TALLINN UNIVERSITY OF TECHNOLOGY

School of Business and Governance

Department of Law

Anastassiya Platonova

DATA PRIVACY REGIME AND CONFIDENTIALITY REQUIREMENTS WITH REGARDS TO USING CLOUD TECHNOLOGY BY LAW FIRMS

Master's Thesis

Programme HAJM, specialisation Law and Technology

Supervisor: Kari Käsper

Tallinn 2019

I declare that the I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is ..... words from the introduction to the end of conclusion.

Anastassiya Platonova .....
(signature, date)

Student code: 177302HAJM
Student e-mail address: platonova.anastassiya@gmail.com

Supervisor: Kari Käsper, MA:
The paper conforms to requirements in force

.....

(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

.....

(name, signature, date)

Abstract

This paper aims to assess the impact of cloud use on the compliance of legal professionals with the requirements of professional secrecy and data protection regime. The hypothesis that was proposed in this paper is that use of the cloud storage and online cloud-based tools by law firms in the course of their work for the purposes of storing documentation wholly or partially compromises the data rights and freedoms of their clients and undermines the confidentiality between a legal professional and a client.

In order to evaluate the hypothesis, an analysis of the relevant legislative framework, including guidelines by regulatory bodies, was carried out with the support of relevant academic sources, as well as an assessment of current situation with regard to cloud use by law firms, to the extent that it is possible, and interpretative legal approach is used to predict potential application of an existing framework to the analysed situation.

As a result, the paper concludes that the hypothesis is true and that the risk presented by cloud computing may be mitigated but not eliminated. Further, the paper proposes splitting the guidelines on the matter in several parts in order to provide more clarity and be able to update them with ease and give clear, regularly updated guidelines on technical aspects of compliance.

Keywords: data protection, legal professional privilege, professional secrecy, confidentiality, cloud

Table of contents

Introduction

It is impossible to deny that the information technology seeps into more and more aspects of the daily life of most people, from online banking and e-governance services to using VPN to watch a favorite TV-show. The same is true for the most professional sectors as well – the application of the information technology becomes more and more integral for the professional activities among different sectors, including medicine[1], education[2] and service[3]. Legal sector tends to be more conservative with regards to most novelties,[4] but it is still starting to employ more complex information technology in the daily activities, albeit the process is going with varying speed depending on the region.[5]

Cloud data storage and other cloud services are becoming virtually omnipresent, despite the associated risks, due to the convenience of use.[6] Additionally, it is much cheaper to use third party storage, email service and so on, than construct a separate server, especially for the SMEs and non-technology-oriented businesses[7]. Cloud computing is still relatively fresh in the age of fast-paced technology growth and have just started to be applied by some legal firms. Some go much further than others and attempt to go completely paperless by relying on the cloud.[8] Ironically, both sides of the debate attempt to explain away their positions by arguing that it ensures better security.[9] Additionally, it has to be said that no legal firm exists in a vacuum and has to adhere to the necessary regulation as well as co-exist and cooperate with the law enforcement and the state administration, which sometimes imposes certain limitations on technology usage in daily activities. It is not always possible to send a cloud link to a state authority and have it accepted. This is always the case for the new technology and is even more strict for a regulated profession.

---

[1] D'Amore, F., Pirone, F (2018) Doctor 2.0. and i-Patient: information technology in medicine and its influence on the physician-patient relationship. – *Italian Journal of Medicine*, Vol. 12, No. 1, 1.
[2] Gibson, D.. et al (2018) Evolving Learning Paradigms: Re-Setting Baselines and Collection Methods of Information and Communication Technology in Education Statistics. – *Educational Technology and Society*, Vol 21, No. 2, 62.
[3] Drotsky, G.A.P. et al (2005) The influence of information and communication technology on the selling activities of the professional sales representative. – *Acta Commercii*, Vol. 5, No. 1, 97.
[4] Lim, R. (2017) *Cultivating Innovation in risk-averse legal industry.* Accessible: http://insight.thomsonreuters.com.au/posts/innovation-risk-averse-legal-industry, 5 May 2019.
[5] Cohen, M.A. (2017) *Global Legal Tech is Transforming Service Delivery.* Accessible: https://www.forbes.com/sites/markcohen1/2017/08/29/global-legal-tech-is-transforming-service-delivery/#57e0ac811346, 5 May 2019.
[6] Columbus, L. (2017) *2017 State of Cloud Adoption and Security.* Accessible: https://www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoption-and-security/, 5 May 2019.
[7] Kennedy, D. (2019) *Techreport 2018: Cloud computing.* Accessible: https://www.lawtechnologytoday.org/2019/01/techreport-2018-cloud-computing/, 5 May 2019.
[8] Dimka, D. (2016) *The Zero-Paper Law Firm - The Ultimate Guide to Going Paperless.* Accessible: https://uptimelegalworks.com/resources#ebooks, 8 October 2018.
[9] King, N.J., Raja, V.T. (2012) Protecting the privacy and security of sensitive customer data in the cloud. - *Computer law and security review*, Vol. 28, 309-310.

That poses a question – as legal professionals often have control over sensitive and personal information and as such have to comply with the data protection legislation and as legal firms also have an additional layer of scrutiny imposed onto them by the professional regulations, the confidentiality requirements and, where applicable, the client-attorney privilege, then how is usage of information technology in the daily work of legal professionals affected by such regulations?

