480] WP29, 'On the right to data portability', op. cit., p. 15.
[481] Article 20 (2), GDPR.
[482] WP29, 'On the right to data portability', op. cit., p. 19.
[483] Ibid, p. 12.
[484] Ibid, p. 7.
[485] NULÍČEK et al., 'GDPR', op. cit., p. 225.
[486] WP29, 'On the right to data portability', op. cit., p. 13.
[487] Ibid, p 14.

3.4.1 Security of personal data

Under the GDPR, both controllers and newly also processors are obliged to implement *appropriate technical and organizational measures* to ensure adequate security of the personal data.[488] For cloud computing, this means that all cloud service providers have this direct responsibility, including those merely providing an infrastructure.[489] The approach of the GDPR towards security is risk-based,[490] in other words, the security measures chosen need to reflect the level of risks associated with the specific processing in question.[491] The risk assessment should take into account primarily the impact on the data subject but also risks for other persons.[492] Other criteria to consider include the costs of implementation, state of the art, scope, context and purposes of the processing.[493] Considerable variety of measures may be implemented. GDPR expressly provides examples such as pseudonymisation and encryption and sets targets that the controllers and processors shall aim to achieve. Firstly, the chosen measure should be able to ensure *ongoing confidentiality, integrity, availability, and resilience* of the systems used for the processing and thus be designed to guarantee a durable security.[494] Closely connected to this target is the requirement of *regular testing* of the *effectiveness* of implemented measures.[495] Another target that the measure has to meet is the *ability to* timely *restore availability and access* in case of incidents.[496] This is a challenge for all ICT systems, where the risk of permanent loss of data is a major concern.[497] Its inclusion however, can be seen as favorable as it fosters awareness about the issues.[498] In terms of organizational measures, the controllers and processors must ensure that any persons acting under their authority strictly follow the instructions of the controller, unless they are required to do otherwise by EU or Member State law.[499]

GDPR introduces general notification obligations regarding personal data breaches,[500] where personal data breach needs to be understood as any breach of security, leading to *accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to,* processed personal data.[501] The cause of the breach may be technical or physical.[502] Notification obligations fall on

---

[488] Article 32 (1), GDPR.

[489] HON, W. Kuan, KOSTA, Eleni, MILLARD, Christopher and STEFANATOU, Dimitra. *Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation* [online]. Queen Mary School of Law Legal Studies Research Paper No. 172/2014 and Tilburg Law School Research Paper No. 07/2014. March 2014, p. 24. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2405971>. Last accessed 2 March 2018.

[490] VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 40.

[491] Recital 76, GDPR.

[492] VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 40.

[493] Article 32 (1), GDPR.

[494] Article 32(1) (b), GDPR, MARTINI, In: 'Datenschutz-Grundverordnung', op. cit., Article 32, rec. 40.

[495] Article 32(1) (d), GDPR.

[496] Article 32(1) (c), GDPR.

[497] MARTINI, In: 'Datenschutz-Grundverordnung', op. cit., Article 32, rec. 41.

[498] HON, KOSTA, MILLARD, STEFANATOU, 'Cloud Accountability', op. cit., p. 26.

[499] Article 32 (4), GDPR. An obligation to do so is stipulated in Article 29, GDPR.

[500] VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 65.

[501] Article 4 (12), GDPR.

[502] Article 32 (1) (c), GDPR.

the controller as well as the processor, including the IaaS cloud service providers. The controller is obliged to notify the competent supervisory authority and document the breach, including the actions taken. If a processor is engaged, it needs to notify the controller. The time limits set for the notification are rather confusing. First, the controller is required to notify *without undue delay* and if feasible, within 72 hours after becoming *aware* of the breach. If the 72-hour limit is not adhered to, the controller shall explain the reasons for the delay. But in case of a controller-processor scenario, the processor shall notify the controller *without undue delay* after becoming aware of the breach, as the 72-hour time limit is not applicable for the processor. The relationship between the notification obligations requires further clarification.

In terms of the content of the notification, it must include at least the essential information outlined in Article 33, such as the nature of the breach and its possible consequences. The only exemption from the notification obligation applies to the controllers in case the breach is unlikely to result in any risk to the rights and freedoms of natural persons, including immaterial damage.[503] However, the burden of proof lies on the controllers.

As far as the communication of the breaches to the data subjects is concerned, the obligation falls only on the controller and needs to take place if the breach is likely to result in *high risk* to the rights and freedoms of natural persons.[504] Exemptions include cases, where the notification would require disproportionate effort or measures were taken to ensure the risks do not materialize. This is at first assessed by the controller, but if the supervisory authority has a different view, it may order the controller to notify the data subjects.

3.4.2 DPIA

Data protection impact assessment (hereinafter 'DPIA') is a preventive instrument designed to ensure and help demonstrate compliance with the GDPR.[505] In line with the risk-based approach, an obligation to carry out DPIA affects only the types of processing which are *likely to result in a high risk to the rights and freedoms of natural persons*.[506] GDPR expressly states that in particular processing using new technologies will likely require a DPIA.[507] According to a non-exhaustive list pursuant to Article 35 (3), processing will be likely high risk also if it involves a systematic and extensive evaluation of personal aspects relating to natural persons, including profiling done by automated means and the use of its results significantly affects these natural persons; large scale processing of sensitive data; or large scale systematic monitoring of public areas. Generally, processing of large amount of data will often need a DPIA.[508] In the future, national supervisor authorities shall issue lists of types of processing that are subject to DPIA and may as well issue a

[503] Recital 85, GDPR.
[504] Article 34, GDPR.
[505] Recital 90, GDPR.
[506] Article 35 (1), GDPR.
[507] Article 35 (1), GDPR.
[508] VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 48.

list of those that are not.[509] Another useful tool to help evaluate whether the processing is likely high risk provide the guidelines issued by WP29. According to WP29, there are nine criteria that a controller should consider before making a decision.[510] The first three are based on the express examples in the GDPR described above. Other decisive factors can be whether the processing involves sensitive data or data of highly personal nature, data concerning vulnerable subjects, is large scale,[511] involves combining or matching data sets, innovative use of new technology or organizational solutions. WP29 states that *in most cases,* if two of the criteria are met, a controller shall carry out DPIA and then *in some cases,* one may be enough.[512] And finally recommends that controllers carry out DPIA even if they are not obliged to, since it is particularly useful for the demonstration of compliance.[513] Taking into account the criteria outlined above, cloud computing services are extremely likely to require a DPIA in most cases.

GDPR provides minimum requirements as far as the content of the DPIA is concerned, such as the description of the processing, its purposes, necessity, proportionality and risks.[514] In terms of its scope, DPIA may be used to assess a single data processing operation, a set of similar ones or even an impact of a cloud service as a whole.[515] The choice of appropriate methodology is left upon the controller, DPIA may take many different forms and is case-specific, though it shall be a genuine assessment of risks as seen from the perspective of the data subjects.[516] Furthermore, DPIA shall be regarded as requiring continuous monitoring of any changes in the processing, which may trigger reassessment.[517]

Although in most cases cloud service providers will be considered processors and the GDPR makes controllers responsible for carrying out the DPIA, processors should assist the controller and provide any necessary information.[518] In practice, substantial help from the cloud service providers's side will be undoubtedly needed. The question is how well this can work in case of multitenant environments, where the processors are large players like Google or Amazon, so that the DPIA is not reduced to a document merely serving a purpose to demonstrate compliance and whether there are instances in the cloud, in which DPIA might not be reasonably needed.[519]

---

[509] Article 35 (4), (5), GDPR.

[510] WP29 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 (WP 248 rev.01), as revised and adopted on 4 October 2017, pp. 9-11.

[511] Some limited guidance on what constitutes large scale processing can be found in WP29 Guidelines on Data Protection Officer 16/EN (WP 243).

[512] WP29, 'On DPIA', op. cit., pp 11-12.

[513] Ibid, p. 8.

[514] Article 35 (7), GDPR. and corresponding Recitals 84 and 90, GDPR.

[515] WP29, 'On DPIA', op. cit., pp. 7-8.

[516] Ibid, p. 17.

[517] GDPR, Article 35 (11) , GDPR and WP29, 'On DPIA', op. cit., p. 14.

[518] Article 28 (3) (f), GDPR.

[519] HON, KOSTA, MILLARD, STEFANATOU, 'Cloud Accountability', op. cit., p. 31.

3.4.3 Codes of Conduct

GDPR encourages formation of approved Codes of Conduct**,** which shall be sector-specific and take into account distinctive features and needs in a particular area of application.[520] Several Codes of Conducts for the cloud are being conceived and the concept is highly relevant for the industry. I will now consider the legal basis of the Codes and reflect on their potential in cloud computing in chapter four.

The Codes are intended to provide guidance on the application of provisions contained in the GDPR and may address issues such as pseudonymisation, notification of personal data breach or the exercise of the rights of data subjects.[521] Recital 98 holds that they are meant to *"calibrate the obligations of controllers and processors".* In a sense, they supplement the deficiencies associated with an omnibus legal regime. Codes may be prepared by Member States, supervisory authorities, the Board, European Commission or *private entities* like associations representing specific controllers or processors.[522]

Once the codes are drawned, the approval procedure depends on whether they relate to processing activites in one Member State only or several. If concerned with a territory of a Member State only, they need to be approved pursuant to Article 40 (5) by a competent supervisory authority, which is obliged to register and publish them. The Codes which shall have general validity would go throught the supervisory authority to the Board, which may assess them and grant approval.[523] The general validity is passed on the Code by way of an implamanting act adopted by the Commission.[524] For the sake of transparency, all Codes shall be made publicly available.[525]

Adherence to the codes shall be monitored by a body which has sufficient expertise and is accredited for these purposes.[526] By submitting themselves to the Code, businesses agree to that extra monitoring.[527] Monitoring body can take actions if an approved code is infringed on and must inform about it the supervisory authority.[528] A failure to do so may result in fines imposed on that monitoring body pursuant to Article 83 (4) (c).

The concept of the Codes was introduced already under the Directive,[529] but the GDPR changes its quality, and considerably expands incentives provided for the businesses should they decide to join a Code of Conduct.[530] Firstly, adherence to the Code may be used as *an element* to

[520] Article 40 (1), GDPR.
[521] Article 40 (2), GDPR provides a non-exhaustive list of provisions that codes may address.
[522] SCHREY, In: 'New European General Data Protection Regulation', op. cit., rec. 566-567.
[523] Article 40 (7), GDPR.
[524] Article 40 (8), (9), GDPR.
[525] Article 40 (11), GDPR.
[526] Articles 40 (4) and 41, GDPR.
[527] SCHREY, In: 'New European General Data Protection Regulation', op. cit., rec. 573.
[528] Article 41 (4), GDPR.
[529] Article 27, GDPR.
[530] SCHREY, In: 'New European General Data Protection Regulation', op. cit., rec. 579.

demonstrate compliance.[531] Though close reading of the provisions implies that it does not have to be deemed a sufficient proof by supervisory authorities.[532] Interestingly, during the negotiations of the GDPR, it was proposed by the Council that it should in certain areas.[533] This does not mean that approved Codes would have no authority. Besides, they may as well serve as competitive advantage[534] and may impact the severity of an administrative fine to be imposed under the GDPR in case of infringments.[535] Adherence to generally valid and approved codes may also ease transfers of personal data to third countries pursuant to Article 46 (2) (e).

3.4.4 Transfers of personal data to third countries

The transfers to third countries concern transfers of personal data which are either [1] undergoing processing or [2] intended for processing after the transfer to a third country, in other words a country that is not a Member State.[536] In practice, personal data are often transferred by the controllers to processors in the US or by processors to sub-processors in the US. Such transfers are allowed only if they comply with the conditions laid down in Article 44 et subseq. of the GDPR. Conditions for personal data transfers under the GDPR are similar to the rules under the Directive, but provide more details.[537] There are five grounds on which the personal data can be transferred:

[1] Adequacy decision adopted by the European Commission (Article 45);
[2] Standard contractual clauses (Article 46 (2) (c), (d));
[3] Binding corporate rules (Article 46 (2) (b));
[4] Approved Codes of Conduct or Certification mechanisms (Article 46 (2) (b), 47);
[5] Any of the derogations under Article 49.

A transfer may take place if the European Commission decides that the third country or a territory or its sector ensures an adequate level of protection, in other words, adopts an adequacy decision. Such transfer then does not require any further specific authorization. The decision needs to be reviewed at least every four years and the situation monitored on an ongoing basis. If the third country no longer ensures adequate level of protection, the Commission may repeal, amend or suspend its decision. The decisions and any updates are published in the Official Journal of the European Union and on the Commission's website. Reacting to *Schrems*, Article

[531] Articles 24 (3) and 28 (5), GDPR.
[532] VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 71.
[533] HON, KOSTA, MILLARD, STEFANATOU, 'Cloud Accountability', op. cit., p. 40.
[534] SCHREY, In: 'New European General Data Protection Regulation', op. cit., rec. 576.
[535] Article 83 (2) (j), GDPR and WP29 Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP253), adopted on 3 October 2017, pp. 15-16.
[536] It is important to note that the EEA Joint Committee may pass a resolution upon which the GDPR will be applicable in the whole European Economic Area and in that case the free flow of personal data will apply in the EEA instead of EU, no additional safeguards will be needed for these transfers PAULY, In: 'Datenschutz-Grundverordnung', op. cit., Art. 44, rec. 3.
[537] VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 116.

45 (2) sets out what elements the Commission needs to take into account when assessing whether the third country ensures adequate level of protection. Recital 104 than confirms that an adequacy decision means that a third country ensures level of protection *"essentially equivalent"*. Adequacy decisions adopted under the Directive remain in force until repealed, suspended or amended. However, the Commission has announced in November 2017 that it is reviewing all the 12 adequacy decisions in place.[538]

In the absence of an adequacy decision, additional appropriate safeguards under Article 46 are available. Currently widely used in cloud computing are the EU Standard Contractual Clauses (known as "SCC"),[539] adopted by the Commission. These clauses commit the party that is established in a third country to guarantee adequate level of data protection with respect to the processing in question. The clauses have to be adopted unaltered between the parties but can form part of a broader agreement, which provides other safeguards.[540] So far, the Commission adopted three sets of SCCs. Two of them for transfers from EU controllers to non-EU controllers and one for transfers from EU controllers to non-EU processors.[541] All SCC have been amended in 2016 as a reaction to *Schrems* and their further faith remains to be seen.

Besides SCC, the appropriate safeguards under the GDPR include also binding corporate rules, internal rules, which need to be approved by the competent supervisory authority in accordance with the consistency mechanism.[542] Article 47 sets out detailed requirements on their content and conditions under which the supervisory authority shall approve them. Under the Directive, binding corporate rules were not provided for in a specific provision, but were developed by WP29 to ease the international transfers in the groups of undertakings.[543]

Another option how to demonstrate that appropriate safeguards are in place is adherence to an approved Code of Conduct or a Certification mechanism with EU-wide validity, together with binding and enforceable commitments of the processor or controller in the third country to actually give effect to the safeguards towards the persons that transfer data to them.[544]

In the absence of the abovementioned options, transfer may take place if any of the *derogations for specific situations* apply.[545] The list provided is exhaustive. Especially relevant in practice may be that a transfer can take place even if there are no guarantees as to the level of data protec-

---

[538] STUPP, Catherine. Commission conducting review of all foreign data transfer deals [online]. Available at: <https://www.euractiv.com/section/data-protection/news/commission-conducting-review-of-all-foreign-data-transfer-deals/>. Last accessed 1 April 2018.

[539] Article 46 (c), (d), GDPR.

[540] VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 120.

[541] 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC C(2001) 1539; 2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries C(2004) 5271 and 2010/87/: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council C(2010) 593.

[542] Article 63, GDPR.

[543] VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 125.

[544] Article 46 (2) (e) (f), GDPR.

[545] Article 49, GDPR.

tion in the receiving third country, if the data subject *explicitly consents* to a proposed transfer. In such a case, he or she needs to be informed also about risks accompanying the transfer. Another derogation to be noted allows tranfers similarly to the lawful grounds for processing, when it is strictly necessary[546] for the performance of a contract between a controller and a data subject or for the performance of a contract entered into in the interest of the data subject between the controller and a third person.

[546] VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 130.

4 The challenges for the cloud

This chapter aims to prove the hypothesis, that the GDPR includes wording and concepts that are highly impractical in cloud computing and therefore pose considerable challenges for the industry. It is divided into five main parts, based on the areas of the GDPR identified as potentially problematic in cloud computing. They represent the challenges in the broadest sense. Within them, the author analyzes either the wording of the provisions or particular concepts, in the light of how cloud computing functions. The chapter builds on the explanations provided in the preceeding parts of this thesis and therefore differentiates between the three cloud service models, where applicable.

4.1 Personal data in cloud computing

The first recognized challenge is the definitional issue. It concerns a theoretical question of which data are regulated as personal data in the cloud. Hon recognizes that there are three potentially problematic aspects to that end:

[1] data anonymisation and pseudonymisation;
[2] data encryption;
[3] data fragmentation.[547]

4.1.1 Anonymisation, Pseudonymisation, and Encryption

As was the case under the Directive, "anonymous data" are not considered personal data under the GDPR.[548] Therefore, cloud service providers may often seek to escape its scope by anonymising the data they process. The GDPR does not include a definition of anonymous data in its Articles or explicitly refer to it anywhere else within its text. It merely confirms in Recital 26 that the GDPR shall not apply to *"anonymous information, namely information that does not relate to an identified or identifiable natural person"* or *"to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable"*. This reference is regarded as a definition of anonymous data.

Another concept that the GDPR refers to and newly introduces at a regulatory level is pseudonymisation, defined in Article 4 (5) as *"the processing of personal data in such a manner that the personal data can no longer be attributed to a data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."*

[547] HON, Kuan W, MILLARD, Christopher and WALDEN Ian. What is Regulated as Personal Data in Clouds? In: *Cloud Computing Law*. United States of America: Oxford University Press, 2013, p. 167.
[548] Recital 26, GDPR.

Recital 26 of the GDPR adds that "personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person."

At first glance, the definition of pseudonymisation read together with Recital 26 appears to regard "pseudonymous data" as personal data.[549] They are only stripped of direct identifiers, which are replaced by pseudonyms. The direct identifiers are then kept separately from the pseudonymous data and protected by technical and organizational measures to prevent reattribution. The process of pseudonymisation is therefore not regarded as leading to de-identification, but merely as preventing direct identification.[550]

Although the GDPR does not use this term, the "pseudonymous data" seem to form a subcategory of personal data, which are characteristic by their strengthened protection gained through the application of a privacy-enhancing technique.[551] As Recital 28 states, pseudonymisation can indeed reduce risks processing poses to the data subjects and also be used to demonstrate compliance with the GDPR. However, its introduction is *"not intended to preclude any other measures of data protection"*.[552] In other words, pseudonymisation does not seem to be allowed to lead to the exclusion of its outcome from the scope of the GDPR, and does not render data anonymous. This is in line with the opinion of WP29 expressed under the regime of the Directive, according to which *"pseudonymisation is not a method of anonymisation",* but merely *"reduces the linkability"*.[553]

GDPR recommends pseudonymisation as a security protection measure,[554] and there are incentives provided if it is employed. For example under Article 6 (4) (e), the controller shall take into account the use of appropriate safeguards, including pseudonymisation, when assessing whether the processing for purpose other than for which the data were collected is compatible with the original one. Under Article 34 (3) (a), the communication of the personal data breach to the data subject may not be required. Moreover, Article 25 lists pseudonymisation among methods that can be used to demonstrate compliance with the concept of data protection by design. In effect, it may seem that the GDPR rightly remedies the controllers and processors, who face increased costs with pseudonymisation.

Another term that the GDPR uses is encryption. Encryption is only referred to in several Articles, but not defined. I will therefore use a conventional definition to introduce the concept.

---

[549] See e.g. RÜCKER, In: 'New European General Data Protection Regulation', op. cit., rec. 101 who states that this is "absolutely clear".

[550] MOURBY, Miranda, MACKEY, Elaine, ELLIOT, Mark, GOWANS, Heather, WALLACE, Susan E., BELL, Jessica, SMITH, Hannah, AIDINLIS, Stergios, KAYE, Jane. Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. In: *Computer Law & Security Review: The International Journal of Technology Law and Practice.* April 2018, Volume 34, Issue 2, p. 223.

[551] STEVENS, Leslie. The Proposed Data Protection Regulation and Its Potential Impact on Social Sciences Research in the UK. In: *European Data Protection Law Review.* 2/2015, Vol. 1, p. 99.