On 25 May 2017 new Data Protection Regulation entered in force in Europe. It has imposed more stringent requirements on the data processors and the data controllers as well as expanded the rights of the data subjects. Last two years have seemingly passed under the sign of the GDPR compliance for many businesses and, undoubtedly, legal offices. However, legal firms have additional requirements imposed on them by the professional regulations with regards to confidentiality. In combination, increase in use of the information technology, particularly, cloud computing, in the daily professional activities and the new data protection regulation provide ample food for thought with regards to the compliance with the professional regulations for the legal sphere.

This work will attempt to conduct an analysis on how secure the cloud computing actually is and what requirements, standards and principles are to be applied to law firms in the use of the cloud computing. In order to do so, the following hypothesis is proposed: use of the cloud storage and online cloud-based tools by law firms in the course of their work for the purposes of storing documentation wholly or partially compromises the data rights and freedoms of their clients and undermines the confidentiality between a legal professional and a client.

The appropriate methodology for this research is a combination of empirical research and interpretative logical approach. Empirical research for the purposes of the paper will be expressed through the analysis of relevant legislation and soft law with supporting scholarly and academic sources and additional use of several sources from the technological field in order to ascertain the technological aspects of security. Interpretative logical approach will be necessary in order to predict the application of general law in the new situation that had arisen.

The scope is to be limited territorially to the EU, the areas of law being researched are the data protection and the professional regulation for legal professionals. American approach and ethical guidelines of Bar Associations of US states will be used for comparison and for the purposes of addressing cross-border issues that might arise for European law firms, as New York Bar had

addressed the issues of the data protection in using the cloud storage solutions by law firms back in 2010 and there is already case law in USA on the confidentiality and client-attorney privilege connected to use of cloud storage use by law firms.

The paper is structured in a following manner: first part on the use of the cloud technology in the daily activities of law firms, second part on the principles and the guidelines that apply to client-attorney relationship that would be relevant in case if clients' personal data is stored or otherwise processed, third part on data protection regime in Europe and how it applies to legal professionals in their daily professional activities, fourth part will concentrate on liability of the parties involved and fifth part that will set out possible recommendations and factors to be taken into account as a conclusion for the research including an evaluation of existing legal framework with regards to its application to cloud-based technology that is involved in everyday professional activities.

It is crucial to analyze the circumstances in an appropriate manner and conclude what is the best way to utilize technology in the legal field as the information provided to legal professionals can be extremely sensitive and can even be likened in that respect to that of medical data. In order to do so, an appropriate and thorough risk assessment is necessary to conduct. That risk assessment should include not only the risks, that are associated with the technology itself, but also the procedures related to the use of that technology and possibilities to implement additional safeguards against such general risk factors such as the human factor. This paper aims to address current state of the treatment of the cloud technology in legal sector, how are associated risks assessed and what are the recommendations from the sector itself and the relevant authorities with regards to addressing those risks.

1.Cloud And Law Firms

1.1.Use of the Cloud Technology in Law Firms

It is important to clarify that a cloud in the context of the cloud based technology refers to the storage space on the servers of the company providing the service, where the data is stored in the course of using the service, instead of storing the data directly on the device of the user of the service, whereas cloud-based technology is any technology that utilizes a cloud, therefore not only services that are used primarily for storing data are considered cloud-based technology.[10] This explanation is very simplistic, but nevertheless sufficient for the purposes of this paper. It is not of essence whether the service itself is cloud-based or cloud is a dedicated data storage such as Google Drive or Dropbox, as the same method is used, and core risks associated with the method itself will remain the same. However, when the risk assessment is conducted for the cloud storage and cloud-based technology, other associated risks may differ, therefore it is important to not equate dedicated cloud storage and cloud-based technology completely.

Cloud-based technology is present in the everyday life of many people, such services as Google, Amazon, Evernote, Facebook are cloud-based, as those services run directly from the servers of their respective companies. However, in order to speak of the issues connected to the use of cloud technology by legal professionals in the course of their professional activities, it is necessary to establish that such use indeed takes place and is spreading, if not already wide-spread.

In Europe, attention to the topic of usage of technology by legal professionals was given later than in United States, which can be easily observed from such facts that the statistics on usage of the cloud technology by legal professionals in European countries is lacking, whereas such a statistic is present for some states in USA[11], that opinion of the ethics committee on the use of cloud technology by lawyers was issued in 2010 by the New York State Bar Association[12], whereas similar guidelines were only issued by the Council of Bars and Law Societies of Europe (CCBE hereinafter) two years later[13]. Therefore, other types of evidence ought to be relied on in order to

[10] Graham, G. (2012) Lost in a Cloud: Overview of the legal obstacles to the growth of cloud computing. – Medijska Istrazivanja, Vol. 18, No. 2, 23-24.
[11] Black, N. (2017) *Significantly more lawyers using cloud computing in 2017*. Accessible: http://www.legalnews.com/washtenaw/1449844, 16 March 2019.
[12] Committee on professional ethics of New York State Bar Association (2010) *Opinion 842*. Accessible: http://www.nysba.org/CustomTemplates/Content.aspx?id=1499, 16 March 2019.
[13] Council of Bars and Law Societies of Europe (2012) CCBE Guidelines On The Use Of Cloud Computing Services By Lawyers. Brussels: CCBE.

establish that a significant number of legal professionals uses cloud in the course of their professional activities.

An abundance of successful legal tech products, that rely on cloud-technology, would serve as proof that a significant number of legal professionals employ cloud technology in the course of their professional activities. One of such products is Clio, which provides a platform akin to a one-stop shop for addressing needs of a law firm, from billable hours tracking solutions to Office365 and Dropbox, through integration of those solutions.[14] This platform has been approved by 65 bar associations and law societies around the world and has a 150 000 strong customer base of legal professionals that use services provided through the platform in their daily activities.[15] Even prominent Estonian legal tech project such as Avokaado also relies on the use of a cloud technology to an extent.

Trends observed by the professionals in the field seem to show that SME law firms are more enthusiastic about adopting technology in general and cloud computing in particular.[16] In last several years CCBE has also issued a number of various guidelines related to the use of technology by lawyers, such as the guidelines on use of online legal platforms by lawyers and the use of cloud technology by lawyers.[17] That goes to show that the use of cloud computing is wide-spread enough for a slow European institution to catch on.

Moreover, cloud-based technology is not necessarily involved in all legal tech projects, but it may be involved with satellite services used by a law firm such as e-mail service, long-term and short-term data storage, time tracking, note-taking and so forth. Each law firm uses email, but the cost of supporting their own email service with their own server is just too high, therefore, a prevalent majority will rely on third party services of varying size and security. Most of the email services are actually cloud based. Outlook or Gmail can be opened from any device and all received and sent emails will be visible as they are stored on the servers of a respective company. Thus, in the majority of cases where a law firm uses an outside email service, it would use a cloud-based

[14] Clio (2019) *About Clio*. Accessible*:* https://www.clio.com/eu/, 16 March 2019.
[15] Clio (2019) *About Clio.* Accessible: https://www.linkedin.com/company/clio---cloud-based-legal-technology/about/, 5 May 2019.
[16] Szabo, O. (2017) *The status of legal tech in Central Eastern Europe: 2017 in Retrospective*. Accessible" https://investcee.hu/status-of-legaltech-in-central-eastern-europe/ , 16 March 019; Clio (2017) *Why Law Firms are moving to the cloud.* Accessible: http://www.nysba.org/WorkArea/DownloadAsset.aspx?id=78979, 16 March 2019.
[17] Council of Bars and Law Societies of Europe (2012) CCBE Guidelines On The Use Of Cloud Computing Services By Lawyers. Brussels: CCBE.; Council of Bars and Law Societies of Europe (2018) CCBE Guide On Lawyers' Use Of Online Legal Platforms. Brussels: CCBE.

technology. Interestingly enough, security of email with regards to client data confidentiality and legal professional privilege had been a concern since the first days of Internet.[18]

Additionally, considerations and preferences of the clients are to be taken into account. Client base of legal firms may vary. Depending on the age and location, where possible, clients may prefer to use cloud in order to present documentation to a lawyer, either through a link to a cloud storage service or as a direct attachment to the email. Thus, in some circumstances, using a cloud service could be a necessity, although there are still some law firms that refuse to accept any information or documentation communicated or transferred digitally.

It is important to establish which kinds of cloud-technology are used by legal professional due to the fact that different types of data would be involved. Major concern is connected with the personal data of the clients, as while other types of data may be important from other standpoints, personal data has a special protection regime in EU. From that point of view, sharing the data between the client and a lawyer or a law firm, between the lawyers of the same company in the course of professional activities, between lawyers of different companies, between lawyers and officials and data storage of the law company seem to be connected with additional risks in respect of personal data. As such, email and direct data storage cloud services seem to be mainly connected with personal data risks, as well as likely most employed by law firms.

1.2.Security

The argument of security is invoked by the both sides of the dialogue on using cloud-technology in the professional activities of the law firm. Several of the key arguments that pro-cloud use parties normally invoke are that professional software as a service providers are more equipped to address technical security compliance and specific security activities than any other in-house solution, cloud storage provides for easy data recoverability and may be superior in terms of data back-up and recovery techniques.[19] At the same time arguments against the cloud that refer to security aspect are possibility of data leaks from big platforms that are likely to be targeted, less control over data, openness to data interception, sharing data with other unknown customer.[20] In other words, the conversation on the security aspect of cloud computing is ongoing and each

[18] Masur, M.J. (1999) Safety in Numbers: Revisiting the Risks to Client Confidences and Attorney-Client Privilege Posed by Internet Electronic Mail. - Berkeley Technology Law Journal, Vol. 14, No. 3, 1119-1120.
[19] King, N.J., Raja, V.T. (2012) *supra nota*, 309-310.
[20] *Ibid*, 309.

company has to choose whether to take that leap of faith based on their level of education in the field, experience and circumstance.

In the meantime, there are some measures employed by the law firms or really any other firms with high confidentiality related risks, for example, a need to protect trade secrets. Those practices are often based on the recommendations of the cloud-based platforms themselves,[21] and can roughly be separated in three categories: access, preparation and technical measures. From the technical perspective, it is recommended to keep all involved applications up-to date and use data encryption to ensure data confidentiality. With regards to the preparation, those measures range from the employee training to the software vulnerability testing and the crisis management protocols, as they are aimed to cover known risk factors. Access related measures restrict who can use the service and to what extent, monitor how and when the service is used. As to whether such measures are sufficient in order to prevent the security risks posed by technology itself is to be addressed at the conclusion of this paper.