[552] Recital 28, GDPR.

[553] WP29 Opinion 05/2014 on Anonymisation Techniques (WP216), adopted on 10 April 2014, p. 3.

[554] Article 32 (1) (a), GDPR.

Encryption is a method commonly used for data security in cloud computing and on the Internet in general as well. Through application of cryptography, the data are converted from a readable form into an encoded format, accessible only when decrypted through the application of a decryption key. The original data form is referred to as *plaintext* and the generated outcome is *ciphertext*.[555] A term key-coded is sometimes used as well, especially in the regulatory context. The GDPR provides similar incentives to the ones provided for pseudonymisation when encryption is used. It generally considers encryption as a measure for risk mitigation.[556] Its existence may be taken into account in the assessment of lawfulness of further processing under Article 6 (4), serve as grounds for the exclusion of the obligation to communicate a personal data breach to the data subject under Article 34 (3) or simply be regarded as an appropriate technical security measure pursuant to Article 32.

Now, the GDPR often lists encryption next to pseudonymisation, treating the two as equal. But the notion of pseudonymisation "and" encryption, used for example in Article 32, implies that the two are in fact not synonyms. WP29 lists encryption as one of the most common pseudonymisation techniques and in the same breath emphasizes that equating encryption to anonymisation is one of the major practical misconceptions.[557] For these reasons, we may conclude that encrypted data are personal data under the GDPR and the reason why the legislator expressly refers to one pseudonymisation technique and no others is unclear.

To sum up, the applicability of the GDPR in terms of its material scope seems to be dependent on the quality of information being either personal or anonymous and has not changed with the express introduction of pseudonymisation.[558] For the most part, this binary perspective tends to lead to *"all or nothing"* situations, which do not take into account the complexities of modern technology.[559]

The interpretation of the concepts of anonymisation, pseudonymisation, and encryption that I just outlined reflects the majority opinion. I will argue that although those conclusions may seem obvious, they may as well be oversimplifications, and that a relevant test should not be whether the data are pseudonymous, but whether a person is identifiable. Otherwise, an effective anonymisation might not be possible in the cloud environment.

4.1.2 What is an effective anonymisation?

Firstly, the notion of *rendering personal data* anonymous signifies that the application of the anonymisation technique on what is still personal data needs to adhere to all the rules laid down by the GDPR. Anonymisation of personal data shall be regarded as processing within the broad

[555] LOSHIN, Peter, COBB, Michael, BAUCHLE, Robert, HAZEN, Fred, LUND, John, OAKLEY, Gabe, RUNDATZ, Frank. Encryption [online]. Available at: <http://searchsecurity.techtarget.com/definition/encryption>. Last accessed 3 March 2018.
[556] Recital 83, GDPR.
[557] WP29, 'Anonymisation Techniques', op. cit., pp. 20-21 and 29.
[558] SPINDLER, Gerald and SCHMECHEL, Philipp. Personal Data and Encryption in the European General Data Protection Regulation. In: *Journal of Intellectual Property, Information Technology and E-Commerce Law.* 7 (2016) 163 para 1, rec. 8, p. 165.
[559] HON, MILLARD, WALDEN, 'What is Regulated as Personal Data in Clouds?', op. cit., p. 168.

notion of the term under Article 4 (2), and legal grounds need to be determined for it to be undertaken lawfully. This view is in line with the opinion of WP29 expressed under the regime of the Directive[560] and seems to be settled.

Secondly, for the data to escape the applicability of the GDPR, the technique used must lead to an outcome where the data subject is *no longer identifiable.*[561] Currently, the limitations of anonymisation are well known, as it is believed that all available techniques pose real risks of re-identification.[562] Anonymous data will therefore never be truly "unidentifiable", not to mention that the risks of re-identification substantially increase as technology advances.

WP29 previously expressed the view that the threshold for effective anonymisation of personal data is very high, supporting a cautious approach.[563] It provided an abstract analysis of the strengths and weaknesses of the most common techniques used for anonymisation, so that controllers were aware of them. The criteria against which the techniques were assessed were strict, asking whether for example an information concerning an individual could still be "inferred". The analysis resulted in the outcome that none of the techniques is completely risk-free, without providing any meaningful guidance.[564] These rigid views signaled to the cloud industry that effective legally acceptable anonymisation may in fact be impossible.

Some argue that sticking to such an opinion could adversely impact innovation and does not strike a proper balance between data protection and freedom of information. Under such strict views, data protection could be rendered limitless,[565] and the concept of anonymisation pointless. But at least for the time being, WP29 does not seem to change its mind, as it has recently referred to its strict opinions again.[566]

Irrespective of fears that effective anonymisation may be unachievable, the determination of whether the data are considered anonymous from the legal perspective is conditional on the question of the data subject's *identifiability*. Recital 26 sets an identifiability test based on whether there are means that are "reasonably likely to be used" by the controller or by another person to identify the person directly or indirectly.[567] Recital 26 of the Directive laid down the same criterion, which has been subject to scrutiny.

---

[560] WP29, 'Anonymisation Techniques', op. cit., p. 6.

[561] Recital 26, GDPR.

[562] See e.g. NARAYANAN, Arvind, FELTEN, Edward W. No silver bullet: De-identification still doesn't work [online]. Princeton, 9 July 2014. Available at: <http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf>. Last accessed 4 March 2018.

[563] WP29, 'Anonymisation Techniques', op. cit.

[564] Ibid, p. 3.

[565] OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. In: *UCLA Law Review.* 13 August 2009, Vol. 57, p. 1741.

[566] WP29 Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing (WP232), adopted on 22 September 2015, p. 7 or WP29 Opinion 2/2017 on data processing at work (WP249), adopted on 8 June 2017, p. 18.

[567] Test that was also needed under the Directive – Recital 26, WP 29, 'On personal data', op. cit., pp. 13-15.

4.1.3 The test of identifiability

There has been much academic debate surrounding the assessment of what the notion of *"means reasonably likely to be used"* encompasses. The question is, whether the approach to its interpretation shall be absolute or relative. In its pure form, *absolute approach* to identifiability requires to consider all, even theoretical, chances of identification. In terms of decryption, this would mean that a person would be identifiable if anyone in the world would be able to decrypt its encrypted data. If applied strictly, since no anonymisation technique is risk-free, this would lead to a situation where rendering data anonymous would be indeed impossible.[568] *Relative approach,* on the other hand, takes into account the necessary effort that the controller would have to put in, so that re-identification could take place, acknowledging that the chances of identification must be realistic for a data subject to be considered identifiable. However, this relative understanding tends to see the chances only from the controller's point of view. It is the controller that must be able to decrypt the data or at least have reasonable chances to obtain additional information to do that.[569]

Let me first turn attention to the wording used in Recital 26 of the GDPR, which refers besides other things to the means that are reasonably likely to be used by a controller or *by another person.* This notion seems to lean towards the absolute approach, considering the abilities of persons other than the controller. But could such person be anyone in the world? Answering in an affirmative would align well with the aim of provision of high data protection to individuals, but hinder the second objective of the GDPR, the free flow of data.[570]

Another notion which inclines towards the absolute approach is that *singling out* may lead to identification according to Recital 26, although using this method, names of persons usually cannot be tied to the data.[571]

On the other hand, the *reasonable likelihood* that means be used can be seen as a relative element, taking into account all objective factors which may be relevant like costs, required time and also technology, not only in terms of its state at the time of the processing but including any future developments.[572]

All things considered, Recital 26 seems to suggest that both relative and absolute elements shall be taken into account. Nevertheless, it does not give a straightforward answer whether identifiability shall be assessed considering abilities of all persons in the world or whether the data may be personal in the hands of one person and not another.

---

[568] SPINDLER, SCHMECHEL, 'Personal Data and Encryption in the European General Data Protection Regulation', op. cit., rec. 12, p. 165.
[569] Ibid, rec. 14, p. 165.
[570] Article 1 (2) – (3), GDPR.
[571] SPINDLER, SCHMECHEL, 'Personal Data and Encryption in the European General Data Protection Regulation', op. cit., rec. 17, p. 166.
[572] Recital 26, GDPR.

Recently, CJEU gave some guidance in *Breyer*, where it considered a question whether a dynamic IP address constitutes personal data in the hands of a website publisher, given that another person, in this case an internet access provider, holds additional information with which it is possible to link the IP address to a natural person.[573] Besides other things, CJEU dealt with a question of indirect identifiability of a data subject. Although the data in question were neither pseudonymised nor anonymised, the Court's argumentation is highly relevant in our context, since the identifiability test was applied.[574]

On the facts of the case, a website publisher was not able to link the IP address directly to an identifiable natural person on its own, but obtaining additional information held by the internet access provider could help.[575] The CJEU held that the IP address nevertheless constituted personal data also *in relation to* that website provider, since the possibility to combine the data with the ones in the hands of the internet access provider constituted means reasonably likely to be used for identification.[576] The website publisher held the information as a precaution of cyberattacks. The German law applicable in this case prohibited the internet access provider to transmit the data to the website publisher directly but would allow transfer in case of cyberattacks. Therefore, there were legal channels reasonably likely to be used, which would allow identification.[577]

As far as the clarification of principles is concerned, the Court noted that it is not necessary that all the information needed for identification are in the hands of one person,[578] and that there would be no means reasonably likely to be used if getting the additional information was prohibited by law.[579] The Court also briefly added that practical impossibility rendering the risk of re-identification in reality *insignificant,* would lead to the same conclusion. Such impossibility could for example stem from the need of disproportionate effort in terms of time or costs.[580]

There are several key takeaways from this case. Unlike in *Sabam*, where the Court held that dynamic IP addresses *in the hands of the internet access provider* were personal data,[581] in *Breyer*, it saw that dynamic IP addresses which are *in the hands of an actor who publishes a website* may be personal data as well. However, the CJEU did not say that dynamic IP addresses would be personal data under all circumstances, being in the hands of anyone. Moreover, it did not explicitly say whether it was immaterial who the third party holding the additional information was for the

[573] 'Breyer', op. cit., para 39.
[574] MOURBY et al., 'Are 'pseudonymised' data always personal data?', op. cit., p. 226.
[575] 'Breyer', op. cit., para 37.
[576] Ibid, para 45.
[577] Ibid, paras 47-49.
[578] Ibid, paras 41, 43.
[579] Ibid, para 46.
[580] Ibid.
[581] Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, EU:C:2011:771, para 51.

data to be identifiable.[582] One view suggests that if there were no legal channels allowing the data to be obtained, simple knowledge on the website publisher's side of a third party which might identify the data subject by combining the information, would not necessarily lead to the same conclusion.[583] The identifiability needs to be assessed on a case-by-case basis.[584] IP addresses may be personal data in the hands of some actors and not others, based on a particular context, practical and legal barriers.[585] The Court seems to mix the relative and absolute approach, providing for some flexibility.[586]

By extension of the logic applied and since Recital 26 of the GDPR mirrors Recital 26 of the Directive applied in *Breyer*, some argue that de-identified data may possibly be regarded as personal or anonymous with regard to certain holders and not others.[587] *Breyer* seems to acknowledge that the relationship between the two actors who hold parts of the information that together may constitute personal data, matters. Ultimately, in the light of this decision, the determination of what constitutes an effective anonymisation technique could become less stringent in the future.[588] However, the real impact of *Breyer* and whether it will be applied in the context of anonymisation and pseudonymisation remains to be seen and the legal uncertainty continues.[589] What is more, the judgement in fact does not deviate from the broad interpretation of the notion of personal data in the EU law.[590] It merely highlights the importance of the identifiability test and explicitly regards means prohibited by law as reasonably unlikely to be used for identification.

4.1.4 Can a pseudonymisation technique render data anonymous?

In light of *Breyer*, another question that arises is, whether legal impact of pseudonymisation should be assessed from the point of view that pseudonymous data are always personal data or whether it is the identifiability test that should serve as a starting point.

WP29 made it clear that pseudonymisation shall not be seen as a method of anonymisation,[591] and Recital 26 of the GDPR seems to follow in its footsteps. Some academics, for example Berberich and Steiner, take this premise and simply assert that if a pseudonymisation

[582] ZUIDERVEEN BORGESIUS, Frederik. The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition (Case Note). In: *European Data Protection Law Review.* 2017, Vol 3, Issue 1, pp. 135-136.
[583] MOURBY et al., 'Are 'pseudonymised' data always personal data?', op. cit., p. 226.
[584] DE HERT, Paul. Data Protection's Future without Democratic Bright Line Rules. Co-Existing with Technologies in Europe after Breyer. In: *European Data Protection Law Review.* 2017. Vol. 3, Issue 1, p. 27.
[585] Ibid.
[586] Ibid.
[587] MOURBY et al., 'Are 'pseudonymised' data always personal data?', op. cit., p. 227.
[588] DE HERT, 'Data Protection's Future', op. cit., p. 27.
[589] MOURBY et al., 'Are 'pseudonymised' data always personal data?', op. cit., p. 227.
[590] KOTULA, Marcin. IP addresses as personal data – the CJEU's judgment in C-582/14 Breyer [online]. Available at: <http://eulawanalysis.blogspot.cz/2017/01/ip-addresses-as-personal-data-cjeus.html>. Last accessed 4 March 2018.
[591] WP29, 'Anonymisation Techniques', op. cit., p. 20.

technique was applied, its outcome are automatically personal data under the GDPR.[592] I consider the arguments emphasizing the significance of the identifiability test as more persuasive.

Let me leave the notion of pseudonymisation pursuant to the GDPR for now. Pseudonymisation can also be afforded a bit different meaning, which is well illustrated by the following definition: *"Pseudonymisation is a technique where direct identifiers are replaced with a fictitious name or code that is unique to an individual but does not itself directly identify them".*[593] This definition which is sometimes referred to as conventional, does not itself determine whether the data are personal. It is neutral and only refers to techniques falling within its ambit.[594]

Adhering to the conventional definition, ICO observed, that the data that have been pseudonymised can fall within the scope of the GDPR or not based on how difficult it is to attribute the pseudonym to an individual.[595] This position acknowledges that effective de-facto anonymisation through pseudonymisation techniques may be possible.

Let me take encryption as a common example of a pseudonymisation technique according to the WP29. There are many scenarios which can come up with encryption. It can be conducted before the client transmits the data to the cloud service provider or undertaken after their receipt. In practice, if encryption is conducted before the transmission to the cloud, cloud service provider may not know what the real nature of the data that it receives is – whether they are personal data of one individual, thousands of people, sensitive data or information linked to companies and not natural persons, encrypted for the sake of trade secrets, or for other reasons.

Hon holds that on condition that a strong encryption method was used and the encryption took place before the data were handed over to the PaaS or IaaS cloud service providers as processors without simultaneous transmission of the key, the data may be considered anonymous with regard to these cloud service providers, based on the facts of a specific case, even if the ciphertext can be decrypted.[596]

Accordingly, with encryption in the cloud, all depends on methods used and the relationship between the parties. If the cloud service provided involves three layers, SaaS provider may be one in thousands of clients of underlying PaaS or IaaS. The SaaS provider then may hold the decryption-key and PaaS and IaaS providers may not. If we take the WP29's view that anonymisation must be irreversible, and encryption cannot in any case lead to anonymisation, strictly speaking, then these encrypted data would be personal data even for the IaaS provider or basically anyone else, since there would be a theoretical possibility of decryption. But the Court in *Breyer* argued that a data subject shall not be identifiable if risks of identification were in reality insignif-

[592] BERBERICH, Matthias and STEINER, Malgorzata. Practitioner's Corner: Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers? In: *European Data Protection Law Review.* 3/2016, Vol. 2, pp. 422-426.

[593] ELLIOT, Mark, MACKEY, Elaine, O'HARA, Kieron and TUDOR, Caroline. The Anonymisation Decision-Making Framework, p. 15. UKAN, 2016. Available at: <https://bit.ly/2ENeUlD>. Last accessed 4 April 2018.

[594] MOURBY et al., 'Are 'pseudonymised' data always personal data?', op. cit., p. 224.

[595] *Information Commissioner's Office, UK.* Overview of the General Data Protection Regulation (GDPR). 20 October 2017, p. 4. Available at: < https://bit.ly/2gZHI4n>. Last accessed 4 April 2018.

[596] HON, MILLARD, WALDEN, 'What is Regulated as Personal Data in Clouds?', op. cit., pp. 175-176.

icant.[597] IaaS provider is naturally data blind, and might not have any effective relationship at all with the SaaS provider, which is one in the myriad of its clients. The SaaS service may be an app, built using PaaS offered by one provider, who engages multiple sub-providers. In reality, it might be highly unlikely that the providers down the stream would have any means using which they could obtain the decryption key. Hon points out that IaaS providers often do not even have control over the form in which their clients choose to upload the data,[598] and their focus is not on the data processing. It seems to be unsatisfactory for the application of law to the IaaS service provider to depend on the client's actions, which the provider may not be able and willing to influence at all.[599]

Perhaps a better illustration is provided by Mourby et al. Let us consider a public authority, which transfers personal data to a research center. The research center encrypts it and holds the direct identifiers separately, with appropriate measures in place to secure them. A researcher who has no direct relationship with the center or the public authority then accesses the data in a secure lab program to conduct medical research. She is only interested in common patterns, has undergone security training and signed an agreement that she will not attempt to identify the data subjects. It is highly unlikely that the researcher would directly obtain the decryption key or any information that would enable her to identify the data subjects. But since the research center holds the key, decryption is not entirely impossible. Encryption is a pseudonymisation technique. If we take the premise that all pseudonymous data are personal data, then the research works with personal data.[600] However, again if we accept that the relevant test is whether a data subject is identifiable, the result might be different. The data could be considered anonymous when in the hands of the researcher. She specializes in medicine not cryptography. Works on a grant that requires timely outcomes and which she would lose if the data were compromised. On top of that, no one would employ her in such a case. In other words, decrypting the data for her would arguably require excessive effort, leading to a conclusion that she does not handle personal data.[601]

Coming back to cloud computing, another example I would like to consider are SaaS storage services. Given that the end-users perform encryption on their data before the transmission through the so-called BYOK (Bring your own Key) encryption technique, not even the SaaS providers may hold the key and be able to decrypt the data. However, in practice it might be problematic to prove that the cloud service providers are transparent about having this ability. For example, Dropbox was previously held liable for lying to its clients about not being able to access their personal data in an intelligible form.[602] Hopefully, since the GDPR strives to shed light on how cloud services work, such information should now be commonly revealed. Nevertheless, it is

[597] 'Breyer', op. cit., para. 28.
[598] HON, MILLARD, WALDEN, 'What is Regulated as Personal Data in Clouds?', op. cit., p. 176.
[599] Ibid.
[600] MOURBY et al., 'Are 'pseudonymised' data always personal data?', op. cit., p. 225.
[601] Ibid.
[602] HON, MILLARD, WALDEN, 'What is Regulated as Personal Data in Clouds?', op. cit., p. 175, footnote 60.

not advisable to use providers without any reputable certifications, such as SO 27001 or SOC 2 Type II.

But things are more complicated than that. Even if the clients upload encrypted data themselves, they may need to decrypt them in order to use the applications. Given that the clients decrypt the data in the environment of the cloud service provider's computing resources, is the provider then considered a processor just because of that action?[603] Under mainstream reading of the GDPR, indisputably yes. Encryption is generally unlikely to lead to render the data subjects unidentifiable in SaaS, since SaaS services often require the data in an unencrypted form to enable its functions.[604] The same applies to the provision of tagging or a search within the data set, including the possibility to convert the data into an interoperable format, aspects that affect right to erasure, rectification and portability under the GDPR. All these functions usually require data processing in an unencrypted form, but as we will see, IaaS clients typically handle these in a self-service manner.

Encryption can as well be employed during the transmission of data only. WP29 indeed previously recommended that the transmissions not only between the systems of the cloud client and cloud service provider, but also for example between the data centers of the provider shall always be undertaken with the data in an encrypted form.[605] Hon argues that the level of strength of encryption may not be required to be as high for transmissions to render the data non-personal, since the time when the possibility of unauthorized access to them exists is relatively short compared to for example storage undertaken by the cloud service provider.[606] She advocates for these nuances to be recognized. Nevertheless, especially in case of use of a strong encryption technique, which could arguably be seen as anonymising the data using the identifiability test, such transfers would not necessarily have to adhere to the rules of the GDPR. Such a conclusion would be a real game changer for the cloud.

On the other hand, if the encryption is undertaken after the transmission of personal data to the cloud by the cloud service provider, traces of unencrypted information may be forgotten in the systems, in form of back-ups and replicas. There is little chance they would be used for identification, should not that be taken into account?