It is not possible to create an absolute defense for something from a technological perspective, nor is it possible to predict the effect of the human factor completely. The purpose of this section is to merely highlight the issue, as it is at the heart of the debate on legal compliance and technology usage. The most that can be done is to use an optimal combination of methods that is available and not excessively burdensome in a particular situation and the purpose of this paper is concluded in describing and evaluating existing the framework and the guidelines in which cloud use by legal professionals has to fit.

Specific technological solutions of the cloud computing are not at the core of the concerns of the potential users of the cloud-services, as many vulnerabilities that stem from those solutions are shared with other services and devices, example being Spectre and Meltdown vulnerabilities present in a fair amount of Intel processors, potential DDoS attacks and vulnerabilities in programming interface. Those risks will always be present in using a computer and Internet services, which cannot be avoided at this point in daily professional activities of a legal professionals. There are undoubtedly exploits that come with using a cloud service specifically, but there are already severe and unavoidable technology-based risks present in the law office. How much more severe would it be to add the risk of cloud specific exploits? Which exploits in the essential devices had not been yet patched up? Nevertheless, the subject is an important one in a

[21] Litify (2017) *10 Cloud Security Best Practices For Attorneys and Law Firms.* Accessible: https://www.litify.com/10-cloud-security-best-practices-attorneys-law-firms/, 16 March 2019.

technical sphere, prompting a number of new and improved solutions[22], but technological development is akin to an arms race between malicious parties and security professionals. Moreover, technical specialists in the field hold the opinion that cloud computing is not yet complete and fully recognize the flaws of the technology.[23]

Some guidance on the balancing of the technological risks with regards to data can be derived from security requirements laid out in the GDPR. However, for the sake of not becoming outdated quickly, the obligations for data controllers and processors with regards to data security laid out in the Article 32 of the GDPR are nevertheless vague. The obligations laid out in the aforementioned article can be summarized in the following: best available solutions are to be used and to be regularly updated, personal data is to be anonymized and encrypted, processes for testing the system and incident response are to be developed, measures are to be taken to prevent processing other than by requirement of the law and request of data controller or processor themselves, recoverability of the data and data access is to be ensured, processing systems and services must possess 'ongoing confidentiality, integrity, availability and resilience'[24]. In other words, the GDPR requires 'appropriate'[25] security measures to be implemented without establishing a specific threshold or specific measures to be implemented, taking a risk-based approach.

1.3.Current Guidelines On Cloud Use By Law Firms

The two main sets of guidelines that are important to highlight in this section are the guidelines from the New York State Bar Association and guidelines from the Council of Bars and Law Societies in Europe. The former were one of the earliest guidelines on the matter and would also be beneficial to evaluate in order to better understand transborder data flow and cross-border data disclosure that will be covered later in this paper, the latter are more relevant for the scope of this paper, as the European legislation is at the focus. It also possible to note that the existence of those guidelines highlights that the usage of the cloud computing by legal professionals is a special circumstance, as regulatory bodies of the industry had issued special guidance on the matter.

[22] Jayapandian, N. et al (2016) Improved Cloud Security Trust on Client Side Data Encryption using HASBE and Blowfish. - *Green Engineering and Technologies*, Coimbatore, India, 19 November 2016.
[23] Ahmed, H. et al (2016) Data security issues in cloud computing: review. – *International Journal of Software Engineering and Computer Systems*, Vol 2, 63.
[24] Regulation (EU) No 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, 4.5.2016, p 1-88 4.5.2016, art. 32, p 1(b).
[25] *Ibid*, art. 32, p 1,2.

As the opinion of the Committee on professional ethics of New York State Bar Association is an earlier document, as it is dated 10 of September of 2010, it will be discussed first. It concentrates on the storage of client's confidential information that uses an online storage provider.[26] Through evaluating existing guidelines on confidentiality, the guidelines conclude that 'a lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure confidentiality in maintained in the manner consistent with the lawyer's obligations'.[27] In order to maintain confidentiality and comply with such obligations, the guidelines recommend the following:

- to ensure that online data storage provider itself has an obligation to preserve confidentiality and security of data and will make a notification if it is required to produce the data,
- to ensure that the security measures, policies, recoverability methods and other procedures are 'adequate under the circumstances',
- to use the available technology in order to prevent compromising of the data,
- to make sure that the service provider is capable of wiping the data and any of its copies if need be.[28]

These recommendations are aimed to help the legal professional exercise control in choosing the best suitable service provider and to provide guidance as to what aspects of the matter are to be closely monitored. It specifically avoids naming specific technologies and methods due to the unpredictable and rapid development of technology and this approach had paid off in that respect, as the guidelines will still be relevant today. However, with regards to the obligations, its main focus is the confidentiality obligation. Additionally, the NYSBA guidelines are rather narrow and do not portray the full picture of the subject-matter, concentrating specifically on answering the posed question without evaluating different outcomes and alternatives.

European guidelines on the matter were not far behind. The CCBE Guidelines on the use of cloud computing services by lawyers from 7 September 2012 are less general and evaluate compliance with data protection legislation in addition to the professional secrecy requirements. These guidelines are very well structured and present a well-rounded overview of the matter, as the main

[26] Committee on professional ethics of New York State Bar Association (2010) *Opinion 842*. Accessible: http://www.nysba.org/CustomTemplates/Content.aspx?id=1499, 16.03.2019.
[27] *Ibid.*
[28] *Ibid.*

aim is to highlight the risks connected with cloud computing. It needs to be highlighted, that guidelines of CCBE are mainly targeting the law societies and bar associations in Europe rather than individual lawyers themselves, but, as this paper concentrates on European legislation and European jurisprudence, it is more suitable to evaluate guidelines provided by CCBE, especially as it would likely be a frame of reference for guidelines issued by law societies and bar associations in European countries.

In their guidelines CCBE acknowledge the benefits that cloud computing may present for a legal practitioner but present a very detailed risk evaluation. Concerns highlighted by the guidelines include data ownership, long-arm foreign legislation and guidelines, data recoverability and back up and policies of the service provider with regards to data storage, data destruction and data security.[29] The following is the summarized recommendations of CCBE with regards to usage of cloud computing services: a legal professional must carry out appropriate due diligence on a service provider, evaluate type of the data to be stored, assess the in-house security measures, evaluate whether the risks will increase or decrease with the use of cloud service, evaluate capabilities of recovering the data from the service provider and take al contractual precautions.[30] The CCBE also recommend informing the clients that law firm uses the cloud storage for the sake of transparency.[31] In conclusion, the CCBE takes a cautious approach and recommends a legal professional to carry out an individual risk assessment in order to determine whether use of a cloud data storage would be appropriate. It seems to be a well-rounded recommendation that although it does not offer entirely new solutions and highlights the factors that are not only connected with the new service but also issues that may arise in the client relationship and in-house aspects of security processes.

Despite a different approach to the subject matter, both those sets of guidelines have nevertheless one thing in common – they are over five years old. In that time a more stringent data protection regime in Europe had taken hold. Therefore, a certain re-evaluation of the guidelines is in order.

[29] Council of Bars and Law Societies of Europe (2012) CCBE Guidelines On The Use Of Cloud Computing Services By Lawyers. Brussels: CCBE.
[30] *Ibid.*
[31] *Ibid.*

2.Client-Attorney Relationship – Principles And Guidelines

2.1.Attorney-Client Privilege And Confidentiality In EU

Attorney-client privilege also known as legal professional privilege is usually understood as special level of protection from seizure awarded to communications by a client with a legal professional in his or her professional capacity for the purpose of giving advice and protecting the rights of the client.[32] Firstly, a few words on the sources of the legal professional privilege in Europe. It is possible to outline at least three sources on the limits and extent of the legal professional privilege when it comes to EU Member states: domestic legislation and guidelines, ECHR jurisprudence and EU jurisprudence.

Domestic legislation among the Member states varies with regards to the requirements for the legal practitioners possess the legal professional privilege and limits of it. For example: 12 countries provide legal professional privilege to in-house counsel, 12 countries do not and the issue is unclear for 3 countries.[33] Other differentiating issues include what kinds of communications are privileged, term of the privilege, circumstances in which privilege may be waived and components of the privilege.[34] Components of the legal professional privilege directly provided in the law may include the duty of confidentiality, the right to refuse to testify and the right to refuse to give evidence on the matters which have been confided to the legal practitioner in his or her professional capacity, those elements may also be provided in the satellite legislation on the matter.[35]

With regards to ECHR protection awarded to the legal professional privilege, it is not expressly provided in the European Convention on Human Rights, but ECHR jurisprudence had developed right to private life by including legal professional privilege under its umbrella.[36] Under ECHR jurisprudence legal professional privilege had also been protected under the right to fair trial, as it is an 'indispensable guarantee' of the right to fair trial.[37]

[32] Murphy, G.(2009) Is it time to rebrand legal professional privilege in EC competition law? An updated look. – *Commonwealth Law Bulletin*, Vol. 35, No. 3, 443.
[33] Holtz, J. (2013) Legal professional privilege in Europe: a missed policy opportunity. – Journal of European *Competition Law&Practice*, Vol. 4, No. 5, 404.
[34] Eva, E. (2015) Lawyers' legal professional privilege in Europe. – *Practical application of Science*, Vol. 3, No 1(7), 34-37.
[35] *Ibid,* 34-37.
[36] *Ibid*, 34.
[37] *Ibid*, 34.

On the European level, respect to confidentiality and professional secrecy is one of the core principles of CCBE Code of Conduct for lawyers.[38] As to the state of EU jurisprudence on legal professional privilege, the situation is often described as dire due to *Akzo* decision and prior jurisprudence of *AM&S*, which had excluded in-house lawyers from professional secrecy due to the principle of independence.[39] Some take a position that this reasoning is flawed, as both in-house and outside counsel have employment relations with the client, unless it is pro bono or voluntary work, in-house and outside counsel are otherwise in the same position and must uphold the same professional standards of ethics and practice.[40] In any case, there are calls to adopt a more precise scope of legal professional privilege that would emphasize commonalities, reconcile differences and prevent professional secrecy from becoming extinct both in EU jurisprudence[41] and ECHR jurisprudence[42]. It is an issue not only on the international level, but on domestic level as well, as new legislation on surveillance and interception of communications at times omits to provide exceptions and protection for professional secrecy, one example of such being British Regulation of Investigatory Powers Act 2000.[43]

To conclude, confidentiality principle in European jurisprudence is an integral part of conduct for legal professionals, existence of which plays no small part in ensuring protection of right to private life and right to fair trial, but at the moment it is going through a critical point due to the direction of development of jurisprudence and legislation in Europe.