4.1.5 Data fragmentation

Along those lines, a question to consider is whether fragments of data (or the so-called shards in the technical jargon), shall be considered personal data. As I explained in the chapter on cloud computing, fragmentation across different computing resources is commonplace in cloud and in fact allows its scalability. Individual fragments of data may or may not contain sufficient

[603] Ibid, p. 177.
[604] Ibid, p. 178
[605] WP29, 'On cloud computing', op. cit., p. 15.
[606] HON, MILLARD, WALDEN, 'What is Regulated as Personal Data in Clouds?', op. cit., pp. 176-177.

information to directly identify a data subject. Based on its intelligibility and content, it may or may not render a person identifiable. Providers use different systems and deeper analysis of the issue may be impossible without knowledge provided directly by them, everything depends on the methods of fragmentation used and measures taken to restrict "reunification" of the fragments.[607] As I emphasized above, use of encryption on the fragments other than during various transfers, mainly with SaaS services may be impractical, as it would disable the very functions of the service. If the fragments were to be considered personal data, this raises issues with obligations under the GDPR, such as effective erasure, as explained further in this chapter.

Arguably, in the light of Breyer and my analysis above, whether data fragments may be considered information related to an identifiable person, should be assessed applying an identifiability test. In most of the cases, data fragments might be de facto put beyond use and their retrieval highly unlikely.[608] Clarification of their status would enhance legal certainty.

Nevertheless, security measures restricting reunification shall be encouraged. Hon provides a good example of how fragments may end up identifying a person if no safeguards are in place and caution exercised. In 2010, Google Street View vehicles collected the photos for online mapping. It turned out that using a non-password protected wifi networks on the way, they captured fragments of data being transmitted over the wifi. In combination with the route recorded, it was possible to detect detailed information about from which house a message was sent and ultimately the usernames and passwords of individuals.[609]

4.1.6 Reflections on the definitional issue

Uncertainty regarding what techniques are considered effective with regard to anonymisation may discourage their use,[610] as the providers are expected to implement costly measures with no certainty whatsoever as whether they would be accepted as compliant by the authorities.[611] Provision of official regularly updated guidelines about the best practice techniques would be very helpful.

Balancing the interests of the data subjects and the controller, who in many cases may want to use the data for multiple purposes, seems to be successfully achieved in case of pseudonymisation in the GDPR at first, as the incentives provided are advantageous for the cloud. But the concept was arguably introduced in line with increasing risks of re-identification as the technology advances.[612] Hon predicts that more and more data will likely fall into the category of

[607] HON, MILLARD, WALDEN, 'What is Regulated as Personal Data in Clouds?', op. cit., p. 179.
[608] Ibid, p. 180.
[609] Ibid, p. 179.
[610] Ibid, p. 169.
[611] WES, Matt. Looking to comply with GDPR? Here's a primer on anonymisation and pseudonymisation [online]. 25 April 2017. Available at: <https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymisation-and-pseudonymisation/>. Last accessed 4 March 2018.
[612] VIDOVIC ŠKRINJAR, Marina. 'EU Data Protection Reform', op. cit., p. 190.

pseudonymised data with the GDPR.[613] If we consider pseudonymous data to be always personal, this would have an adverse impact on cloud computing, preventing it from carrying out its business model in case of SaaS services based on data mining. Seen through the lens of WP29's current strict interpretation of anonymisation, the threshold for rendering data anonymous may be pushed even higher up, as the authorities may lean towards seeing the techniques as falling into the "middle category".

Article 40 of the GDPR lists among matters that may be specified by the Codes of Conduct besides other things also pseudonymisation. The list is non-exhaustive, so the codes could as well concern anonymisation techniques. However, in its opinion on the C-SIG code of conduct, WP29 criticized that reference to anonymisation was in fact absent from the code and recommended that it should be included in the final version, together with the emphasis that standards required are high.[614] On top of that, the WP29 did not forget to mention that no links between pseudonymisation and possibility of exclusion of the provider from the scope of the GDPR shall be made.[615] Given the current state of both Codes of Conduct related to cloud computing which I will refer to later in this chapter and the fact that the codes will only serve as a guidance to compliance and will not necessarily prevent the authorities from considering the technique ineffective, I cannot see that Codes of Conduct may be expected to tackle the issue in the near future. At least for now, when the GDPR comes into effect in May 2018, cloud service providers will continue to face considerable uncertainty with regard to anonymisation, highlighted by the possibility of imposition of enormous fines in case of incompliance.

In my view, a good solution might be to adopt standards for de-identification similar to the ones in effect in the US under Health Insurance Portability and Accountability Act ("HIPAA"). HIPAA provides that if the standards for de-identification are met, the data are considered anonymous, given the processing entity does not have any reasonable basis to believe that it can be used to identify an individual.[616] These standards are split into a safe harbor and expert determination method. The safe harbor requires the data to be stripped of 18 types of identifiers (such as names, email addresses, but also IP addresses). The expert opinion requires that after the application of statistical or scientific principles, the expert states that there is only a very small risk that the recipient of the anonymous data could identify an individual.[617] In other words, controllers and processers are not faced with the impossible task to provide risk-free anonymisation solutions.

Another option that would help cloud service providers and is easier to adopt, would be a clear statement by the CJEU or the data protection authorities, imposing on cloud service providers an obligation to follow the technological developments and check whether the technique they

---

[613] HON, KOSTA, MILLARD, STEFANATOU, 'Cloud Accountability', op. cit., p. 10.
[614] WP29, 'C-SIG Code of Conduct', op. cit., p. 7.
[615] Ibid.
[616] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) P.L. No. 104-191, 110 Stat. 1938 (1996), section 164.514 (a).
[617] Ibid, sections 164.514 (b) (1) and (2). Further guidance on HIPAA standards available at: <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard>. Last accessed 4 March 2018.

use still holds, taking into account possible impact on the data subject in case of unauthorized access, storage period and so on. This is an approach that for example UK ICO adopted after the WP29's rigid opinion on anonymisation techniques.[618] A risk-based approach also resonates throughout the obligations set out in the GDPR, so it would fit well within its framework.

All in all, the GDPR should allow more flexibility in terms of the assessment of the outcome of pseudonymisation techniques, taking the test of identifiability as a starting point to determine whether the data are personal. However, the test also requires further clarification by the CJEU.

4.2 Controller and processor relationships in the cloud

The second challenge that I recognize concerns determination of who is a controller and who is a processor, and their relationship and obligations.

4.2.1 Distinguishing between controllers and processors

Whether the cloud service providers and their clients are processors or controllers needs to be assessed on a case-by-case basis taking into account the nature of a specific service.[619] The possibilities are endless. In cloud computing, to determine what role do cloud service providers have is not straightforward, as the level of their involvement in the processing significantly differs across cloud service models. However, the distinction is critical, since controllers and processors have different roles and responsibilities under the data protection law.

Even within the same service, the same provider can act as a processor with regard to certain data or processing operations and as a controller for other.[620] A good example is Facebook as a SaaS service provider, which may not have any influence over the purpose of sharing posts. However, besides allowing users to share practically whatever they want, Facebook also scans the posts for profiling of individuals to be able to show them only the advertisements they might be interested in. In such a case, Facebook may act as a controller. Therefore, each processing operation shall be considered separately.[621]

However, a common opinion[622] is that in most scenarios, the cloud service providers will be processors. How does that fit with the definitions under Article 4 (7) and (8) of the GDPR?

It may seem as if it is the cloud service provider who really determines the means of the processing (when understanding the means as being technical mainly, e.g. hardware, software or

---

[618] *Information Commissioner's Office, UK.* Anonymisation: Managing Data Protection Risk. Code of Practice. November 2012. Available at: <https://bit.ly/2qwK1xy>. Last accessed 4 April 2018.

[619] VIDOVIC ŠKRINJAR, Marina. 'EU Data Protection Reform', op. cit., p. 176.

[620] HON, Kuan W, MILLARD, Christopher and WALDEN, Ian. Who is Responsible for Personal Data in Clouds? In: *Cloud Computing Law*. United States of America: Oxford University Press, 2013, pp. 194-195.

[621] Ibid, p. 206.

[622] WP29, 'On cloud computing', op. cit., p. 8.

data centers to be used)[623] and since the controller shall determine both the purposes and the means of the processing of personal data,[624] the cloud service provider would logically be the controller. As I pointed out in the analysis of the definition, key is who determines the purpose of the processing. The controller, if it decides to employ a cloud service provider, shall exercise at least a high level decision-making power over the basic elements of the means used for the processing, but can delegate the determination of the rest. For example, the controller shall be able to choose the tools, designed by the cloud service provider, to be used in the processing, decide how long the data should be processed or who has access to them.[625] This is seen as sufficient by the WP29, which requires that the essential elements regarding the means of the processing be reserved to the controller.[626] In other instances, the cloud client may merely instruct the provider to use the methods appropriate for the purpose of the processing and still remains a controller.[627]

There has been a considerable discussion about the cases in which a cloud service provider may be considered a controller. Cloud service provider will be a controller (or joint controller) if he processes the data for his own purposes.[628] Cloud service providers may have two types of clients, either corporate or individual. Corporate clients usually use the services for their own business purposes and provide a product or a service to their own clients (end-users). SaaS cloud service providers might offer services directly to individuals, who often use the services under household exemption.[629] Generally, it is more likely that a SaaS cloud service provider that has an end-user, a natural person as a client, is a controller with regard to at least some of the processing operations performed on the data related to the use of the service[630] (such services include e.g. emails or document editing programs). The personal data concerned in that case will be account data as well as data generated through the use of the service.[631]

A classic example of when a SaaS service provider is a controller are business models, where services are provided for free to individuals and often based on a trade-off of personal data for the actual service. In such cases, the cloud service providers may be considered controllers, because they (at least partially) determine the purpose of the processing. However, what the lawful grounds for such processing in these cases under the GDPR are is a different question. Commonly, consent is used as a legal basis, but since the requirements for consent has been substantially increased with the GDPR, problematic could be for example its aspect of unconditionality.[632]

---

[623] HON, MILLARD, WALDEN, 'Who is Responsible?', op. cit., p. 208.
[624] Article 4 (7), GDPR.
[625] HON, MILLARD, WALDEN, 'Who is Responsible?', op. cit., p. 208.
[626] WP29, 'On the concepts of "controller" and "processor"', op. cit., p. 14.
[627] Ibid, pp. 14-15.
[628] WP29, 'On cloud computing', op. cit., p. 8.
[629] See chapter 3.1.1.
[630] HON, MILLARD, WALDEN, 'Who is Responsible?', op. cit., p. 206.
[631] Ibid.
[632] Article 7 (4), GDPR.

And even if we were able to argue that such cloud service providers were allowed to obtain consent, what percentage of clients that would deny would it take to destroy the business model?

It shall be noted that in their terms of service, SaaS cloud service providers tend to avoid being classified as controllers. However, the assessment is based on factual circumstances, which prevail over any contractual stipulations.[633] This argument stems not only from the analysis provided by the WP29 on controllers and processors, but also from the very wording of the definition of a controller. The controller is the one who *determines*, not necessarily *lawfully determines* purposes and means of the processing.[634]

The problematic aspects of the determination of accountability based on whether the cloud service provider is a controller or processor do not end here. Professors from the Cloud Legal Project have previously in my view plausibly argued that this binary distinction does not take into account the nature of IaaS services, which should be categorized as neutral intermediaries.[635] The thing is that IaaS providers often do not themselves process the personal data in a meaningful way, but merely provide the infrastructure on which the processing is undertaken by the cloud clients as controllers in a self-serviced way. IaaS providers may lack access to the stored information, for example if the cloud clients encrypt the data before deploying them onto the infrastructure and in any case, are often not involved in the processing even to the extent that they would be aware if the information processed are personal data or even sensitive data. In other words, they have little to no knowledge about the processing activities undertaken. Similar problem may arise with some PaaS providers and SaaS providers, who offer storage as a service only.[636] As the GDPR definition of personal data largely builds on the Directive, cautious approach requires that cloud computing cannot count on the interpretation other than encrypted data are pseudonymised and therefore personal, regardless of who holds the key.[637] Therefore, it seems likely that IaaS service providers will without further assessment be always regarded as processors. Even if the cloud client as a controller keeps full control over the data and their processing, IaaS service provider is in reality data blind,[638] and on top of that not entitled to identify personal data under the agreement with the cloud client.[639]

Hon shows how illogical it is to consider IaaS providers to always be processors by providing a comparison with computer rental, often used as an illustration of IaaS services. "If you rent

---

[633] TEHRANI, Pardis Moslemzadeh et al. The problem of binary distinction in cloud computing and the necessity for a different approach: Positions of the European Union and Canada. In: *Computer Law & Security Review: The International Journal of Technology Law and Practice.* October 2017, Volume 33, Issue 5, p. 676.

[634] Article 4 (7), GDPR.

[635] HON, MILLARD, WALDEN, 'Who is Responsible?', op. cit., pp. 210 et subseq.

[636] HON, Kuan W. Update E-Commerce Directive to address imbalance in GDPR liabilities for infrastructure cloud providers, says expert [online]. 3 October 2016. Available at: < https://www.out-law.com/en/articles/2016/september/update-e-commerce-directive-to-address-imbalance-in-gdpr-liabilities-for-infrastructure-cloud-providers-says-expert/>. Last accessed 2 March 2018.

[637] MAGGIORE, Massimo. EU: Cloud computing: obligations under the Directive v. GDPR. In: *Data Protection Leader.* June 2016, Vol. 13, Issue 6, p. 14.

[638] Ibid.

[639] WP29, 'C-SIG Code of Conduct', op. cit., p. 7.

a computer from a rental company and use that computer to process personal data on your own free will, the rental company is not treated as a data processor under the EU data protection law,"[640] she says.

It seemed that by incorporating a provision stating that the GDPR is without prejudice to the application of the E-commerce directive and the liability of the intermediary service providers in particular,[641] the distinguished nature of IaaS services was recognized.[642] However, as Hon points out, the defences of mere hosting, caching and other under the E-commerce directive are not available when it comes to data protection in the cloud. The E-commerce directive itself states that the questions relating to *information society services* covered by the Directive (GDPR in the near future) are not covered,[643] and calls for the amendment to address this issue.[644] As a result, cloud service provider may have a defence in terms of copyright infringement liability, but not data protection, in the very same situation.[645] This opinion is upheld by the ongoing discussions about the status of IaaS cloud service providers as processors. As I will continue to advocate, considering IaaS cloud service providers to be processors disregards how IaaS works. Another question that arises whether it would not be more suitable to allocate the responsibilities of the actors not based on a binary concept of a controller and processor, but possibly a more flexible approach merely emphasizing accountability, without necessarily giving names to the actors,[646] but that would require a truly revolutionary reform of the EU data protection framework.

4.2.2 Specific obligations of the cloud service providers as processors

Until now, cloud service providers tried to evade being classified as controllers, since under the Directive processors had few obligations. This fact nevertheless led to a broad construction of the term controller by the CJEU.[647] But the GDPR fundamentally changes the data processor-controller relationship as a whole. It allocates responsibilities also to the processors,[648] who are subject to the same astronomic fines as controllers and have to interact directly with the supervisory authorities, who will have investigative powers over them.[649] Besides that, anyone who suffers immaterial or material damage is entitled to claim damages also from the processor, in case the processor did not comply with its obligations under the GDPR or acted outside or contrary to lawful instructions of a controller.[650]

---

[640] HON, 'Update E-Commerce Directive'.
[641] Article 2 (4), GDPR.
[642] Recital 21 adds "*that this E-Commerce Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States*".
[643] Article 1 (5) (b), E-commerce directive.
[644] HON, 'Update E-Commerce Directive', op. cit.
[645] Ibid.
[646] TEHRANI et al., 'The problem of binary distinction', op. cit, p. 683.
[647] In 'Google Spain', CJEU held that Google was a controller to ensure effective data protection.
[648] Article 28, GDPR.
[649] VIDOVIC ŠKRINJAR, Marina. 'EU Data Protection Reform', op. cit., p. 179.
[650] 82 (2), GDPR.

Moreover, cloud service providers as processors may have another strong reason to comply. A 2017 privacy governance report shows that corporate cloud clients as controllers heavily consider GDPR compliance when choosing a provider,[651] in line with their obligation of due diligence under which they shall only choose processors with *"sufficient guarantees to implement appropriate technical and organizational measures"*[652]. Therefore, cloud service providers need to offer services designed in a way that allows controllers to fulfill all their obligations, if they want to stay competitive. They can no longer hide.[653] I will now look at some of the obligations of the processors, which may be impractical in the cloud.

Firstly, in terms of the security of the processing, not only controllers, but also processors are obliged to implement organizational and technical measures.[654] The assessment of which measures are appropriate shall be risk-based, taking into account the very specifics of the processing.[655] This obligation seems to require personalized risk-assessments, based on the nature, scope, context and purposes of the cloud client's needs.[656] But public cloud services are not designed around the possibility of customisation.[657] Quite on the contrary, they are standardized services, which is the main reason why they allow economies of scale. They may have thousands of clients. Building in scenario-specific security measures for every one of them is not possible in the public cloud.[658]

Secondly, the GDPR places a new obligation to keep records of the processing activities on the controllers as well as processors,[659] and sets out what information needs to be included in broad terms. The required level of detail, for example as far as the purpose of the processing is concerned, remains unclear and calls for specification.[660] The purpose of the records is to facilitate demonstration of compliance with GDPR as they have to be made available to s supervisory authority upon request.[661] The obligation of record-keeping arguably does not make any sense for IaaS service providers and in most of the cases also for the providers of PaaS. As was pointed out, these providers are by nature of the service they provide not interested in the data that are being processed on a platform or an infrastructure, and often do not even have visibility into it. Instead of acknowledging how these services function, the GDPR seems to force them to take interest in

---

[651] *The International Association of Privacy Professionals.* IAPP-EY Annual Privacy Governance Report 2017 [online]. Available at: <https://iapp.org/media/pdf/resource_center/IAPP-EY-Governance-Report-2017.pdf>. xv-xvi. Last accessed 2 March 2018.

[652] Article 28 (1), GDPR.

[653] WEBBER, Mark. The GDPR's impact on the cloud service provider as a processor [online]. In: *Privacy & Data Protection,* 2016, Vol. 16, Issue 4., p 11. Available at: <http://www.fieldfisher.com/media/3993765/the-gdprs-impact-on-the-cloud-service-provider-as-a-processor-mark-webber-privacy-data-protection.pdf>. Last accessed 2 March 2018.

[654] Article 32, GDPR.

[655] Ibid, *"taking into account […] the nature, scope, context and purposes of the processing"*.

[656] WEBBER, 'The GDPR's impact on the cloud service provider as a processor', op. cit., p. 12.

[657] MAGGIORE, ‚Cloud computing: obligations under the Directive v. GDPR', op. cit., p. 14.

[658] WEBBER, 'The GDPR's impact on the cloud service provider as a processor', op. cit., p. 12.

[659] Article 30 (1), (2), GDPR.

[660] VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., pp. 44-45.

[661] Recital 82, GDPR.

the personal data processing undertaken by their clients.[662] Let me take IaaS, provided that the infrastructure is used in a self-service manner and the cloud client as a controller actually implements its own security systems, to oblige the IaaS provider to keep records of how these data are processed, seems absolutely illogical.[663] What is more, I doubt that having an extra actor gaining more visibility into the processing enhances the protection of personal data.

Although the GDPR still places the ultimate responsibility on the controllers, processors have a wide obligation to *assist* them, among other things with responses to the data subject's requests for exercise of their rights, security processing requirements, data breach notifications and even data protection impact assessment,[664] all that while taking into account the very specifics of their processing. But as repeatedly emphasized, public clouds are not built around customisation, so the fulfilment of these obligations may in practice be compromised. In terms of the data breach notification, there was no such general obligation placed on all processors at a statutory level until now, but it was a recognized good practice with regard to some services in contracts with sophisticated cloud clients.[665] Consequently, negotiating similar conditions may be difficult for clients, who are ordinary tenants.[666] If interpreted strictly, data breach notifications also may not make sense again in IaaS and similar services, where cloud service providers act as neutral intermediaries.

To sum up, the GDPR introduces new obligations imposed directly on processors. Some of them are cloud impractical, since they expect implementation of tailor made measures. Other do not take into account the specifics of different service models. I will look at some of them in more detail in the following subchapters.