2.2.Council Of Bars And Law Societies In Europe – Relevant Guidelines

The CCBE provides several documents that explain European approach to legal professional privilege and confidentiality. The main document is Charter on Core Principles of European legal profession and Code of Conduct for European Lawyers, which are supplemented by commentary and explanatory memorandum respectively. In those documents CCBE establishes legal professional privilege as one of the core principles of legal profession in Europe. In understanding of the CCBE, it is not only the duty of a lawyer but also a human right of the client.[44] The Code

[38] CCBE (2013) Charter of core principles of the European legal profession and Code of conduct for European lawyers. Brussels: CCBE.
[39] Holtz, J. (2013) *supra nota*, 412.
[40] Murphy, G.(2009) *supra nota*, 455.
[41] *Ibid*, 460.
[42] Eva, E. (2015*) supra nota*, 37.
[43] Webley, L. (2016) Interception of communications and legal professional privilege and the rule of law. – *Legal ethics*, Vol. 19, No. 1, 174.
[44] CCBE (2013) Charter of core principles of the European legal profession and Code of conduct for European lawyers. Brussels: CCBE.

of Conduct for European Lawyers in a designated section on confidentiality establishes the duty to keep all information received in the course of his or her professional activities, that is not limited in time and extends to the staff and employees of the legal professional.[45]

The CCBE also issued a dedicated statement on legal professional privilege due to reported infringements of the privilege by the state authorities through calling upon legal professionals in tackling tax and administrative issues, considering lawyers as accomplices to their clients and trespassing against legal professional privilege in order to tackle organized crime and terrorist activity.[46] The purpose of the statement was to once again underline that the core of the legal professional privilege is protection of the client and right to fair trial, as there can be no adequate advice without knowing the full picture and there can be no full picture without trust.[47]

This issue is especially important to mention in the light of recent trespasses against the legal professional privilege for the advantage of the governmental surveillance and interception of communication, as it can not be excluded that in outsourcing data storage, service providers may be called upon by the supervisory or law enforcement authorities to provide evidence. As it is an obligation of a legal professional to safeguard against making confidential information public – if the service provider chosen by a legal professional does not comply with necessary standards that it must comply with in order for a legal professional to store data with that provider, it is equivalent 'to leaving the file on the park bench'[48]. In connection to that CCBE had issued specialized guidelines "On protection of client confidentiality within the context of surveillance activities".[49] The purpose of this paper was to assist legislators and policy makers in addressing legal professional privilege with regards to legislative process on surveillance and policy making on surveillance respectively. Additionally, CCBE had also made several reports on the state of legal

[45] CCBE (2013) Charter of core principles of the European legal profession and Code of conduct for European lawyers. Brussels: CCBE.
[46]CCBE (2017) *CCBE Statement of professional secrecy/Legal professional privilege(LLP)*. Accessible: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_Postion_Papers/EN_DEON_20170915_Statement-on-professional-secrecy_LPP.pdf, 16 March 2019.
[47] *Ibid.*
[48] Harleysville Insurance Company v Holding Funeral Home Inc., No. 1:15 cv 00057, 2017 U.S. Dist. LEXIS 18714 (W.D. Va. Feb. 9, 2017).
[49] CCBE (2016) *CCBE Recommendations on the protection of client confidentiality within the context of surveillance activities.* Accessible: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20160428_CCBE_recommendations_on_the_protection_of_client_confidentiality_within_the_context_of_surveillance_activities.pdf, 16 March 2019.

professional privilege in Member states: Edwards report from 1976[50], update to Edwards report[51] and Fish report from 2004[52].

The aforementioned papers by CCBE are dedicated to the topic of legal professional privilege, but it is nevertheless covered also where it is needed to provide a better understanding of subject matter, example being the CCBE Guidelines on lawyers' use of online legal platforms and the CCBE Guidelines on the use of cloud computing services by lawyers that briefly address professional secrecy for better understanding of main subject-matter. It is possible to conclude on the basis of aforementioned, that the CCBE considers professional secrecy/legal professional privilege and confidentiality, as its integral part, as a very significant part for conduct of a legal professional in Europe.

2.3.EU Approach To Attorney-Client Privilege In The Context of The Cloud

Although ECJ had previously ruled on legal professional privilege and its limits in judgements such as *AM&S*, *Hilti*, *Akzo*, at the moment there is no dedicated ECJ jurisprudence on the matter of legal professional privilege in the cloud. It may be possible to rely on prior discussed CCBE guidelines on the matter in order to establish a European approach.

With regards to existing EU jurisprudence on the legal professional privilege in general, it applies to external, EEA qualified legal professionals,[53] extends to the documents confined to the text or contents of such advice[54] and to the preparatory documents that were drawn up for the purpose of obtaining advice or exercising the rights to defense[55]. The part where third-country legal professional privilege is not protected in the EU will undoubtedly be problematic for cross-border

[50]CCBE (1976) *The professional secret, confidentiality and legal professional privilege in the nine member states of the European community.* Accessible: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_Reports/EN_DEON_19761029_Edwards_report.pdf, 16 March 2019.
[51]CCBE (2003) *The professional secret, confidentiality and legal professional privilege in Europe.* Accessible: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_Reports/EN_DEON_20030930_Update_of_th_Edwards_report.pdf, 16 March 2019.
[52] CCBE (2004) *Regulated legal professionals and professional privilege within the European Union, the European Economic Area and Switzerland, and certain other European jurisdictions.* Accessible: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_Reports/EN_DEON_20040227_Fish_report.pdf, 16 March 2019.
[53] Court decision, 18.05.1982, AM & S Europe Limited v Commission of the European Communities, 155/79, ECLI:EU:C:1982:157.
[54] Court decision, 02.03.1994, Hilti AG v Commission of the European Communities, C-53/92 P, ECLI:EU:C:1994:77.
[55] Court decision, 14.09.2010, Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v European Commission, C-550/07, ECLI:EU:C:2010:512.