4.2.3 Compulsory provisions of cloud contracts

The relationship between the processor and the controller must be governed by a written contract or other binding legal act.[667] This has been mandatory under Directive as well, but in practice the agreements often lacked sufficient detail. GDPR therefore sets out quite extensive list of what it has to include to ensure strong contractual commitments are in place. As WP29 previously stated, any imbalance of power between a cloud client, possibly a SME, and a cloud service provider, possibly businesses like Google, Apple, or Amazon, does not excuse the client from its obligation not to agree to terms that would threaten compliance with data protection laws.[668]

Some of the requirements on compulsory provisions reflect what was previously recognized as the best practice. At first glance, there are no valid objections against inclusion of terms regard-

[662] WEBBER, 'The GDPR's impact on the cloud service provider as a processor', op. cit., p. 12.
[663] Ibid.
[664] Article 28 (3), GDPR.
[665] WEBBER, 'The GDPR's impact on the cloud service provider as a processor', op. cit., p. 13.
[666] HON, KOSTA, MILLARD, STEFANATOU, 'Cloud Accountability', op. cit., p. 39.
[667] Article 28 (3) and (9), GDPR.
[668] WP29, 'On cloud computing', op. cit., p. 8.

ing subject-matter, duration, nature, purpose, or allocation of responsibilities in the contract.[669] However, if we look closer and take an example of a "data blind" IaaS cloud service provider and its client, a company, which instead of renting computers, wants to "rent" an infrastructure, then even these elements of a contract does not seem to fit well with the notion of IaaS services. Their clients, who may not be willing to disclose all the details about their processing, will be forced to do so, or face administrative fines – regardless of the fact that IaaS service providers in practice do not care about these details.[670] But some of the undertakings compulsory under the GDPR do not make sense in cloud computing in general.

Firstly, the cloud service provider can only engage a sub-processor, in other words another cloud service provider in a lower layer of the chain, upon *prior written authorization* of the cloud client.[671] If the authorization is only general, the cloud service provider must inform the client about any intended change prior to its realization to allow for objections. However, SaaS or PaaS services are often already designed as based on a particular PaaS or IaaS. Take an example of Dropbox as a SaaS service architected on Amazon's IaaS. It does not make much sense that Dropbox should be obliged to ask every customer to consent to any such engagements prior to their realization.[672] At best, providers nowadays inform the potential clients about the sub-processors engaged in the processing. But potential clients do not have any chance to authorize cloud service providers down the chain prior to their engagement or push to change provider's stable business agreements with sub-providers to change to reflect their processing.[673] The type of consent that the GDPR requires in terms of sub-processor engagement cannot be unconditional in the cloud environment. Any objections may only lead to a change of service on the client's side.[674] Furthermore, what if the changes are urgently needed in case that for example servers used fail.[675] It is then not in the client's interest to wait until all the other clients using the same provider are notified and given space to authorize the change of a sub-provider.

Secondly, the GDPR requires the provider to enter into a contract with the sub-provider, which guarantees that the sub-provider undertakes the same obligations as set out in the contract between a client and a provider.[676] However, sub-providers, cloud service providers of PaaS or IaaS like Amazon or Google service myriad of cloud service providers with thousands of their own clients and end-users, and therefore reflection of any individual contractual requirements is impossible in practice. Unless all the data processing agreements are identical, providers face the obligation to communicate every single document agreed on with the clients to a provider like

[669] Article 28 (3), GDPR.

[670] HON, Kuan W. GDPR: Killing cloud quickly? [online]. March 17, 2016. Available at: < https://iapp.org/news/a/gdpr-killing-cloud-quickly/>. Last accessed 3 March 2018.

[671] Article 28 (2), GDPR.

[672] HON, 'Killing cloud quickly?', op. cit.

[673] HON, MILLARD, WALDEN, 'Who is Responsible?', op. cit., p. 203.

[674] HON, 'Killing cloud quickly?', op. cit.

[675] HON, MILLARD, WALDEN, 'Who is Responsible?', op. cit., p. 203.

[676] Article 28 (4), GDPR.

Amazon, which will most likely not make any changes to its services based on the specifics of every single contract. The obligation to ensure that sub-providers follow the same obligations as stipulated in controller – processor agreements may only lead either to a situation where providers will push on contracts to remain standardized and non-negotiable, or the absorption of the risks by the first-layer cloud service provider.[677] Weber plausibly argues that imposition of an obligation to pass on *"substantially similar"* terms might have been achievable in practice and points out that all cloud services providers are aware of the fact that to fit in well with the cloud computing nature, all obstacles connected to sub-contracting shall be at best avoided.[678]

Article 28 (3) (a) of the GDPR requires to be stipulated in a contract that cloud service providers process personal data *only on documented instructions* from the cloud client. If the provider acts outside of them, it risks that it may be treated as a controller[679] or worse, be subject to administrative fines for any damage caused by the processing.[680] The instruction requirement mirrors the misunderstanding of cloud computing as just another modern outsourcing scenario. But in the cloud, cloud service providers are not meant to be instructed or tasked by individual clients and carry out customized activities on their behalf.[681] Besides that, what can be considered as an instruction in cloud computing? Hon gives examples of when the instructions requirement may not work. For example, if the instructions were equal to requests to the cloud service provider's systems, which failed to respond (e.g. to save changes in a document in a SaaS service), would that be a failure to comply with the instructions?

If cloud providers were obliged to follow the cloud client's instructions regarding how the applications are maintained or regarding aspects of the infrastructure, cloud service providers would be unable to comply at all. Not to mention that all the instructions shall be documented. Coming again to the issue repeatedly expressed in this thesis, public cloud is designed as standardized. If cloud clients were allowed to instruct the provider on the specifics of the service, this would either disrupt cost savings or in case that the instructions of individual clients conflicted, destroy the service.

A good illustration of how cloud works is a comparison with the situation when one decides not to cook food on his or her own. The options are among others to hire a cook or a caterer – a cloud service provider. With cooking, caterers may be able to follow diet plans of their clients, accommodate allergies of every single person. But cloud mostly involves caterers and cooks that offer merely to heat up ready meals.[682]

Coming back to the IaaS specifics, there are no instructions at all in this service model, as the client does conduct his own operations on the infrastructure and merely uses it in a self-

[677] WEBBER, 'The GDPR's impact on the cloud service provider as a processor', op. cit., p. 13.
[678] Ibid.
[679] Article 28 (10), GDPR.
[680] Article 82 (2), GDPR.
[681] MAGGIORE, 'Cloud computing: obligations under the Directive v. GDPR', op. cit., p. 14.
[682] HON, MILLARD, WALDEN, 'Who is Responsible?', op. cit., p. 199.

service manner.[683] Moreover, more important than the instructions is arguably the overall security of the service, in other words ensuring that the food being heated up is not rotten.[684] The term instructions might have been replaced by a more suitable and technology-neutral word.[685] I would suggest an obligation to process the data besides in line with the underlying purposes specified by the client, also in a way that shall be reasonably expected by the cloud clients, would be more cloud friendly. Hon states that the instruction requirement aims to prevent unauthorized access or disclosure and this fear would be better addressed by clearly emphasized express prohibition of use or disclosure of the data without controller's authorization.[686]

To sum up, the GDPR prescribes that the data processing agreements between cloud services shall contain some cloud impractical compulsory provisions, such as the sub-processor authorization or the instructions requirement. These are unlikely to be eliminated even if presumed standard contractual clauses for the controller-processor relationship are adopted by the Commission or a supervisory authority in the future.[687]

4.2.4 Data protection by design and by default

Another obligation that has significant effects on the cloud industry is the obligation of a controller to comply with the concepts of privacy by design and by default laid down in Article 25 of the GDPR. Although a novelty in the data protection legislative of the EU, a concept of privacy by design, of which the data protection by design is a variation, has been discussed since 1995, when Canadian and Dutch data protection authorities published a joint publication on privacy enhancing technologies (hereinafter 'PETs').[688] Professor Ann Cavoukian then coined the term privacy by design itself. From the EU perspective, European Commission first issued a Communication to promote PETs in 2007.[689] Then in 2010, it explained the term data protection by design as a principle key to comprehensive data protection.[690] The concept gained enthusiastic support both from legal and technology professionals, and was endorsed by supervisory authorities across Member States.[691] Nevertheless, at EU regulatory level, data protection by design is introduced by the GDPR for the first time.

---

[683] VIDOVIC ŠKRINJAR, Marina. 'EU Data Protection Reform', op. cit., p. 178.

[684] HON, MILLARD, WALDEN, 'Who is Responsible?', op. cit., pp. 200-201.

[685] Ibid, p. 215.

[686] HON, 'Killing cloud quickly?', op. cit.

[687] Article 28 (6) – (8), GDPR.

[688] HES, Ronald and BORKING, John (Eds.). Privacy-enhancing technologies: The path to anonymity. Den Haag: Registratiekamer, 1995.

[689] European Commission. Communication COM (2007) 228 from the Commission to the European Parliament and the Council. On Promoting Data Protection by Privacy Enhancing Technologies (PETs). (Not published in the OJC), 2007.

[690] European Commission. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the regions. A comprehensive approach on personal data protection in the European Union. COM/2010/0609 final, p. 11 et subseq.

[691] ROMANOU, Anna. The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. In: *Computer Law & Security Review: The International Journal of Technology Law and Practice.* April 2018, Volume 34, Issue 2, pp. 100-101.

From the ICT perspective, data protection by design, as it is understood at present days, is an approach which requires developers of ICT systems used for data processing to consider legal data protection principles right from the beginning of their development. These principles need to be embedded into them throughout the lifecycle of a product or a service, until the ultimate erasure of the data. The core idea is that appropriate data protection would be impossible to ensure, if the means of the processing were not developed with suitable features.[692] Therefore, data protection safeguards must be built into every cloud service.

However, data protection by design needs to be regarded as a *holistic approach* under the GDPR, and to equate it with PETs would be a misunderstanding.[693] Therefore, the concept requires implementation of both technical and organizational measures, such as business processes and practices.[694]

For better illustration of what data privacy by design encompasses, it might be helpful to imagine it as another fundamental principle of the GDPR, which stands on seven building blocks introduced by Cavoukian. These require that the cloud service providers implement in their services measures which are: [1] proactive and preventive, [2] their default position provides the highest protection possible, [3] its safeguards are integral to the system, [4] while not diminishing its functionality, [5] the protection is end-to-end, in place until the data are securely destroyed, [6] the measures taken are transparent and [7] the systems are user-friendly.[695] Cloud industry professionals shall note especially the requirement that the measures should not compromise the functionality of their services.

The GDPR expressly refers to the second block introduced by Cavoukian as a concept of the data protection by default, which requires that the default settings of the systems used for the processing are such that only the minimum necessary amount of personal data is collected and processed, storage time is the shortest possible and their accessibility confined as much as possible.[696] Implementation of the concept of data protection by default is most relevant with regard to SaaS services and requires that the end-user of the application does not have to change the settings to receive the highest data protection available. The measure therefore aims to help tackle a pressing issue among apps or social networking, which collect as much data as possible.[697]

But not only SaaS services need to be revised and adapted in light of data protection by design and by default. The best practice would be to evaluate what needs to be done based on extensive audits and data protection impact assessments, having all the actors in layered clouds

[692] NULÍČEK et al., 'GDPR', op. cit., p. 260.

[693] ROMANOU, 'The necessity of the implementation of Privacy by Design', op. cit., p. 102.

[694] Article 25 (1), GDPR.

[695] CAVOUKIAN, Ann and CHIBBA, Michelle. *Start with Privacy by Design in All Big Data Applications.* In: Guide to Big Data Applications. SRINIVASAN, S. (Ed.). Springer International Publishing, 2018, p. 40.

[696] Article 25 (2), GDPR.

[697] MARTINI, In: 'Datenschutz-Grundverordnung', op. cit., Art. 25, rec 45.

involved.[698] Significant changes in service functionalities, architectures and development of new components may be needed. For many, there is a shift in thinking, IT developers are taught to make data protection principles integral part of the development of their services.[699] However, solutions are highly service-specific and by far not straightforward to design. Recital 78 proposes the use of pseudonymisation, data minimisation or enabling data subjects to monitor the processing. Undoubtedly, more specific guidance for implementation of appropriate measures is needed.[700] At the moment, recommendations issued by ENISA, which developed its own strategy, may be helpful.[701]

The fact that different controllers have different levels of control over the services they use can again be problematic in the cloud, since they may not be able to influence the design of the services in public clouds, which are standardized. This may disable them from a risk-based evaluation with regard to their specific processing, which Article 25 of the GDPR requires, and holds them accountable for.[702] Nevertheless, the introduction of the data protection by design and default seems to be a step in the right direction, and could actually have a far-reaching positive impact on the level of data protection offered. In any case, specification of what is required is needed,[703] especially given that the enforcement of principles in the GDPR is supported by severe administrative fines.[704] Approved Certification mechanisms may help to prove compliance in the future.[705] But until then, the cloud industry is left with considerable legal uncertainty regarding what measures will be deemed appropriate in terms of compliance.

4.3 Data subject's rights for the digital age

As emphasized in this thesis, the GDPR significantly strengthens the rights of the data subjects, aiming to give them more control over their data. Regardless whether they are considered processors or controllers, cloud service providers and their corporate clients need to make sure that their services are adjusted accordingly. The controllers will be in the position to interact with the data subjects directly, if they make any request and the processors will have to promptly assist them.[706] But is the accommodation of the data subject's request always possible in

[698] RUBIN, Ludo. Five ways European Data Privacy regulations will disrupt Online Video and OTT Businesses [online]. Available at: <https://bit.ly/2qTksF9>. Last accessed 4 March 2018.

[699] SCHREY, In: 'New European General Data Protection Regulation', op. cit., rec. 536.

[700] ROMANOU, 'The necessity of the implementation of Privacy by Design', op. cit., p. 109.

[701] ENISA. Privacy and Security in Personal Data Clouds. Final Report. November 2016. Available at: < https://www.enisa.europa.eu/publications/privacy-and-security-in-personal-data-clouds/at_download/fullReport>. Last accessed 3 March 2018, pp. 16 et subseq.

[702] HON, KOSTA, MILLARD, STEFANATOU, 'Cloud Accountability', op. cit., p. 29.

[703] Ibid.

[704] 83 (4) (a), GDPR.

[705] Article 25 (3), GDPR.

[706] Article 28 (3), 12 (1), GDPR.

the cloud? The two most discussed rights in this regard are the right to erasure and the right to data portability.

4.3.1 Right to erasure

According to a survey conducted by computing.co.uk among one hundred ICT companies with more than one hundred employees, the by-far biggest fear in terms of inability to comply with the GDPR seems to be personal data erasure upon request.[707]

Legally, the right to erasure is not absolute. The data subject may request deletion only under the conditions laid down in Article 17 and provided that none of the exemptions, implying that the processing is nevertheless necessary for one of the reasons set out therein, applies. The controller bears the ultimate responsibility for the erasure. However, the implementation of technical measures that will allow it falls on a cloud service provider, no matter what status it may have. The right to erasure also encompasses the so-called right to be forgotten, which requires the controllers to inform any other controllers about the data subject's request to erase any links to the data, if the controller made the data public. This obligation is qualified by the requirement to *take reasonable steps* including technical measures to inform – not to ensure erasure of the links. All accompanying costs and available technology have to be taken into account as well.[708]

The first concern with regard to cloud computing is how can the personal data be *truly erased* in the cloud. They are often spread across many databases, backed-up in some form or archived, in order to prevent their permanent loss in case the service suddenly shuts down. The processing itself generates data fragments needed to enable scalability of computing resources and fast access. In other words, the operations undertaken on the data are split into sub-operations and the data into fragments of information, which can be located in different places simultaneously.[709] On top of that, such splitting of operations is automatic by the very nature of cloud computing services. Also, since the services are commonly layered, there are multiple cloud service providers involved and the location of personal data must therefore be tracked down across many environments managed by different actors if effective erasure shall be achieved. Some claim that *"true erasure"* is an impossible target and that Internet has indeed *"an eternal memory"*.[710]

Let us use mobile applications used for business purposes as a good illustration of how problematic can traceability of every single copy of information be.[711] The user of the app can upload personal data of his or her clients (for example scan documents containing such infor-

---

[707] LEONARD, John. The right to erasure is the top GDPR compliance concern [online]. 22 May 2017. Available at: <https://www.computing.co.uk/ctg/analysis/3010528/the-right-of-erasure-is-the-top-gdpr-compliance-concern>. Last accessed 3 March 2018.

[708] Article 17 (2), GDPR.

[709] HON, MILLARD, WALDEN, 'What is Regulated as Personal Data in Clouds?', op. cit., p. 181.

[710] LAZZERI, Francesco. The EU's right to be forgotten as applied to cloud computing in the context of online privacy issues. Abstract. In: *Opinio Juris in Comparatione*. Vol. I, n. I, 2015.

[711] TURNER, Paul. Fuhgettaboutit: the GDPR "Right to Erasure" [online]. 1 November 2017. Available at: <https://bit.ly/2qAbjlH>. Last accessed 3 March 2018.

mation into the app). The app then automatically synchronizes its content with the online version of the service and possibly also internal systems of the business that the user works for. Now, the online SaaS version of the service can be built on different PaaS or IaaS than the mobile app, bringing in even more actors that handle the resources where the data flow. Obviously, simply deleting the document from the app will not by itself mean that they are erased. The controller, who is responsible for the accommodation of the data subject's request is the user of the app in our example. The personal data of its client that were processed through the app, its online version and internal systems of the company, now flow around computing resources of three different cloud service providers, in a myriad of copies, back-ups and fragments. How can he ensure that the data are erased? Even the cloud service providers may not be able to locate every single copy of the information.

Many cloud computing services were not designed to allow extensive indexing of the data sets and easy determination and search of every location of the data. Implementation of new functions is necessary, but well within reach.[712] Nevertheless, a survey conducted in 2017 among both EU and US cloud service providers revealed that between 15-20% of them are unable to sufficiently locate subsets of all personal data processed,[713] not talking about their fragments. Even those services that used metadata tagging before, need to implement GDPR specific labels, with regard to identification and location of the data sets that shall be erased. Proper determination of tags requires absolute clarity in terms of legal interpretation of which data are concerned and what standard of erasure is required.

There is no definition of erasure itself in the GDPR. Paal explains that it shall result in a situation where the data are no longer useable (i.e. no one is able to access them or process in any way), at least without extreme effort.[714] WP29 suggests that the data need to be erased truly irretrievably, including their storage in any previous stage of processing, copies or even fragments,[715] setting a very high and possibly unachievable target. The method used for erasure is considered irrelevant. Hon similarly to Paal plausibly argues that with data fragments and other traces of information forgotten in the systems, the law should differentiate between truly retrievable information and something that ICO considered an information that is no longer live and may be extremely difficult to retrieve.[716] ICO further argues that in case the data are encrypted, merely losing the decryption key may render them absolutely useless and de-facto erased.[717]

ENISA also argues that a target steming from a strict interpretation requiring irretrievability is not possible using the known technical means. It suggests that practical could be allowing

[712] Ibid.
[713] Press release: Locating customer data will be half the battle to fulfill EU GDPR's 'right to be forgotten' [online]. Available at: <https://www.blancco.com/press-releases/locating-customer-data-will-half-battle-fulfill-eu-gdprs-right-forgotten/>. Last accessed 5 March 2018.
[714] PAAL, In: 'Datenschutz-Grundverordnung', op. cit., Art. 17, rec. 30.
[715] WP29, 'On cloud computing', op. cit., p. 12.
[716] HON, MILLARD, WALDEN, 'What is Regulated as Personal Data in Clouds?', op. cit., pp. 180-181.
[717] Ibid.

encrypted copies of the data to be retained, given that security measures are in place to prevent unauthorized access.[718] But it is hard to rely on an assumption that the degree of deletion is flexible, given the rigid interpretation by WP29. There is a pressing need for establishment of standards or clarification of a degree at which the erasure is deemed compliant with the GDPR. A good truly technology-neutral approach would be to allow flexibility, taking into account the risks associated with the processing.[719] Moreover, the capabilities of a specific service shall be taken into account. Along those lines, IaaS service providers seem to have an easiest life preparing to allow erasure, since the emerging cloud Code of Conduct for IaaS recommends them merely to enable their clients to design and deploy their own deletion solutions.[720]

In case of SaaS services targeted at individual clients, who use their services under the household exemption, the cloud services providers may benefit from enabling end-users to access their data remotely,[721] so that they can modify, restrict or delete them directly. ENISA adds that although recommendable, the service providers should ensure that these measures do not conflict with other legal obligations.[722] I would consider it an adequate precaution to build in pop-up boxes that will in such cases ask the end-user if he or she wishes to delate the original data permanently. This approach was already adopted for example by iPhone's Photos, which inform upon erasure of a saved picture that the photo will be erased from all iCloud photo libraries on devices connected by the Apple ID and subsequently, whether the user wants to be able to recover it for up to thirty days or delete immediately. One needs to be reminded however, that such erasure may not in the future adhere to the standards of the GDPR, once they are set. Until then, the cloud community is left with uncertainty, whether the WP29's strict opinion will be upheld or not.

The second concern with regard to the right to erasure seems to be a bit overlooked by the IT community. As already mentioned, the right to erasure is not absolute. The fulfilment of the obligation to erase the data requires prior assessment of whether one of the exemptions applies.[723] The most problematic for cloud service providers may be deciding whether the processing of the personal data in question is necessary for exercising the right of freedom of expression and information.[724] This qualification has been added to the provision following criticism that the right to erasure conflicts with other fundamental rights.[725] Now, the balancing test has been left up to the

[718] ENISA. The right to be forgotten – between expectations and practice. November 2012. Available at: <https://www.enisa.europa.eu/publications/the-right-to-be-forgotten>. Last accessed 3 March 2018, p. 7.
[719] HON, KOSTA, MILLARD, STEFANATOU, 'Cloud Accountability', op. cit., p. 12.
[720] CISPE.cloud. Code of Conduct for Cloud Service Providers. 27 January 2017. Available at: <https://cispe.cloud/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf>. Last accessed 3 March 2018, p. 21.
[721] Recital 63, GDPR.
[722] ENISA. 'The right to be forgotten – between expectations and practice', op. cit., p. 14.
[723] Article 17 (3), GDPR.
[724] Ibid.
[725] See e.g. REDING, Viviane. The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age [online]. SPEECH/12/26. Available at: <http://europa.eu/rapid/press-release_SPEECH-12-26_cs.htm>. Last accessed 3 March 2018.

controllers. If they choose not to erase the data, they have to be able to prove their judgment was correct, in line with the principle of accountability. The data subject can challenge such decision under Articles 77 and 79. Given the risk of high administrative fines in case of non-compliance,[726] it is likely that at least smaller controllers will rather accommodate requests for erasure almost *automatically,* than to face the burden of proof towards supervisory authorities or courts.[727] This could have far-reaching adverse effect on the freedom of expression and information.

It shall be noted that Google in its transparency report from 2017 revealed that it indeed conducts a balancing test, without specifying any details. According to that report, from the end of May 2014 till mid-March 2018, Google deleted almost one million URL addresses, which accounted to about 44 % of the requests.[728] I will not attempt to judge these statistics, but leave an open question, whether and how players much smaller than Google, lacking appropriate resources, compliance departments and in-house lawyers, will create and conduct any balancing test.[729]

The scenario that there are serious risks that controllers may tend to delete data more often than a balancing test conducted by authorities or courts would allow, seems to be confirmed by the fact that the discussions on the right to erasure in the ICT community frequently do not even mention the need to undertake the balancing test but focus on the technical aspects of the erasure instead. Moreover, when the decision is left upon the controllers, the application of the provision may be in fact quite unsystematic. Therefore, it is of utmost importance that detailed instructions are provided in the future. These need to be accessible enough for all cloud service clients and providers.

The third concern relates to the obligation to *take reasonable steps* to inform other controllers that a request for erasure has been lodged, if the controller made the data public.[730] Besides the criteria of the costs and available technology, the legislator does not provide any further guidance on what measures taken to identify and inform will be considered sufficient. But especially in the cloud environment, other controllers may be extremely difficult to trace.[731]

The original version of the proposal of the GDPR provided more onerous requirements with regard to the right to be forgotten, one of them being to take not only *reasonable steps,* but *all* reasonable steps, as a reaction to the questioning of the enforceability of the provision.[732] Mitrou claims that the obligation to inform other controllers will in fact not be a significant burden, since the notion of reasonable steps allows for considerable discretion on controller's side

[726] Article 83 (5) (b), GDPR.
[727] VIDOVIC ŠKRINJAR, Marina. 'EU Data Protection Reform', op. cit., p. 184.
[728] See: <https://transparencyreport.google.com/eu-privacy/overview>. Last accessed 3 March 2018.
[729] VIDOVIC ŠKRINJAR, Marina. 'EU Data Protection Reform', op. cit., p. 184.
[730] Article 17 (2), GDPR.
[731] ENISA. 'The right to be forgotten – between expectations and practice', op. cit., p. 8.
[732] MITROU, 'A Law for the Digital Age?', op. cit., p. 45.

and failure to track down all other possible controllers will be easily justifiable in the world of internet.[733] Paal further points out that the obligation may be unclear in terms of its territorial scope.[734] WP29 previously expressed the view that de-listing should not be limited to EU domains, in case of publication of the information online, since this would not sufficiently guarantee the effective protection of the data subjects' rights.[735]

To sum up, there are several challenges that cloud computing faces with regard to the right to erasure. Firstly, it is unclear what standard of erasure is required. If strict interpretation is adopted, then cloud services may not be able to comply technically.[736] Secondly, determination of when the request asking for erasure shall be accommodated needs further clarification, mainly regarding the balancing test.[737] Thirdly, the same applies in term of what constitutes reasonable efforts when contacting other controllers of personal data made public.

4.3.2 Right to data portability

Another concern among cloud computing professionals is the compliance with the right to data portability. The right to data portability is often coined the only truly new right under the GDPR. It addresses one of the main concerns expressed by WP29 in its opinion on cloud computing, that is lack of interoperability between the individual services, which often results in the so-called vendor lock-in situations.[738] Cloud clients are in these cases forced to continue to use the same service due to the difficulty with the transmission of data, although they would prefer otherwise. WP29 emphasizes that most cloud service providers do not use formats that would allow for easy migration of data to another service.[739] This is an issue concerning not only end-users of SaaS or corporate cloud clients of SaaS, but also cloud clients that built their application using a particular platform provider, requiring the use of a specific programming language.[740]

Nevertheless, in the original proposal of the GDPR in the Recital 55, the Commission expressed the intention to target with the right to data portability as a new Internet-specific right, SaaS applications, especially social networking. The data meant to be ported thus concerned photos, lists of friends, calendars, history, or communication.[741] But Article 20 of the adopted GDPR falls on all cloud computing services and social networking is no longer expressly mentioned in the Recitals. Although GDPR regards it as a responsibility of a controller to ensure data portability, it is quite obvious that the challenge is faced by the party providing the service.

---

[733] Ibid.
[734] PAAL, In: 'Datenschutz-Grundverordnung', op. cit., Art. 17, rec. 37.
[735] WP29 Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v agencia espanola de proteccion de datos (AEPD) and Mario Costeja González" C-131/12 (WP 225), adopted on 26 November 2014, p. 9.
[736] ENISA. 'The right to be forgotten – between expectations and practice', op. cit., p. 8.
[737] Ibid.
[738] WP29, 'On cloud computing', op. cit., p. 5.
[739] Ibid, p. 16.
[740] Ibid.
[741] MITROU, 'A Law for the Digital Age?', op. cit., p. 47.

From the legal perspective, it needs to be clarified that the right to data portability applies only under circumstances set out in Article 20 (1), where the processing is carried out by automated means and based on a contract or consent. This restriction of the right to data portability is subject to criticism.[742] Hon holds that practical expression of the provision in cloud computing may be quite limited, when restricted to consent and contract as lawful grounds for the processing,[743] as also legitimate interest is expected to gain more popularity under the GDPR.

Nevertheless, a pressing question urgently needing clarification is to which data the right to data portability applies. The right to data portability requires that data subjects shall be able to receive and transmit without hindrance data that concern them and were *provided by them.*[744] WP29 issued guidance in which it construed the notion "provided by" broadly, emphasizing that the data provided by the data subject are not only the data provided knowingly, but also indirectly, through the use of the service.[745] Thus, according to WP29, data provided by the data subject include information *derived* from the use of any smart devices, i.e. raw data, activity logs and location data. Nevertheless, WP29 holds that on the other hand, the data *inferred* do not fall into the category,[746] bringing in some more confusion. This interpretation received a lot of criticism, allegedly also from the European Commission, whose spokesman said that *"the scope should not go beyond what was agreed in the trilogues."*[747] The same opinion was expressed by several leading data protection lawyers.[748] Seen from a different angle, the wider the scope of the data service providers would be required to hand over, the greater the transparency there would be, regarding what data they really collect.

Similarly to the right to erasure, there is a qualification which requires data controllers to conduct a balancing test when accommodating the data subject's request to port their data. In this case, controllers assess the right of the data subject against rights and freedoms of others, which shall not be adversely impacted.[749] Such exercise at the discretion of the controller may be undesirable with regard to the protection of others. In case of the data portability, WP29 made it clear that the the data subject's requests are especially important and the controllers shall seek to accommodate it.[750] The argument that if the transmission involves a migration of data to a service *similar* to the one which is being abandoned, with the *same or compatible purpose* of data processing,[751] it is unlikely that such transmission would adversely impact rights of others, seems to

[742] Ibid.

[743] HON, KOSTA, MILLARD, STEFANATOU, 'Cloud Accountability', op. cit., p. 45.

[744] Article 20 (1), GDPR.

[745] WP29, 'On the right to data portability', op. cit., pp. 10-11.

[746] Ibid.

[747] MEYER, David. European Commission, experts uneasy over WP29 data portability interpretation [online]. Available at: <https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1/>. Last accessed 3 March 2018.

[748] Ibid.

[749] Article 20 (4), GDPR.

[750] WP29, 'On the right to data portability', op. cit., p. 12.

[751] Ibid, p. 11.

be convincing. Moreover, WP29 suggests that it will almost always be possible to transmit or give out at least part of the data to the data subject. Nevertheless, I hold that cloud service providers shall always try to regard the balancing test as a comprehensive and genuine assessment and such opinions of the WP29 only imply that it acknowledges that difficulties with practical applicability of the provision will arise. But such simplifications, may threaten rights and freedoms of persons other than the data subjects. Though in case of transmissions, an additional safeguard lies on the side of the receiving cloud service providers, since the new controller or processor must also ensure compliance with the GDPR, especially the principle of data minimisation, which would not allow for processing of data that is unnecessary.[752]

Technically, although the right to data portability does not require cloud services to be compatible,[753] as this would be literally impossible in practice, it does insist on *interoperability,* supporting *reuse* of the data. In other words, the format used by cloud services needs to be structured, commonly used and machine-readable.[754] Common standards are mostly yet to be developed with regard to individual services provided.[755] The technical feasibility of direct transmissions between the services remains to be seen in practice. Attempts to find technical solutions respecting specifics of a particular service and determination of standards are underway. Various have been suggested for example by researches from the Carnegie Mellon University.[756] They plausibly argue that regardless of the fears in the cloud computing community, data portability is well within reach as it is technically possible with mere extension of the existing methods. As was the intention of the legislator, the challenge falls most harshly on SaaS providers.

In IaaS, the corporate cloud clients may be in a self-service way able to migrate most of the data.[757] With lack of visibility into the product, IaaS service providers might in many cases not be in a position to assist them with data portability solutions.[758] PaaS providers have better visibility into the data and might assist their clients, again mostly corporate, with the requests for portability by implementing metadata classification – a capability to tag data sets in order to locate them based on certain characteristics.[759] For example, Microsoft Azure already offers a similar function.[760]

In SaaS, the cloud service providers often acting as controllers will directly respond to the data subject's request. They have appropriate visibility and access to the data, which allows them to develop application program interfaces (APIs) to enable individuals to extract their data direct-

[752] Article 5 (1) (c), GDPR.

[753] Recital 68, GDPR.

[754] Article 20 (1), GDPR.

[755] WP29, 'On the right to data portability', op. cit., pp. 17-18.

[756] WANG, Yunfan and SHAH, Anuj. Supporting Data Portability in the Cloud Under the GDPR [online]. 2017, p. 10. Research paper. Carnegie Mellon University. Available at: <http://alicloud-common.oss-ap-southeast-1.aliyuncs.com/Supporting_Data_Portability_in_the_Cloud_Under_the_GDPR.pdf>. Last accessed 2 March 2018.

[757] Ibid.

[758] Ibid, p. 19.

[759] Ibid, pp. 21-22.

[760] Ibid, p. 24.

ly. A great disadvantage of this solution is that APIs, since they are developed by a particular provider, often in fact lack interoperability.[761] Another possible solution is an adoption of standard protocols, if available for particular services, which are mostly generally accepted.[762]

Some providers also allow end-users to download their data in a file that has a standard and commonly used format, which may be favorable under GDPR.[763] However, these formats need to be flexible enough to allow not only access, but also *reuse*. In terms of direct transmissibility in SaaS, researchers suggest development of service-model specific standardized protocols.[764] They further provide an example of Post Office Protocol, already widely used, which allows data migration between personal emails such as Gmail and Yahoo.[765]

In any case, even if data portability required only extensions on the existing technology as research suggests, the implementation costs will be high for the providers who were not already using them. In my view it is questionable whether the requirement to guarantee data migration free of charge (with minor exemptions)[766] is justifiable. WP29 holds that these costs should not be the reason to charge the data subjects, but as Vidovic points out,[767] the EU Expert Group on Cloud Computing Contracts previously considered that it should be a chargeable service.[768] Otherwise, especially in case of data portability, the new rules may greatly impact competition, giving an advantage to the big players. There is in fact a policy recommendation to reflect data portability in some way in the EU competition rules.[769] The contrary argument that the large cloud service providers could use to their advantage if there were indeed fees allowed for portability, expressed by Vidovic,[770] can in my view be easily rebutted by the GDPR's requirement that there shall be no hindrance from the transmitting controller's side.[771] Abusive fees would not stand the test. The ties of the right to data portability to competition law would merit deep analysis, but this is nevertheless not the aim of this thesis.

Mitrou interestingly provides a compelling argument why data portability may not reach the initial goal of the legislators, to allow migration from one social network app to another. The issue is that the controllers are not obliged to adopt technically compatible solutions, unless they already exist.[772] But it is the social networks which are largely closed towards other services provided and do not possess measures to allow interoperability. Allowing them not to develop new

[761] Ibid, p. 14.
[762] Ibid.
[763] Ibid.
[764] Ibid, p. 16.
[765] Ibid.
[766] Article 12 (5), GDPR.
[767] WP29, 'On the right to data portability', op. cit., p. 12.
[768] VIDOVIC ŠKRINJAR, Marina. 'EU Data Protection Reform', op. cit., p. 184.
[769] ENGELS, Barbara. Data portability among online platforms. In: *Internet Policy Review.* 11 June 2016, Vol. 5, Issue 2. Available at: <https://policyreview.info/articles/analysis/data-portability-among-online-platforms>. Last accessed 4 April 2018.
[770] VIDOVIC ŠKRINJAR, Marina. 'EU Data Protection Reform', op. cit., p. 184.
[771] Article 20 (1), GDPR.
[772] Recital 68, GDPR.

techniques would provide an escape path from the obligation of direct transfers between services.[773] I would add that in SaaS in general, cloud clients do not possess considerable technical expertise. Allowing them to receive the data from the app and having to transmit them themselves, could discourage them from the exercise of the right to data portability. Besides that, social networking providers may not see distinct competitive advantage in offering direct data migration.

To sum up, there are well-founded fears that the right to data portability might not materialize in practice, due to its reduction to processing based on consent or contract only or relaxed requirements concerning how far the cloud service provider has to go with the development of new techniques. From the legal point of view, clarification is also needed in terms of what data are considered *provided by* the data subject. There is considerable legal uncertainty for SaaS and PaaS cloud service providers, which needs to be resolved.

4.4 Transparency principle challenges

The problem with lack of transparency was spelled out as one of the key issues regarding cloud computing in the course of the data protection reform in the EU. Consequently, GDPR puts considerable emphasis on the newly explicitly included transparency principle, requiring that the personal data are processed in a manner transparent *to the data subject*.[774] Transparency is realized by extensive information obligations of the controller and reflected in the requirements that any communication with the data subjects must fulfil.[775] In terms of an appropriate communication of the information to the data subject, the threshold is high. SaaS service providers as controllers will need to ensure that the information is easily understandable to an average data subject concerned,[776] and at the same time avoid information fatigue.[777]

4.4.1 Uncovering the layers of cloud computing

In SaaS, cloud service providers as controllers usually choose to communicate to the data subjects information needed in form of documents coined with various titles, such as privacy policy, statement or notice.[778] Their appropriate form needs to be determined based on the specific service offered and be such to ensure that the data subjects do not have to actively seek the information[779] and that the majority of the data subjects actually notices the information.[780] In

[773] MITROU, 'A Law for the Digital Age?', op. cit., pp. 47-48.
[774] Article 5 (1) (a), GDPR.
[775] See chapter 3.3.1.
[776] PAAL, In: 'Datenschutz-Grundverordnung', op. cit., Art. 12, rec. 26-28.
[777] WP29, 'Guidelines on transparency', op. cit., p. 7.
[778] KAMARINOU, Dimitra, MILLARD, Christopher, HON, Kuan W. *Privacy in the Clouds: an Empirical Study of the Terms of Service and Privacy Policies of 20 Cloud Service Providers.* Queen Mary University of London, School of Law, Legal Studies Research Paper No 209/2015, pp. 12-13.
[779] WP29, 'Guidelines on transparency', op. cit., p. 16.
[780] Ibid, p. 13.

the online environment generally, WP29 recommends the use of the so-called *layered privacy statements.* The first layer then should provide a clear overview of the information available and essential information about the processing, with the strongest impact on the data subject. The second and third layer may offer more detailed information, which the data subject may choose to access. The information in different layers cannot contradict and nothing surprising shall be concealed in the second and third layers.[781] This multi-layered approach has already been widely used by SaaS cloud service providers.[782]

WP29 describes other transparency tools that can be used in the online context, such as "push" notices, bringing the information to the notice of the data subject just before the use of the service, "pull" notices, which shall facilitate access to the information or a *single privacy dashboard,* a website, which serves as a directory to all the information available.[783] GDPR also expressly supports use of the visualization tools, by stipulating that the information may be provided in combination with *standardized icons*.[784] The European Commission is empowered to specify which information shall be presented in this form and corresponding procedures.[785] It's mainly the standardizes icons, which may facilitate the communication of the information in the multi-layered approach described above.

However, WP29 warns that the sole use of icons cannot substitute provision of information.[786] In other words, they would possibly need to accompany a link to the full text. Moreover, a US study previously showed that when individual clients of SaaS cloud services were exposed to multi-layered cloud contracts, they rarely examined any other layer besides the first one, not becoming aware of most of the information provided.[787] It is therefore questionable whether this approach can achieve the ambitious goal to truly inform the data subjects about how their data are handled in a complex cloud environment. Especially in terms of the requirement to inform the data subject about the recipients of their personal data or at least their categories.[788]

If we imagine an average user of an iPhone app, who does not have any idea that the data stored therein may be simultaneously processed by another IaaS service provider, or how cloud computing functions at all and assume that the provider of the app needs to make sure the information that another actor is employed in the processing reaches that person, how would that work? If such information is put in a third layer of the cloud contract, it may never reach the data subject and moreover, this may constitute hiding possibly surprising information about the processing and can imply incompliance with the GDPR. If the information pops up on the iPhone display upon the use of an app, it may substantially disrupt the user experience, while the user

[781] Ibid, p. 17.
[782] KAMARINOU, MILLARD, HON, 'Privacy in the Clouds', op. cit., p. 13.
[783] WP29, 'Guidelines on transparency', op. cit., p. 17.
[784] Article 12 (8), GDPR.
[785] Ibid.
[786] WP29, 'Guidelines on transparency', op. cit., p. 22.
[787] KAMARINOU, MILLARD, HON, 'Privacy in the Clouds', op. cit., p. 13.
[788] Article 13 (1) (e), 14 (1) (e), GDPR.

may not understand or care, simply quickly clicking the "I agree" button to be able to continue to use the service.

The author of this thesis holds that providing sufficient information about the processing under the GDPR while avoiding information fatigue is a challenge for SaaS cloud service providers. The obligation shall allow flexibility in practice, following the risk-based approach and what information may be reasonably expected to be comprehensible and desired by the data subjects in question. Wide information obligation puts pressure on the cloud, when its implementation in such a scope may not necessarily improve data protection. Emphasis on security of the processing is arguably a more important cause to pursue.

4.5 Extraterritoriality and transfers to third countries

4.5.1 Extraterritoriality

The broadly designed territorial scope of the GDPR is expected to ensure comprehensive protection of the data subjects and set global standards,[789] where processors and controllers would rather implement the strict GDPR regime to all business activities than having to differentiate.[790] Although this ambitious goal may not materialize in practice, the newly shaped conditions for the territorial scope are expected to have a large impact on cloud computing.