data disclosure and should be taken into account by third-country lawyers in their professional activities in the EU.[56] Another interesting point that would be useful to have a court opinion about the influence of the cloud computing on the confidentiality obligation. With regards to cloud technology, data transmission process takes place through the Internet and can be somewhat easily intercepted especially if appropriate measures are not adopted, which may lead to waiving the privilege altogether or disclosing confidential information and personal data.[57] American case *Harleysville Insurance Company v Holding Funeral Home Inc*. had ruled on the issue and had found that using insufficiently protected cloud service without taking appropriate precautions may lead to the waiving attorney-client privilege.[58]

This chapter had given a rather brief overview of regulations that surround attorney-client relationship and highlighted its importance in the European legal framework. Nevertheless, it can not be denied that EU jurisprudence on the matter had been subject to criticism. In that light, legal professionals should exercise great care with regards to professional secrecy and confidentiality requirements. It is also interesting to mention, that research on technical aspects of maintaining client data confidentiality in context of legal professional privilege had frequently been under evaluation, especially in the context of search and seizure and data erasure. Legal professionals are not always aware that it is not enough to dump a file into the 'Trash bin' to get rid of it and it lays a certain print on hard disc hygiene, which prompted IT forensic research on the topic, proposing a solution for data cherry-picking.[59]

However, European jurisprudence with regards to the legal professional privilege is contained in the area of competition law. Seemingly, the ECJ had to a certain extent avoiding addressing legal professional privilege on the EU level unless absolutely necessary, in part due to the complexity and variety of legal professional privilege from state to state. It is possible, that a spill-over effect may occur with regard to the interpretation of the legal professional privilege in the EU competition law for the purposes of consistency, if ECJ decides to address legal professional privilege in the context of other area of law than competition law. However, at the moment the reach of EU jurisprudence with regards to legal professional privilege is limited, one of the reasons

[56] Gonzales-Diaz, F.E., Stuart, P. (2017) Legal professional privilege under EU law: current issue. – *Competition law and policy debate*, Vol. 3, No. 3, 59.
[57] Joint, A., Baker, E., Eccles, E. (2009) Hey, you, get off that cloud? - *Computer law and security review*, Vol. 25, 273.
[58] Harleysville Insurance Company v Holding Funeral Home Inc., No. 1:15 cv 00057, 2017 U.S. Dist. LEXIS 18714 (W.D. Va. Feb. 9, 2017).
[59] Jiang, Z.L. et al (2013) Maintaining Hard Disk Integrity With Digital Legal Professional Privilege (LPP) Data. – *IEEE Transactions on Information Forensics and Security*, Vol. 8, No. 5, 827.

being the question of competence. Even though existing jurisprudence allows to map out the general approach, the details of the practical application of the legal professional privilege will mainly fall into the scope of domestic Member State legislation.

3.Data Protection Regime

3.1.Law Firm In The Context Of The GDPR

Partially, the initial concern that had given rise to this paper is that despite giving advice on the GDPR compliance, legal professionals may have paid less attention to their own practices in respect to data protection. In order to have a proper discussion in this chapter, status of a law firm with regards to data processes in the understanding of the GDPR must be defined and distinction must be drawn between the data protected by the GDPR and data protected by confidentiality obligation that is part of legal professional privilege.

Legal professional privilege and confidentiality obligation that comes with it protects any and all communications between the client and the lawyer in his or her professional capacity, with certain reservations depending on a particular regime. Meanwhile, the GDPR is aimed at the protection of the personal data of the individual. Article 2 defines that the material scope of the GDPR is processing of personal data wholly or partially by automated means and processing by other means when personal data forms part of filing system or is intended to form a part of filing system.[60] Processing of personal data that can take place during legal practice does not seem to be caught by exclusions laid out in the Article 2.[61]

With regards to data, the GDPR defines personal data as any information that can be referred to identified or identifiable person.[62] Confidential and personal data do not necessarily overlap, but nevertheless most data obtained by a legal professional would be covered by a data related obligation with some deviations depending on a Member state. With high likelihood, legal professional will receive personal data of the client, with deviations related to the area of practice and service provided to the client.

As to the status of the law firm, under the GDPR, it is clear more often than not. Even though legal professionals are usually representatives and therefore acting on behalf of their client or clients, often clients set out a goal to be achieved and allow legal professionals to choose means

[60] Regulation (EU) No 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, 4.5.2016, p 1-88 4.5.2016, art. 2, p 1.
[61] *Ibid*, art.2, p 2,3.
[62] *Ibid,* art. 4, p 1.

and methods in achieving this result, effectively entrusting the control to legal professionals.[63] The main difference between the data controller and data processor is that data controller determines the purpose and/or means of processing the data, whereas data processor, well, processes the data on the behalf of the controller.[64] In prevalent majority of the cases a legal professional will be a data controller, although it is possible that in some cases a legal professional may be considered a data processor due to particular circumstances of the case. Article 29 Working party had expressed that where a traditional role and professional expertise of service provider play a predominant role, such service provider will likely be considered a data controller.[65]

More particular opinion comes from the UK ICO, which suggests that legal professionals will be considered data controllers at least in the cases where clients have little understanding of the process employed by legal professionals and process of providing legal advice regarding third parties.[66] For a legal professional, who is already under stringent obligations of data confidentiality, it is a better approach to operate under assumption that he or she is a data controller, which will help address the risk of misidentification of the situation in case of operating on case-by-case basis of assuming the mantle of either data processor or data controller depending on the circumstance. This paper will continue under the assumption that legal professionals are data controllers, that may also process data.