Firstly, the processing will fall within the scope of the GDPR if deemed to be undertaken in the context of the activities of an establishment of a controller or a processor in the EU,[791] even if the processed data are exclusively personal data of data subjects not in the EU[792] and the processing does not take place in the EU. This jurisdiction trigger maintains the provision of a Directive interpreted by the CJEU, which has made it clear that both notions, an establishment and the context of an establishment, need to be construed extremely broadly in *Google Spain* and *Weltimmo*. As Gömann sums up, the cases where the EU data protection laws would not apply to international processing were basically reduced only to situations where the processor or controller is *"not established on EU territory at all"* or where the activity of the establishment does not show even *a tiny link* to the processing activities of the controller or processor.[793] Such extensive interpretation implies that with regard to cloud computing, the sole existence of a data center in the EU may be expected to trigger the application of the GDPR, which could possibly discourage cloud service providers from setting up EU data centers or using them for processing of personal

[789] GÖMANN, Merlin. The new territorial scope of EU data protection law: deconstructing a revolutionary achievement. In: Common Market Law Review. (2017) 54, pp. 567-568.
[790] SCHUMACHER, In: 'New European General Data Protection Regulation', op. cit., rec. 204.
[791] Article 3 (1), GDPR.
[792] VIDOVIC ŠKRINJAR, Marina. 'EU Data Protection Reform', op. cit., p. 194.
[793] GÖMANN, 'The new territorial scope of EU data protection law', op. cit., p. 574.

data of non-EU data subjects.[794] The same applies to non-EU processors, who may not choose to engage EU-based sub-processors as a result.

The newly inserted provision triggering application of the GDPR to the processing activities, even if undertaken by third country controllers and processors who are not established in the EU and the processing does not take place on the EU territory, based on whether they *offer* goods and services to the data subjects in the EU *or monitor* their behavior, which takes place in the EU, attempts to correct any possible gaps in applicability still theoretically left upon the application of the first trigger.[795] However, the "offering of a service" notion itself attracted criticism.[796] Recital 23 states that whether there is an offering of services to the data subjects in the EU depends on whether the controller or processor *apparently envisages* such offering, a term based on *Pammer* and the CJEU's reference to envisaging on a trader's side to do business with the consumers in the EU.[797] The term "envisaging" seems to be compromising legal certainty due to its subjective nature. Although referred to as *a targeting* approach,[798] the GDPR does not use this term and there is also no mention of any other more suitable word, such as "directing" of a service.[799] Any subjective intentions describing the "envisaging" are difficult to judge and prove.[800] On top of that, there is nothing in the non-exhaustive list of the criteria to be taken into account provided by Recital 23 that would suggest any other than broad interpretation can be expected in the future.

Consequently, in the cloud, even if cloud service providers or clients tried to evade having an establishment in the EU, it seems as they would literally have to opt out from doing business in the EU, if they wanted to escape the applicability of the GDPR. With an offering of an app on an iPhone through online App Store, it would arguably be enough if it was offered in the Czech language (Weltimmo), or if it was possible to pay for its download in Euro (Recital 23). Although mere accessibility of a website may be generally insufficient to ascertain the envisaging according to Recital 23, I would argue that it is uncertain how such notion will be applied. For example, if the cloud services provided are accompanied by any EU-specific IP rights, this may rebut the mere accessibility of the service in the EU as insufficient.

On the other hand, one can imagine cases in which cloud service providers may still be able to escape the GDPR. In a hypothetical scenario, an app is offered by a third country controller established in Singapore, available in English, which is one of the official languages there. Pay-

---

[794] HON, KOSTA, MILLARD, STEFANATOU, 'Cloud Accountability', op. cit., pp. 23-24, recommended to explicitly state that the sole existence of data centers in the EU does not trigger GDPR applicability.

[795] GÖMANN, 'The new territorial scope of EU data protection law', op. cit., p. 582.

[796] See e.g. SVANTESSON, Dan Jerker B. Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation. In: *International Data Privacy Law.* November 2015, Vol 5, No. 4, pp. 226-234.

[797] 'Pammer', op. cit., paras 92-93.

[798] HON, Kuan W., HÖRNLE, Julia and MILLARD, Christopher. Data protection jurisdiction and cloud computing – when are cloud users and providers subject to EU data protection law? The cloud of unknowing. In: International Review of Law, Computers & Technology. 30 July 2012. Vol. 26, Issue 2-3, p. 152.

[799] HON, KOSTA, MILLARD, STEFANATOU, 'Cloud Accountability', op. cit., p. 24.

[800] GÖMANN, 'The new territorial scope of EU data protection law', op. cit., p. 586.

ment is offered in Bitcoins or other virtual currency, which is not Member State specific. In this case, even if the controller aimed at doing business in the EU, it seems as even a broad interpretation of the term "envisages" would not necessarily produce a result of placing the processing under the GDPR.[801]

In terms of monitoring of the behavior, which takes place in the EU by a third country processor or controller, this may be arguably problematic to detect.[802] Moreover, it is uncertain what will be the test of an *online behaviour taking place in the EU*. Is it going to be a place from which the data subject accesses the service, the location of the servers or the many locations where the information that is being monitored flows?[803] After all, there are certainly more ambiguous cases than those of SaaS cloud service providers, who monitor the end-user activities for profiling and subsequent behavioral advertising.

To sum up, as Gömann predicts, the concept of establishment may continue to play the main role in triggering the applicability of the GDPR, if the tendency of its broad interpretation continues.[804] Besides that, given the obligation of a controller or processor not established in the EU, whose processing would fall under the scope of the GDPR based on offering of services or monitoring, to appoint a representative in the EU, such situations may quickly lead us back to Article 3 (1) and its rules on establishment. Having a representative in the EU is undoubtedly likely to lead to "stable arrangements".[805] The newly added Article 3 (2) and its vague terms need clarification, their application may otherwise prove challenging in practice.

Seen from another angle, the threat of substantial administrative fines,[806] efforts to remain competitive and extensive media coverage of the GDPR seem to guarantee well that most players will not risk trying to escape the offering or monitoring territorial scope provisions. Therefore, the competitors not established in the EU, doing business in the EU, will likely face the same conditions in terms of data protection as their European counterparts.[807] It indeed seems like every US cloud service provider faces real risk of being subject to the GDPR.[808]

4.5.2 Transfers to third countries

What constitutes a "transfer" remains an unresolved question under the GDPR, as the term itself is not defined. The only interpretation provided by CJEU was in *Lindqvist*, where the Court held that there was *no* transfer of data to another country, where Mrs Lindqvist loaded personal data onto an Internet page, making it accessible to anyone who connects to the

[801] Inspiration drawn from GÖMANN, 'The new territorial scope of EU data protection law', p. 586.
[802] Ibid, p. 587.
[803] Ibid.
[804] Ibid, p. 575.
[805] Ibid.
[806] SVANTESSON, Dan Jerker B. The extraterritoriality of EU Data Privacy Law – its theoretical justification and its practical effect on U.S. Businesses. In: *Stanford Journal of International Law.* (2014) 50 (1), – p. 75.
[807] GÖMANN, 'The new territorial scope of EU data protection law', op. cit., 588.
[808] SVANTESSON, 'The extraterritoriality', op. cit., p. 74.

Internet, including people in third countries.[809] But the term has been generally interpreted as involving not only the moving of the "physical location" of personal data, but also remote access to such data from a third country.[810] This means that what constitutes a transfer tends to be construed broadly and the transfer provisions are likely to be triggered in any case of the cooperation between non-EU and EU cloud service providers, sub-providers and clients.

As majority of large cloud service providers is located in the US, concerns with transfers circle mainly around inadequate data protection therein. There is a growing fear that US law enforcement agencies may be able to access the data stored in the cloud, which are protected by the EU data protection law, if the cloud service provider is a US company. This issue is currently being discussed in what became known as a *Microsoft Ireland* case. In 2013, Microsoft was ordered under the US Stored Communications Act[811] to disclose email data allegedly related to a drug-trafficking case. It handed over the emails stored in the US but refused to do so with the information stored on a server owned by its EU subsidiary and located in Ireland. The lower level US court initially issued a warrant requiring Microsoft to hand the data over. The case then moved on to the US Court of Appeals for the Second Circuit, which reversed the decision. Currently, the data protection lawsuit is still pending, since the United States Department of Justice appealed to the Supreme Court of the US, which agreed to hear the case. The European Commission has filed an *amicus curiae* on behalf of the EU in support of neither party in December 2017, claiming significant interests in the case in terms of correct interpretation of EU law during the proceedings, since the data stored are subject to European data protection laws.[812] On the point of the EU law, Commission states that the question is whether the warrant requiring Microsoft to disclose the data violates its obligations under the GDPR. The discussion already taking place in the previous stages of the case, focuses on Article 48 of the GDPR and its Recital 115, which limit the enforcement of a third country court decisions in the EU, if they require data transfer not authorized under the EU law. Enforcement of these decisions can only be based on an international agreement, such as a mutual legal assistance treaty, third country court order by itself is insufficient to make a transfer lawful.[813] Requirements of Article 48 are without prejudice to other grounds for transfer.[814] Though the Commission explores whether the transfer may be allowed under any of the safeguards under Article 49, such as transfer for important reasons of public interest and necessary for the purposes of compelling legitimate interest, given they are not overridden by the interests or rights or freedoms of the data subjects, the ultimate argument requires that the application of Mutual Legal Assistance Treaties with the US and EU/Ireland are

[809] 'Lindqvist', op. cit., paras 68-69.

[810] HON, Kuan W, MILLARD, Christopher, SINGH, Jatinder, WALDEN, Ian and CROWCROFT, Jon. Policy, legal and regulatory implications of a Europe-only cloud. In: *International Journal of Law and Information Technology.* 2016, 24, p. 263.

[811] The Stored Communications Act, Pub.L. 99–508, effective 21 October 1986.

[812] Brief of the European Commission on behalf of the European Union as *Amicus Curiae* in support of neither party. United States of America v. Microsoft Corporation. In the Supreme Court of the United States. No. 17-2. 13 December 2017, p. 3.

[813] Ibid, pp. 13-14.

[814] Ibid.

given priority[815] in line with Article 48 and risks of conflict with foreign (EU) law is avoided.[816] Microsoft argues that the Stored Communications Act dating back to 1986 is outdated and cannot apply strictly to the world of cloud computing where cloud service providers store data on servers based all around the world in thousands of locations.[817] The law enforcement argues that they can access the data with one click and therefore it should not matter where they are stored and that refusals of tech businesses to disclose data harm criminal investigations.[818] In the meantime, the so-called Cloud Act has been introduced in the US Congress.[819] If passed, it would allow third countries to enter into agreements with the US, which would legalize cross-border access to the digital information under certain circumstances. Nevertheless, the decision of the Supreme Court of the US is going to be of utmost importance for the subsequent development concerning transfers to the US and data protection law in the US and EU in general.

In the meantime, widely used for transfers in cloud computing are the standard contractual clauses**,** which also at the moment face an uncertain future. Irish High Court judge Caroline Costello recently gave a judgment in Data Protection Commissioner v Facebook & Schrems[820] and *decided to refer* the questions concerning the validity of the three SCC Commission decisions enabling transfers to third countries. The case has not been referred to the CJEU yet, as judge Costello awaits further submissions of the parties involved. Therefore, as of now, the SCC remains a valid safeguard to be used for data transfers. It is unclear when the case will be submitted to the CJEU and if the CJEU will consider this issue.

The author interviewed several data protection compliance practitioners based in the EU engaged with cloud service providers in the Sillicon Valley. Tomáš Honzák, dealing with data protection compliance in GoodData said that he sees as a considerable issue that non-EU business overly rely on the SCC, instead of focusing on questions of purposes of the processing, its necessity, risks and technical measures that can be taken to secure the transfer. The same opinion in the scholarly field expressed Hon by stating that discussions about international transfers of data in the cloud should be focused on meeting minimum security requirements and restrictions of

[815] Ibid, pp. 3-4, 14.
[816] Ibid, p. 5.
[817] SMITH, Brad. US Supreme Court will hear petition to review Microsoft search warrant case while momentum to modernize the law continues in Congress [online]. 16 October 2017. Available at: <https://blogs.microsoft.com/on-the-issues/2017/10/16/us-supreme-court-will-hear-petition-to-review-microsoft-search-warrant-case-while-momentum-to-modernize-the-law-continues-in-congress/>. Last accessed 4 April 2018.
[818] LARSON, Selena. Supreme Court to hear high-stakes Microsoft case testing email privacy [online]. 25 February 2018. Available at: <http://money.cnn.com/2018/02/25/technology/microsoft-us-supreme-court-data-sharing/index.html>. Last accessed 4 April 2018.
[819] S.2383 – CLOUD Act. A Bill to amend title 18, United States Code, to improve law enforcement access to data stored across borders, and for other purposes. Introduced in Senate (02/06/2018). Available at: <https://www.congress.gov/bill/115th-congress/senate-bill/2383/text>. Last accessed 4 April 2018.
[820] The Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems, 2016 No. 4809 P., The Irish High Court. Available at: <https://www.dataprotection.ie/docs/EN/03-10-2017-High-Court-orders-a-reference-to-CJEU/m/1666.htm>. Last accessed 4 April 2018.

disclosure.[821] Employment of encryption may be more important than physical location of the data in terms of protection against unauthorized access.[822] In any case, currently available SCC do not apply to a situation when the cloud service provider as a processor is established in the EU and transfers to a sub-processor in the US, a very common case in cloud computing.[823] Mr Honzák adds that their draft version is commonly used, which can be seen as extremely unfortunate.[824]

Another possible ground for transfers to the US cloud service providers is perhaps the most well-known adequacy decision of the European Commission, the EU-US Privacy Shield, which concerns businesses in the US that are self-certified pursuant to the decision.[825] To date, there are 2816 US companies that are self-certified.[826] However, the fate of the EU-US Privacy Shield is uncertain. The previous deal between EU and US, the so-called Safe Harbor adequacy decision was declared invalid by CJEU on the 6th October 2015 in *Schrems*, for concerns over lack of guarantees regarding interference with the fundamental rights and freedoms with regard to access to data by the US intelligence services.[827] European data protection supervisor Giovanni Buttarelli previously said that the Privacy Shield should be temporary[828] and its amendment as data protection law tightens under the GDPR is expected.[829] Moreover, in September 2016, Digital Rights Ireland Ltd brought an action before CJEU claiming inadequate protection of data under the Privacy Shield. However, the annulment request has been ruled inadmissible in November 2017.[830] All in all, the EU-US Privacy Shield does not seem to be a reliable tool for data transfers.

In summary, the transfer provisions are restrictive, but cloud computing is borderless. With uncertainty surrounding the EU-US Privacy Shield, cloud service providers' realistic options in terms of lawful grounds seem to be only binding corporate rules, confined to the groups of undertakings, or standard contractual clauses, which are subject to criticism. This seems unsatisfactory for the cloud industry, especially given the missing definition of what constitutes a transfer. Moreover, in case that a non-EU controller as a cloud client wanted to use an EU-based processor as a cloud service provider, the application of transfer provisions of the GDPR would

---

821 HON, MILLARD, WALDEN, 'Who is Responsible?', op. cit., p. 201.

822 HON, MILLARD, SINGH, WALDEN, and CROWCROFT. 'Europe-only cloud', op. cit., pp. 264-265.

823 VIDOVIC ŠKRINJAR, Marina. 'EU Data Protection Reform', op. cit., p. 200.

824 WP29 Working document 01/2014 on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor" (WP214), adopted on 21 March 2014.

825 VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., pp. 122-125.

826 As of 4 April 2018. For updates see: <https://www.privacyshield.gov/list>.

827 'Schrems', op. cit., paras 88-89.

828 STUPP, Catherine. EU privacy watchdog: Privacy shield should be temporary [online]. 3 August 2018. Available at: <https://www.euractiv.com/section/data-protection/interview/eu-privacy-watchdog-privacy-shield-should-be-temporary/>. Last accessed 4 April 2018.

829 VOIGT, VON DEM BUSSCHE, 'The EU General Data Protection Regulation (GDPR)', op. cit., p. 122.

830 O'DONOGHUE, Cynthia, O'BRIEN, John. CJEU rules Digital Rights Ireland's Privacy Shield invalidation action inadmissible [online]. 8 December 2017. Available at: <https://www.technologylawdispatch.com/2017/12/privacy-data-protection/cjeu-rules-digital-rights-irelands-privacy-shield-invalidation-action-inadmissible/>. Last accessed 4 April 2018.

be triggered for a transfer back to the controller. This seems to be an unfortunate side effect of the GDPR, not necessarily providing any protection to the data subjects in the EU.[831]

4.6 Can cloud Codes of Conduct help?

There is a lot of hope that cloud Codes of Conduct may specify the vague rules in the GDPR, so that cloud industry has easier time complying with some of the cloud-impractical provisions. The European Data Protection Supervisor noted that *"cloud computing specific Codes of Conduct drawn up by the industry and approved by the relevant data protection authorities could be a useful tool to enhance compliance"*[832].

The situation around cloud Codes of Conduct is largely confusing.[833] Firstly, there is the so-called C-SIG EU Data Protection Code of Conduct for Cloud Service Providers. It is still being finalized and emerged through the work of a sub-group of the Cloud Select Industry Group,[834] focusing on drawing up the code. This sub-group was established in response to the Communication of the Commission on Unleashing the Potential of Cloud Computing in Europe, where the Commission undertook that it will work with the industry to agree on a code. Still under the regime of the Directive, which also supported Codes of Conduct,[835] C-SIG submitted its work to the WP29 for their opinion in 2015. WP29 recognized number of substantial gaps in the code stating that it does not meet even the minimum requirements set out in the Directive, and does not provide enough added value.[836] In its opinion, WP29 repeated some of its rigid views on anonymisation, pseudonymisation, or instructions requirement in the cloud.[837] More importantly, it emphasized that the code did not refer to any specific scenarios in the cloud.[838] After that, C-SIG code has been rebranded and a separate organization EU Cloud Code of Conduct (CoC) established in a ceremony organized by the Commission. Nevertheless, CoC's current version 1.7 published in May 2017 still refers to the Directive and can be seen at best as a general commentary.[839] Code's dedicated website only notes that GDPR ready version shall be published in a due course. Latest news from February 2018 talk about new sections addressing the right to data portability added to the code or acknowledgment of differences between SaaS,

---

[831] MOEREL, Lokke. The data transfer regime for processors does not make sense and requires clarification [online]. 9 June 2016. Available at: <https://iapp.org/news/a/gdpr-conundrums-data-transfer/>. Last accessed 4 April 2018.

[832] HUSTINX, Peter. Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe". Brussels, 16 November 2012, rec. 71. Available at: <https://edps.europa.eu/sites/edp/files/publication/12-11-16_cloud_computing_en.pdf>. Last accessed 4 April 2018.

[833] CHASTANET, Pierre. Presentation: Codes of Conduct. 15 February 2017. Available at: <http://ec.europa.eu/newsroom/document.cfm?doc_id=42973>. Last accessed 4 April 2018.

[834] See: <https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct>. Last accessed 4 April 2018.

[835] Articles 27 and 30, Directive.

[836] WP29, 'C-SIG Code of Conduct', op. cit., p. 2.

[837] Ibid, pp. 7-9

[838] Ibid, p. 6.

[839] C-SIG. Code of Conduct for Cloud Service Providers [online]. May 2017, v. 1.7. Available at: < https://eucoc.cloud/fileadmin/cloud-coc/files/European_Cloud_Code_of_Conduct.pdf>. Last accessed 3 March 2018.

PaaS, and IaaS, while staying open to all cloud service providers.[840] Secondly, CISPE drew up a Code of Conduct for Cloud Infrastructure Service Providers, and claims that the current version released in January 2017 is GDPR compliant.[841] There are no reports regarding the views of any authorities on CISPE code available. However, it appropriately takes into account specifics of IaaS and attempts to provide more detailed guidance in comparison to CoC. Thirdly, I shall mention CSA[842] Code of Conduct for the GDPR, which focuses on B2B cloud computing services, regardless if they operate within IaaS, PaaS, or SaaS models. There is currently no opinion issued by the authorities concerning this code available, though it seems to be mostly just a commentary.

To conclude, it is hard to tell when any cloud-specific Codes of Conduct will be finalized and approved pursuant to the GDPR and if so, how much added value they will provide for the industry. As of now, cloud service providers are left to face the challenges of the GDPR on their own. Personally, I see the path taken by CISPE as the right one and am hopeful that not only cloud-specific, but also PaaS or SaaS-specific codes will emerge.

[840] Press Release: "One year EU Cloud Code of Conduct & 100 Days to go to GDPR" [online]. Available at: < https://eucoc.cloud/en/detail/news/press-release-one-year-eu-cloud-code-of-conduct-100-days-to-go-to-gdpr.html>. Last accessed 3 March 2018.

[841] CISPE.cloud. Code of Conduct for Cloud Service Providers [online]. 27 January 2017. Available at: <https://cispe.cloud/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf>. Last accessed 3 March 2018.

[842] Cloud Security Alliance is an organization dedicated to the best practices in terms of security in the cloud. See <https://cloudsecurityalliance.org/about/>. Last accessed 4 March 2018.

5 Conclusion

This thesis aimed to analyze whether the GDPR can be regarded as cloud friendly. The proposed hypothesis was that it cannot be, since it includes wording and concepts, which are highly impractical in cloud computing. In the first chapters, foundations of cloud computing, data protection law in the EU, and GDPR were laid down. In the fourth and last chapter, I used them as building blocks and recognized several problematic areas, which pose challenges for the cloud industry, seeking to ascertain whether they hinder practical applicability of the GDPR or give rise to considerable legal uncertainty.

The first challenge that I considered concerns the very definition of personal data and related concepts of anonymisation, pseudonymisation, and encryption under the GDPR. The mainstream approach to interpretation based on Recital 26 requires that pseudonymous data are considered personal data. This is highly unfavourable for the cloud, since it does not reflect that the possibility of reidentification may differ based on a pseudonymisation technique used. I argued that employment of strong encryption or other pseudonymisation techniques should be allowed to lead to anonymisation of the data, based on the circumstances of a specific case. I see the wording of Recital 26 of the GDPR as confusing. In *Breyer*, CJEU highlighted the relevant test for the assessment of whether the data subjects are identifiable and the data personal. This is judged based on whether there are means reasonably likely to be used for identification. By extension of the argumentation in *Breyer*, I consider that the test of identifiability should serve as a starting point for the differentiation between personal and non-personal data. This would allow flexibility reflecting how cloud computing functions. If the technique applied led to data anonymisation would be assessed on a case-by-case basis and *in relation* to a specific cloud service provider or cloud client. If the contrary opinion is upheld, anonymisation may be unachievable in the cloud. On the whole, the legal uncertainty regarding what is considered an effective anonymisation that the cloud industry currently faces is unsatisfactory and calls for rectification.

The second challenge analyzed concerns the differentiation of controllers and processors in the complex cloud environment, their relationship and obligations. I argued that a distinguished nature of IaaS service providers who do not process data in a meaningful way, should have been acknowledged in the GDPR and showed, how treating them as processors may lead to absurd scenarios. For instance, in terms of the record-keeping obligation or compulsory provisions of the data processing agreements. With regard to other cloud computing services, the issue largely circles around the fact the GDPR does not reflect that public clouds are by their nature standardized. Its requirements such as prior authorization of sub-processors or processing of the data only upon documented instructions therefore cannot work in practice. Non-compliance however attracts exorbitant administrative fines. Though generally positive, as problematic can also be seen the newly introduced concepts of data protection by design and by default, which urgently need further clarification to enhance legal certainty. On balance, as regards the second challenge, main-

ly the issues with the nature of IaaS provider, prior authorization of sub-processors and the documented instructions requirement should have been in my view addressed at a regulatory level.

The third challenge that I considered concerns the right to erasure and the right to data portability. In terms of erasure, I show how the data may be simultaneously located in different environments managed by multiple cloud service providers and true erasure of the data may be unachievable. Since the required standard of erasure is not set by the GDPR, I explore different opinions expressed by WP29 or legal scholars and conclude that an attainable erasure in the cloud needs to allow more flexibility than was required by WP29. Moreover, there are other aspects of the right to erasure needing clarification, especially related to the exemption of the obligation to erase data upon request when the processing is necessary for the exercising of the right of freedom of expression and information. As far as the right to data portability is concerned, it is mostly relevant in SaaS services, mainly social networking, and is technically regarded as an achievable target. However, the wording of the provision in the GDPR allows for escape paths, which may substantially limit its practical impact. All things considered, as laid down in the GDPR, the right to data erasure is applicable to the cloud only with difficulties. Especially the uncertainty regarding what constitutes effective erasure needs to be urgently reduced. The goals of the data portability, on the other hand, may not materialize in practice.

The fourth challenge that I recognized concerns the transparency principle and wide information obligation towards the data subjects. I see it as too extensive to be fullfilable in practice and what is more not necessarily leading to higher protection of personal data. On an example of SaaS apps, I showed that some of the requirements may only be a burden. An average end-user may not be concerned with the app provider's use of a platform provided by a different cloud service provider, and the app provider should not be forced to inform the data subjects about these issues. Accordingly, focus should rather be shifted on technical security measures and safeguards regarding unauthorized access.

As the fifth challenge, I considered the broadened territorial scope of the GDPR together with the international transfers of personal data. In terms of applicability of the GDPR to the processing undertaken by non-EU processors and controllers, I acknowledge the critics regarding the question of what constitutes an "offering of the services" to the data subjects in the EU in an online environment. The criterion based on whether the controller or processor "apparently envisages" such offering of the services included in Recital 23 threatens legal certainty, since it has a subjective nature. The provided examples suggest that the provision will be construed broadly in the future. There is also an ambiguity regarding the notion of monitoring of the behaviour taking place within EU, in terms of what location shall be considered when online. Nevertheless, given the broad reading of what constitutes an establishment and when the processing is considered in the context of its activities, I conclude that cloud service providers are unlikely to escape the application of the GDPR, unless they withdraw from doing business in the EU.

As far as transfers are concerned, the term "transfer" itself remains undefined, which is unfavorable for cloud computing and in my view should have been addressed at a regulatory level. Although the CJEU ruled in *Lindqvist* that mere upload of personal data on a website accessed from a third country does not constitute a transfer, transfers are currently not seen as requiring physical relocation of the data. Remote access to the personal data by a non-EU processor in the US is sufficient. This leads to wide application of provisions restricting transfers in the cloud. Acknowledgement of whether there is a logical access to the personal data in a third country, for example when the data are strongly encrypted, would be more cloud friendly in these terms. Nevertheless, the GDPR does not recognize these nuances and requires adherence to the rules for transfers, which do not solve issues brought up under the Directive, such as the routine usage of the standard contractual clauses in cloud transfers between the US and EU, or uncertain future of the EU-US Privacy Shield adequacy decision. Given these points, the GDPR regulation of international transfers is unsatisfactory for the cloud, which is by its nature borderless. However, the problems with transfers are major in general and there are currently no satisfactory long-term solutions. I expect their significance to be highlighted in the coming years.

All in all, I acknowledge that a regulation which sets out to be omnibus cannot be too specific, as taking into account particularities of one sector could hinder applicability in another.

But I agree with Hon, that the data protection regime could have been designed as more nuanced, proportionate and above all flexible[843] in order to truly reflect the reality of the cloud computing. GDPR would be truly technology-neutral and possibly able to stand the test of the time, if it allowed more flexibility and refrained from the use of language which is illogical when applied to the cloud.

I see as the biggest issues for the cloud, the lack of recognition of different strength of pseudonymisation techniques, uncertainties surrounding the test of the identifiability of the data subjects and complete disregard of the specifics of IaaS cloud services. A provider who does not meaningfully process personal data should not be regarded as a processor.

Number of other terms and concepts used in the GDPR require further clarification to enhance legal certainty of cloud service providers and their clients, or even allow practical applicability. We can reasonably expect CJEU to address these issues in the coming years. The development of its case law will be interesting to observe. Chances are that also the cloud Codes of Conduct may help to tackle some of the minor issues in the future and provide the much-needed guidelines. The cloud industry would also greatly benefit from development of official and appropriate cloud service model specific standards. These may be the solutions in the long run, but the cloud service providers have to comply now. Given the points presented, the GDPR therefore cannot be seen as "cloud friendly".

[843] HON, MILLARD, WALDEN, 'What is Regulated as Personal Data in Clouds?', op. cit., p. 189.

6 List of Abbreviations

API	Application Programming Interface
BYOK	Bring your own Key
CSA	Cloud Security Alliance
CCTV	Closed Circuit Television
CISPE	Cloud Infrastructure Service Providers
C-SIG	Cloud Select Industry Group
CoC	EU Cloud Code of Conduct
CJEU	Court of Justice of the European Union
DPIA	Data Protection Impact Assessment
EC Treaty	Treaty Establishing the European Community
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	EDPB European Data Protection Board
EU	European Union
ENISA	European Union Agency for Network and Information Security
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
ICT	Information and Communications Technologies
ICO	Information Commissioner's Office
IaaS	Infrastructure as a Service
IP	Internet Protocol
ISP	Internet Service Provider
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
PaaS	Platform as a Service
RAID	Redundant Array of Independent Disks
SaaS	Software as a Service
SCC	Standard Contractual Clauses
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
URL	Uniform Resource Locator
UK	United Kingdom
US	United States
VM	Virtual Machine
WP29	Article 29 Working Party

7 Bibliography

7.1 Books and book chapters

BLACK, Nicole. *Cloud computing for lawyers.* United States of America: American Bar Association, 2012. ISBN 978-1-61632-884-9.

CAVOUKIAN, Ann and CHIBBA, Michelle. *Start with Privacy by Design in All Big Data Applications.* In: Guide to Big Data Applications. SRINIVASAN, S. (Ed.). Springer International Publishing, 2018, pp. 29-48. ISBN 978-3-319-53817-4.

DONÁT, Josef, TOMÍŠEK, Jan. Právo v síti. Průvodce právem na internetu. 352 s., 1. vyd. Praha, C.H. Beck, 2016. ISBN 978-80-7400-610-4.

FUSTER GONZÁLES, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* First Edition. Brussels: 2014, Springer International Publishing, 2014. 272 pp. ISBN 978-3-319-05023-2.

HES, Ronald and BORKING, John (Eds.). Privacy-enhancing technologies: The path to anonymity. Den Haag: Registratiekamer, 1995. pp. 1-60. ISBN 90-346-32-024.

HON, Kuan W, MILLARD, Christopher and WALDEN, Ian. What is Regulated as Personal Data in Clouds? In: *Cloud Computing Law*. United States of America: Oxford University Press, 2013, pp. 167-192. ISBN 978–0–19–967167–0.

HON, Kuan W, MILLARD, Christopher and WALDEN, Ian. Who is Responsible for Personal Data in Clouds? In: *Cloud Computing Law*. United States of America: Oxford University Press, 2013, pp. 193-219. ISBN 978–0–19–967167–0.

HON, Kuan W and MILLARD, Christopher. Cloud Technologies and Services. In: *Cloud Computing Law*. United States of America: Oxford University Press, 2013, pp. 3-17. ISBN 978–0–19–967167–0.

KRANENBORG, Herke. Article 8. In: *The EU Charter of Fundamental Rights: A Commentary*. PEERS, Steve, HARVEY, Tamara, KENNER, Jeff and WARD, Angela (Eds.). London: Hart Publishing Ltd., 2014, 223–266 pp. ISBN 978-1-78-225182-8.

LENAERTS, Koen, VAN NUFFEL, Piet. *European Union Law.* Third edition. BRAY, Robert, CAMBIEN, Nathan (Eds.). London: Sweet & Maxwell, 2011. 1083 pp. ISBN 978-0-414-04816-4.

LYNSKEY, Orla. *The Foundations of EU Data Protection Law.* First edition. Oxford: Oxford University Press, 2015. 307 pp. ISBN 978-0-19-871823-9.

MITROU, Lilian. The General Data Protection Regulation. A Law for the Digital Age? In: *EU Internet Law.* Regulation and Enforcement. SYNODINOU, Tatiana-Eleni, JOUGLEUX,

Philippe, MARKOU, Christina, PRASTITOU, Thalia (Eds.), Springer International Publishing, 2017, pp. 19-57.

NULÍČEK, Michal, DONÁT, Josef, NONNEMANN, František, LICHNOVSKÝ, Bohuslav, TOMÍŠEK, Jan. *GDPR.* Obecné nařízení o ochraně osobních údajů. Praktický komentář. První vydání. Praha: Wolters Kluwer ČR, 2017, 544 s. ISBN 978-80-7552-765-3.

PAAL, Boris P., PAULY, Daniel A. (Eds.). Datenschutz-Grundverordnung. Beck'sche Kompakt-Kommentare. München 2017. ISBN 978-3-406-69570-4.

ROUNTREE, Derrick and CASTRILLO, Ileana. *The Basics of Cloud Computing.* Understanding the Fundamentals of Cloud Computing in Theory and in Practice. Waltham: Syngress. ISBN: 978-0-12-405932-0.

RÜCKER, Daniel, KUGLER, Tobias (Eds.). *New European General Data Protection Regulation.* A Practitioner's guide. Ensuring Compliant Corporate Practice. First edition. 291 pp. Baden-Baden: Jointly published by Nomos, C.H. BECK and Hart Publishing. ISBN 978-3-8487-3262-3.

SERVENT RIPOLL, Ariadna. Protecting or Processing? Recasting EU Data Protection Norms. In: *Privacy, Data Protection and Cybersecurity in Europe.* SHÜNEMANN, Wolf J. BAUMANN, Max-Otto (Eds.). Springer International Publishing, 2017. 145 pp. ISBN 978-3-319-53634-7.

VAN DER SLOOT, Bart. Legal Fundamentalism: Is Data Protection Really a Fundamental Right? In: *Data Protection and Privacy: (In)visibilities and Infrastructures.* LEENES, Ronald, VAN BRAKEL, Rosamunde, GUTWIRTH, Serge and DE HERT, Paul, (Eds.) Switzerland: Springer International Publishing, 2017. ISBN 978-3-319-50796-5.

VOIGT, Paul, VON DEM BUSSCHE, Axel. *The EU General Data Protection Regulation (GDPR).* A Practical Guide. Springer International Publishing, 2017, 383 pp. ISBN 978-3-319-57959-7.

7.2 Articles and research papers

BERBERICH, Matthias and STEINER, Malgorzata. Practitioner's Corner: Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers? In: *European Data Protection Law Review.* 3/2016, Vol. 2, pp. 422-426.

DE HERT, Paul. Data Protection's Future without Democratic Bright Line Rules. Co-Existing with Technologies in Europe after Breyer. In: *European Data Protection Law Review.* 2017. Vol. 3, Issue 1, pp. 20-35.

ENGELS, Barbara. Data portability among online platforms. In: *Internet Policy Review.* 11 June 2016, Vol. 5, Issue 2. Available at: <https://policyreview.info/articles/analysis/data-portability-among-online-platforms>.

FUSTER GONZÁLES, Gloria and GELLERT, Raphael. The fundamental right of data protection in the European Union: in search of an uncharted right. In: *International Review of Law, Computers & Technology.* March 2012, Vol. 26, No. 1, pp. 73-82.

GÖMANN, Merlin. The new territorial scope of EU data protection law: deconstructing a revolutionary achievement. In: *Common Market Law Review.* (2017) 54, pp. 567-590.

HON, Kuan W., HÖRNLE, Julia and MILLARD, Christopher. Data protection jurisdiction and cloud computing – when are cloud users and providers subject to EU data protection law? The cloud of unknowing. In: International Review of Law, Computers & Technology. 30 July 2012. Vol. 26, Issue 2-3. pp. 129-164.

HON, W. Kuan, KOSTA, Eleni, MILLARD, Christopher and STEFANATOU, Dimitra. *Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation* [online]. Queen Mary School of Law Legal Studies Research Paper No. 172/2014 and Tilburg Law School Research Paper No. 07/2014. March 2014, pp. 3-54. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2405971>.

HON, Kuan W, MILLARD, Christopher, SINGH, Jatinder, WALDEN, Ian and CROWCROFT, Jon. Policy, legal and regulatory implications of a Europe-only cloud. In: *International Journal of Law and Information Technology.* 2016, 24, pp. 251-278.

HUSTINX, Peter. EU data protection law: The review of directive 95/46/EC and the proposed general data protection regulation. In: *Collected courses of the European University Institute's Academy of European Law, 24th Session on European Union Law*, *1-12 July 2013.* Available at: <https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf>.

HUSTINX, Peter. Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe". Brussels, 16 November 2012. Available at: <https://edps.europa.eu/sites/edp/files/publication/12-11-16_cloud_computing_en.pdf>.

KAMARINOU, Dimitra, MILLARD, Christopher, HON, Kuan W. *Privacy in the Clouds: an Empirical Study of the Terms of Service and Privacy Policies of 20 Cloud Service Providers.* Queen Mary University of London, School of Law, Legal Studies Research Paper No 209/2015, pp. 3-70.

KOKOTT, Juliane and SOBOTTA, Christoph. The distinction between privacy and data protection. In: *International Data Privacy Law,* 2013, Vol. 3, No. 4, pp. 222-228.

LAZZERI, Francesco. The EU's right to be forgotten as applied to cloud computing in the context of online privacy issues. Abstract. In: *Opinio Juris in Comparatione.* Vol. I, n. I, 2015.

MAGGIORE, Massimo. EU: Cloud computing: obligations under the Directive v. GDPR. In: *Data Protection Leader.* June 2016, Vol. 13, Issue 6, pp. 14-16.

MOURBY, Miranda, MACKEY, Elaine, ELLIOT, Mark, GOWANS, Heather, WALLACE, Susan E., BELL, Jessica, SMITH, Hannah, AIDINLIS, Stergios, KAYE, Jane. Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. In: *Computer Law & Security Review: The International Journal of Technology Law and Practice.* April 2018, Volume 34, Issue 2, pp. 222-233.

NARAYANAN, Arvind, FELTEN, Edward W. No silver bullet: De-identification still doesn't work [online]. Princeton, 9 July 2014. Available at: <http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf>.

OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. In: *UCLA Law Review.* 13 August 2009, Vol. 57, 77 pp.

REDING, Viviane. The upcoming data protection reform for the European Union. *International Data Privacy Law.* 2011, Vol. 1, No. 13, pp. 3-5.

ROMANOU, Anna. The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. In: *Computer Law & Security Review: The International Journal of Technology Law and Practice.* April 2018, Volume 34, Issue 2, pp. 99-110.

SPINDLER, Gerald and SCHMECHEL, Philipp. Personal Data and Encryption in the European General Data Protection Regulation. In: *Journal of Intellectual Property, Information Technology and E-Commerce Law.* 7 (2016) 163 para 1, pp. 163-177.

STAIGER, Dominic Nicolaj. *Data protection compliance in the cloud.* Zürich, 2017. Dissertation. Universität Zürich. Prof. em. Rolf H. Weber, Chair.

STEVENS, Leslie. The Proposed Data Protection Regulation and Its Potential Impact on Social Sciences Research in the UK. In: *European Data Protection Law Review.* 2/2015, Vol. 1, pp. 97-112.

SVANTESSON, Dan Jerker B. Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation. In: *International Data Privacy Law.* November 2015, Vol 5, No. 4, pp. 226-234.

SVANTESSON, Dan Jerker B. The extraterritoriality of EU Data Privacy Law – its theoretical justification and its practical effect on U.S. Businesses. In: *Stanford Journal of International Law.* (2014) 50 (1), pp. 53-117.

TEHRANI, Pardis Moslemzadeh et al. The problem of binary distinction in cloud computing and the necessity for a different approach: Positions of the European Union and Canada. In: *Computer Law & Security Review: The International Journal of Technology Law and Practice.* October 2017, Volume 33, Issue 5, pp. 672-684.

VIDOVIC ŠKRINJAR, Marina. EU Data Protection Reform: Challenges for Cloud Computing. In: *Croatian Yearbook of European law & Policy.* 2016, Vol. 12, No. 12, pp. 171-206.

WANG, Yunfan and SHAH, Anuj. Supporting Data Portability in the Cloud Under the GDPR [online]. 2017, pp. 1-41. Research paper. Carnegie Mellon University. Available at: <http://alicloud-common.oss-ap-southeast1.aliyuncs.com/Supporting_Data_Portability_in_the_Cloud_Under_the_GDPR.pdf>.

WEBBER, Mark. The GDPR's impact on the cloud service provider as a processor [online]. In: *Privacy & Data Protection,* 2016, Vol. 16, Issue 4, pp. 11-14. Available at: <http://www.fieldfisher.com/media/3993765/the-gdprs-impact-on-the-cloud-service-provider-as-a-processor-mark-webber-privacy-data-protection.pdf>.

ZUIDERVEEN BORGESIUS, Frederik. The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition (Case Note). In: *European Data Protection Law Review.* 2017, Vol 3, Issue 1, pp. 130-137.

7.3 Legal documents

7.3.1 Primary law

Charter of Fundamental Rights of the European Union, 2012 OJ C 326.

Consolidated version of the Treaty on the Functioning of the European Union, 2012 OJ C 326/01.

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community 2007 OJ C 306/01.

7.3.2 Secondary law

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

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8.

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 ('Directive on electronic commerce'), OJ L 178.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201/37.

Directive 2006/24/EC of the European Parliament and the of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available

electronic communications services or of public communications networks and amending Directive 2002/58/EC, 2016 OJ L 105/54.

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350/60.

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), OJ L 119/1.

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/89.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194/1.

7.3.3 European Commission Decisions, Communications, and other documents

2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC C(2001) 1539.

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

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

Brief of the European Commission on behalf of the European Union as *Amicus Curiae* in support of neither party. United States of America v. Microsoft Corporation. In the Supreme Court of the United States. No. 17-2. 13 December 2017.

European Commission. Communication COM (2007) 228 from the Commission to the European Parliament and the Council. On Promoting Data Protection by Privacy Enhancing Technologies (PETs). (Not published in the OJC), 2007.

European Commission. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the regions. A comprehensive approach on personal data protection in the European Union. COM/2010/0609 final.

European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Unleashing the Potential of Cloud Computing in Europe. COM(2012) 529 final.

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final.

European Commission. Commission Staff Working Paper. Impact Assessment. Brussels, 25. 1. 2012, SEC (2012) 72 final, Annex 2.

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207.

2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215.

7.3.4 Other

Explanations relating to the Charter of Fundamental Rights, OJ C 303, 14.12.2007.

Explanatory Report to Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg: 28 January 1981, European Treaty Series – No. 108.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 108.

S.2383 – CLOUD Act. A Bill to amend title 18, United States Code, to improve law enforcement access to data stored across borders, and for other purposes. Introduced in Senate (02/06/2018). Available at: <https://www.congress.gov/bill/115th-congress/senate-bill/2383/text>.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) P.L. No. 104-191, 110 Stat. 1938 (1996).

The Stored Communications Act, Pub.L. 99–508, effective 21 October 1986.

7.3.5 Cases

Friedrich Stork & Cie v High Authority of the European Coal and Steel Community, C-1/58, EU:C:1959:4.

Erich Stauder v City of Ulm – Sozialamt, C-29/69, EU:C:1969:57.

Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel, C-11/70, EU:C:1970:114.

J. Nold, Kohlen-und Baustoffgroßhandlung v Commission of the European Communities, C-4/73, EU:C:1974:51.

Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk, joined cases C-465/00 and C-138/01 and C-139/01, EU:C:2003:294.

Criminal proceedings against Bodil Lindqvist, C-101/01, EU:C:2003:596.

Productores de Música de España (Promusicae) v Telefónica de España SAU, C-275/06, EU:C:2008:54.

College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer, C-553/07, EU:C:2009:293.

Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy. Satamedia, C-73/07, EU:C:2008:727.

Volker und Markus Schecke and Eifert v Land Hessen, joined cases C-92/09 and C-93/09, EU:C:2010:662.

Deutsche Telekom AG v Bundesrepublik Deutschland, C-543/09, EU:C:2011:279.

Peter Pammer v Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmbH v Oliver Heller, joint cases C-585/08 and C-144/09, EU:C:2010:740.

Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, EU:C:2011:771.

Digital Rights Ireland, Joined Cases C-293/12 and C-594/12, EU:C:2014:238.

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, EU:C:2014:317.

František Ryneš v. Úřad pro ochranu osobních údajů, C-212/13, EU:C:2014:2428.

Coty Germany GmbH v Stadtsparkasse Magdeburg, C-580/13, EU:C:2015:485.

Maximillian Schrems v Data Protection Commissioner, C-362/14, EU:C:2015:650.

Patrick Breyer v Bundesrepublik Deutschland, C-582/14, EU:C:2016:779.

Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, EU:C:2015:639.

Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni, C-398/15, EU:C:2017:197.

Peter Nowak v Data Protection Commissioner, Case C-434/16, EU:C:2017:994.

7.4 Other cases

Niemietz v Germany App no 13710/88. ECtHR, 16 December 1992. A-251-B.

The Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems, 2016 No. 4809 P., the Irish High Court. Available at: <https://www.dataprotection.ie/docs/EN/03-10-2017-High-Court-orders-a-reference-to-CJEU/m/1666.htm>.

7.5 WP29 documents

WP29 Opinion 4/2007 on the concept of personal data (WP136), adopted on 20 June 2007.

WP29 Opinion 5/2009 on online social networking (WP163), adopted on 12 June 2009.

WP29 Opinion 1/2010 on the concepts of "controller" and "processor" (WP169), adopted on 16 February 2010.

WP29 Opinion 3/2010 on the principle of accountability (WP 173), adopted on 13 July 2010.

WP29 Opinion 15/2011 on the definition of consent (WP187), adopted 13 July 2011.

WP29 Opinion 02/2012 on facial recognition in online and mobile services (WP192), adopted on 22 March 2012.

WP29 Opinion 05/2012 on cloud computing (WP196), adopted on 1 July 2012.

WP29 Opinion 03/2013 on purpose limitation (WP 203), adopted on 2 April 2013.

WP29 Working document 01/2014 on Draft Ad hoc contractual clauses “EU data processor to non-EU sub-processor" (WP214), adopted on 21 March 2014.

WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), adopted on 9 April 2014.

WP29 Opinion 05/2014 on Anonymisation Techniques (WP216), adopted on 10 April 2014.

WP29 Guidelines on the implementation of the Court of Justice of the European Union judgment on “Google Spain and inc v agencia espanola de proteccion de datos (AEPD) and Mario Costeja González“ C-131/12 (WP 225), adopted on 26 November 2014.

WP29 Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing (WP232), adopted on 22 September 2015.

WP29 Guidelines on transparency under Regulation 2016/679 (WP260), adopted, but still to be finalized.

WP29 Guidelines on the right to data portability (WP242 rev.01), as last revised and adopted on 5 April 2017.

WP29 Opinion 2/2017 on data processing at work (WP249), adopted on 8 June 2017.

WP29 Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP253), adopted on 3 October 2017.

WP29 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 (WP 248 rev.01), as revised and adopted on 4 October 2017.

WP29 Guidelines on Consent under Regulation 2016/679 (WP259), adopted on 28 November 2017.

7.6 Online publications

CISPE.cloud. Code of Conduct for Cloud Service Providers. 27 January 2017. Available at: <https://cispe.cloud/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf>.

C-SIG. Code of Conduct for Cloud Service Providers. May 2017, v. 1.7. Available at: < https://eucoc.cloud/fileadmin/cloud-coc/files/European_Cloud_Code_of_Conduct.pdf>.

ELLIOT, Mark, MACKEY, Elaine, O'HARA, Kieron and TUDOR, Caroline. The Anonymisation Decision-Making Framework. UKAN, 2016. Available at: <https://bit.ly/2ENeUlD>.

ENISA. Privacy and Security in Personal Data Clouds. Final Report. November 2016. Available at: <https://www.enisa.europa.eu/publications/privacy-and-security-in-personal-data-clouds/at_download/fullReport>.

ENISA. The right to be forgotten – between expectations and practice. November 2012. Available at: <https://www.enisa.europa.eu/publications/the-right-to-be-forgotten>.

Information Commissioner's Office, UK. Overview of the General Data Protection Regulation (GDPR). 20 October 2017, p. 4. Available at: < https://bit.ly/2gZHI4n>.

Information Commissioner's Office, UK. Anonymisation: Managing Data Protection Risk. Code of Practice. November 2012. Available at: <https://bit.ly/2qwK1xy>.

MELL, Peter and GRANCE, Timothy. The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. Gaithersburg: National Institute of Standards and Technology, U.S. Department of Commerce, 2011. Available at: < http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.

The International Association of Privacy Professionals. IAPP-EY Annual Privacy Governance Report 2017 [online]. Available at: < https://iapp.org/media/pdf/resource_center/IAPP-EY-Governance-Report-2017.pdf>.

7.7 Online articles and other sources

BARTOLETTI, Dave. Predictions 2018: Cloud computing accelerates enterprise transformation everywhere [online]. 7 November 2017. Available at: <https://go.forrester.com/blogs/predictions-2018-cloud-computing-accelerates-enterprise-transformation everywhere/>.

BEAL, Vangie. The Differences between Thick and Thin Client Hardware [online]. 6 July 2006. Available at: <https://www.webopedia.com/DidYouKnow/Hardware_Software/thin_client.asp>.

BENSON, Patrick. The Cloud Defined, Part 2 of 8: Broad Network Access [online]. 5 May 2013. Available at: <http://www.pbenson.net/2013/05/the-cloud-defined-part-2-of-8-broad-network-access/>.

BENSON, Patrick. The Cloud Defined, Part 3 of 8: Resource Pooling [online]. 6 May 2013. Available at: <http://www.pbenson.net/2013/05/the-cloud-defined-part-3-of-8-resource-pooling/>.

BIGELOW, Stephen J. Platform as a Service (PaaS) [online]. September 2017. Available at: < https://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS>.

BOISVERT, Michelle and BIGELOW, Stephen J. Infrastructure as a Service (IaaS) [online]. September 2017. Available at: <https://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS>.

BUTLER, Brandon. 3 types of private clouds: Which one's right for you? [online]. 24 November 2015. Available at: <https://www.webopedia.com/TERM/E/everything-as-a-service_xaas.html?relatedterms>.

CHASTANET, Pierre. Presentation: Codes of Conduct. 15 February 2017. Available at: <http://ec.europa.eu/newsroom/document.cfm?doc_id=42973>.

Cloud Industry Forum. Adoption of Cloud computing continues upward trend as a mainstream IT deployment option [online]. Available at: <https://www.cloudindustryforum.org/content/adoption-cloud-computing-continues-upward-trend-mainstream-it-deployment-option>.

FOGARTY, Kevin. Cloud Computing Definitions and Solutions [online]. 10 September 2009. Available at: <https://www.cio.com/article/2424886/cloud-computing/cloud-computing-definitions-and-solutions.html>.

Gartner. Gartner Says Global IT Spending to Reach $3.7 Trillion in 2018 [online]. 3 October 2017. Available at: <https://www.gartner.com/newsroom/id/3811363>.

GORDON, Michael and MARCHESINI, Kathryn. Examples of Cloud Computing Services [online]. 2010. Available at: <http://www.unc.edu/courses/2010spring/law/357c/001/cloudcomputing/examples.html>.

HARVEY, Kate. The Future is XaaS: What you need to know about Everything-as-a-service [online]. 7 February 2017. Available at: <https://www.chargify.com/blog/xaas-everything-as-a-service/>.

HON, Kuan W. GDPR: Killing cloud quickly? [online]. March 17, 2016. Available at: <https://iapp.org/news/a/gdpr-killing-cloud-quickly/>.

HON, Kuan W. Update E-Commerce Directive to address imbalance in GDPR liabilities for infrastructure cloud providers, says expert [online]. 3 October 2016. Available at: <https://www.out-law.com/en/articles/2016/september/update-e-commerce-directive-to-address-imbalance-in-gdpr-liabilities-for-infrastructure-cloud-providers-says-expert/>.

KOTULA, Marcin. IP addresses as personal data – the CJEU's judgment in C-582/14 Breyer [online]. Available at: <http://eulawanalysis.blogspot.cz/2017/01/ip-addresses-as-personal-data-cjeus.html>.

LARSON, Selena. Supreme Court to hear high-stakes Microsoft case testing email privacy [online]. 25 February 2018. Available at: <http://money.cnn.com/2018/02/25/technology/microsoft-us-supreme-court-data-sharing/index.html>.

LEONARD, John. The right to erasure is the top GDPR compliance concern [online]. 22 May 2017. Available at: <https://www.computing.co.uk/ctg/analysis/3010528/the-right-of-erasure-is-the-top-gdpr-compliance-concern>.

LOSHIN, Peter, COBB, Michael, BAUCHLE, Robert, HAZEN, Fred, LUND, John, OAKLEY, Gabe, RUNDATZ, Frank. Encryption [online]. Available at: <http://searchsecurity.techtarget.com/definition/encryption>.

MCLELLAN, Charles. XaaS: Why 'everything' is now a service [online]. 1 November 2017. Available at: <http://www.zdnet.com/article/xaas-why-everything-is-now-a-service/>.

MEYER, David. European Commission, experts uneasy over WP29 data portability interpretation [online]. Available at: <https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1/>.

Modernization of Convention 108 (CAHDATA). *Council of Europe* [online]. Available at: <https://www.coe.int/en/web/data-protection/convention108/modernisation>.

MOEREL, Lokke. The data transfer regime for processors does not make sense and requires clarification [online]. 9 June 2016. Available at: <https://iapp.org/news/a/gdpr-conundrums-data-transfer/>.

NOVET, Jordan. Apple confirms it uses Google's cloud for iCloud [online]. 26 February 2018. Available at: < https://www.cnbc.com/2018/02/26/apple-confirms-it-uses-google-cloud-for-icloud.html>.

O'DONOGHUE, Cynthia, O'BRIEN, John. CJEU rules Digital Rights Ireland's Privacy Shield invalidation action inadmissible [online]. 8 December 2017. Available at: <https://www.technologylawdispatch.com/2017/12/privacy-data-protection/cjeu-rules-digital-rights-irelands-privacy-shield-invalidation-action-inadmissible/>.

ORME, Joe. ECJ determines that exam scripts and examiner comments are personal data [online]. 21 December 2017. Available at: <https://www.lexology.com/library/detail.aspx?g=41928c90-2435-403d-9c04-e04d8b051e28>.

PEERS, Steve. The CJEU's Google Spain judgment: failing to balance privacy and freedom of expression [online]. 13 May 2014. Available at: <http://eulawanalysis.blogspot.cz/2014/05/the-cjeus-google-spain-judgment-failing.html>.

PEERS, Steve. 'The Right to be Forgotten': The future EU legislation takes shape [online]. 23 September 2014. Available at: <http://eulawanalysis.blogspot.cz/search?q=right+to+erasure>.

Press Release: "One year EU Cloud Code of Conduct & 100 Days to go to GDPR" [online]. Available at: < https://eucoc.cloud/en/detail/news/press-release-one-year-eu-cloud-code-of-conduct-100-days-to-go-to-gdpr.html>.

Press release: Locating customer data will be half the battle to fulfill EU GDPR's 'right to be forgotten' [online]. Available at: <https://www.blancco.com/press-releases/locating-customer-data-will-half-battle-fulfill-eu-gdprs-right-forgotten/>.

Redhat. Understanding virtualization [online]. Available at: <https://www.redhat.com/en/topics/virtualization>.

REDING, Viviane. The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age [online]. SPEECH/12/26. Available at: <http://europa.eu/rapid/press-release_SPEECH-12-26_cs.htm>.

RUBIN, Ludo. Five ways European Data Privacy regulations will disrupt Online Video and OTT Businesses [online]. Available at: <https://bit.ly/2qTksF9>.

SMITH, Brad. US Supreme Court will hear petition to review Microsoft search warrant case while momentum to modernize the law continues in Congress [online]. 16 October 2017. Available at: <https://blogs.microsoft.com/on-the-issues/2017/10/16/us-supreme-court-will-hear-petition-to-review-microsoft-search-warrant-case-while-momentum-to-modernize-the-law-continues-in-congress/>.

STROUD, Forrest. Everything-as-a-Service (XaaS) [online]. Available at: <https://www.webopedia.com/TERM/E/everything-as-a-service_xaas.html?relatedterms>.

STUPP, Catherine. Commission conducting review of all foreign data transfer deals [online]. Available at: <https://www.euractiv.com/section/data-protection/news/commission-conducting-review-of-all-foreign-data-transfer-deals/>.

STUPP, Catherine. EU privacy watchdog: Privacy shield should be temporary [online]. 3 August 2018. Available at: <https://www.euractiv.com/section/data-protection/interview/eu-privacy-watchdog-privacy-shield-should-be-temporary/>.

TURNER, Paul. Fuhgettaboutit: the GDPR "Right to Erasure" [online]. 1 November 2017. Available at: < https://www.scality.com/blog/fuhgettaboutit-the-gdpr-right-to-erasure/>.

WOODS, Lorna. Bringing Data Protection Home? The CJEU rules on data protection law and home *CCTV* [online]. In: <www.eulawanalysis.blogspot.cz>. Available at: <http://eulawanalysis.blogspot.cz/2014/12/bringing-data-protection-home-cjeu.html>.

WES, Matt. Looking to comply with GDPR? Here's a primer on anonymization and pseudonymization [online]. 25 April 2017. Available at: <https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/>.

General Data Protection Regulation: Challenges for the Cloud

Abstract

This thesis recognizes and analyses some of the fundamental challenges that the General Data Protection Regulation poses for cloud computing. Its aim is to answer the question whether the GDPR can be regarded as cloud friendly. The hypothesis that is proposed and tested is that it cannot be, since it includes concepts and wording that are impractical in cloud computing. This is assessed based on how different cloud computing services function. The thesis therefore lays down foundations of both legal and technical understanding of the data protection in the cloud in the first chapters. The analysis of the challenges then builds on this knowledge. The challenges of the GDPR for the cloud are divided into five groups. Firstly, what is regulated as personal data in the cloud is consider with regard to the concepts of anonymisation, pseudonymisation and encryption. Secondly, controller – processor relationship and their obligations in the complex cloud environment are deconstructed. The issues concerning distinguishing between the controller and the processor in the cloud, new specific obligations of cloud service providers who act as processors and compulsory provisions of the data processing agreements, which do not make sense in the cloud are highlighted. The concepts of data protection by design and by default are also dealt with. Thirdly, the most relevant rights of the data subjects in the cloud are analyzed. These are the right to erasure and the right to data portability. Another challenge recognized concerns the emphasis that the GDPR puts on transparency principle and how that forces even SaaS service providers to uncover layers of cloud computing to the data subjects. Lastly, aspects of extraterritoriality and international transfers relevant in the cloud are acknowledged. The thesis then ascertains whether cloud codes of conduct, the emergence of which the GDPR presumes, can help to tackle the recognizes issues and concludes with the discussion on whether the GDPR is cloud friendly based on the analysis provided.

Key words: GDPR, cloud, data protection

Obecné nařízení o ochraně osobních údajů: výzvy pro cloud

Abstrakt

Tato diplomová práce identifikuje a analyzuje vybrané výzvy, které Obecné nařízení o ochraně osobních údajů představuje pro oblast cloud computingu. Jejím cílem je odpovědět na otázku, jestli může být GDPR považováno za přívětivé pro cloud. Navržená a testovaná hypotéza je, že nemůže, neboť obsahuje instituty a formulace, které jsou v praxi cloud computingu nerealistické. Toto je hodnoceno s ohledem na to, jak odlišné cloudové služby fungují. Diplomová práce proto ve svých prvních kapitolách poskytuje právní i technické základy, na jejichž znalosti poté analýza výzev staví. Výzvy GDPR pro cloud jsou rozděleny do pěti hlavních skupin. Nejprve je řešeno, co je regulováno jako osobní údaje v cloudu, a to s ohledem na anonymizaci, pseudonymizaci a šifrování. Poté je kriticky rozebrán vztah mezi správci a zpracovateli ve složitém cloudovém prostředí. Jsou zdůrazněny otázky týkající se rozlišení mezi správci a zpracovateli v cloudu, nových povinností poskytovatelů cloudových služeb, kteří vystupují jako zpracovatelé a povinných ujednání smluv mezi zpracovateli a správci, které nedávají v cloudu smysl. Taktéž je pojednáno o záměrné a standardní ochraně osobních údajů. Dále jsou analyzována práva subjektů ochrany osobních údajů nejvýznamnější v kontextu cloudu. Těmi jsou právo na výmaz a právo na přenositelnost údajů. Další výzvou, která je rozpoznána, je důraz, který GDPR klade na zásadu transparentnosti. Tato zásada nutí dokonce i poskytovatele SaaS služeb odhalit vrstvy poskytování služby subjektům údajů. Nakonec jsou uváženy pro cloud významné aspekty extrateritoriality GDPR a předávání osobních údajů do zahraničí. Diplomová práce poté zvažuje, zda cloudové kodexy chování, jejichž vznik GDPR předpokládá, mohou pomoci vyřešit rozpoznané problémy a je uzavřena diskuzí, zda GDPR může na základě provedené analýzy být považováno za přívětivé pro cloud.

Klíčová slova: GDPR, cloud, ochrana osobních údajů