Here to a brief reiteration of what are the obligations of data controllers under the GDPR. Data processors have to comply with general principles for data processing under the Regulation that are laid out in the Chapter 2[67], for that purpose data controller has to apply appropriate technical measures and update them timely as well as develop appropriate data protection policies[68], where such measures are implemented, they must ensure by design and by default that personal data is

[63] ICO (2014) *Data controllers and data processors: what the difference is and what the governance implications are*. Accessible: https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf, 16 March 2019.
[64] Regulation (EU) No 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, 4.5.2016, p 1-88 4.5.2016, art. 4, p 6,7.
[65] Article 29 Data Protection Working Party (2010) *Opinion 1/2010 on the concepts of "controller" and "processor"*. Accessible: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf, 16 March 2019.
[66]ICO (2014) *Data controllers and data processors: what the difference is and what the governance implications are*. Accessible: https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf, 16 March 2019.
[67] Regulation (EU) No 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, 4.5.2016, p 1-88 4.5.2016, art.5-11.
[68] *Ibid*, art. 24, p 1.

only processed where necessary[69]. Privacy by design and by default constitute an integral legal obligation and essential principle of the GDPR which provides a better understanding of appropriate security measures required by the GDPR.[70] It is important to keep in mind privacy by design, as often product owners of a service state that it is not a necessary specification in the service design.[71] Data controller is also obliged to maintain the record of processing activities[72], ensure appropriate security of processing[73], cooperate with supervisory authority[74], notify the data breach to the supervisory authority[75] and data subject where that breach presents a high risk to rights and freedoms of the data subject[76], carry out a data protection impact assessment (hereinafter DPIA) for a high risk processing method[77] and consult supervisory authority where such assessment will indicate high risk[78] and designate a data protection officer (hereinafter DPO)[79].

Among the cited benefits of the GDPR for the obliged entities are increased consumer trust to such entities due to better handling of the data and new potential business opportunities, decreased authority supervision.[80] Whereas legal professionals undoubtedly benefit from decreased authority supervision, trust is already a foundation of a relationship between the legal professional and a client and a reason for existence of confidentiality obligation. Nevertheless, necessity to comply with the GDPR requirements for legal professionals is apparent.

The GDPR also provides that where obligation of professional secrecy are interacting with data protection, supervisory bodies should have a specific set of powers, presumably, more limited than that in a 'normal' situation, where such powers will only apply to personal data collected as a result of an activity covered by a professional secrecy obligation.[81] It would be prudent to discuss further in this sub-chapter the impact of professional secrecy obligation on the GDPR compliance,

[69] *Ibid*, art. 25, p 1,2.
[70] Romanou, A. (2018) The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. - *Computer law and security review*, Vol. 34, 102.
[71] Färjsjö, F., Stenberg, E. (2017)Ensuring Continuous Security in the Cloud and Compliance with GDPR. (Master's thesis) University of Uppsala, Department of Technology and natural sciences, Uppsala, 45.
[72] Regulation (EU) No 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, 4.5.2016, p 1-88 4.5.2016, art. 30, p 1.
[73] *Ibid*, art. 31, p 1.
[74] *Ibid*, art. 32, p 1.
[75] *Ibid*, art. 33, p 1.
[76] *Ibid*, art. 34, p 1.
[77] *Ibid*, art. 35, p 1.
[78] *Ibid*, art. 36, p 1.
[79] *Ibid*, art. 37, p 1.
[80] Mikkonen, T. (2014) Perceptions of controllers on EU data protection reform: a Finnish perspective. - *Computer law and security review*, Vol. 30, 192.
[81] Regulation (EU) No 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, 4.5.2016, p 1-88 4.5.2016, art. 90, p 1.

DPIA for cloud-based technologies in the context of legal professional activities, as well as discuss the approach of 'appropriateness' adopted by the Regulation.

Assuming that legal professional is a data controller, he or she is under an obligation to carry out a DPIA in case of employing new method for the processing of data in order to estimate risks or where a method carries high risks for rights and freedoms of data subjects. Consequently, in case a legal professional is employing (which is the majority of cases, although the professionals themselves may not be fully aware of it) or will employ cloud-based technology, he or she is required to carry out a relevant DPIA. Such assessment in accordance with the Regulation must include at least the following: description of processing method, assessment of necessity of processing, assessment of the risks to rights and freedoms of data subject and countermeasures addressing those risks.[82] There are technological tools that can assist in that process, such as existing privacy impact assessment tools, developed for cloud storage compliance analysis.[83] However, in using cloud-based technologies, that are not a dedicated cloud storage such privacy impact assessment tools may not be available.

DPIA is a logical consequence of privacy impact assessments that have gradually gained popularity in data security industry and have been employed by the Commission as a method of meta-regulation.[84] It aims to give greater control to the data controller, as it will most likely have better expertise than the regulator.[85] This approach provides greater flexibility, but it also relies on the assumption, that all data controllers are capable of assessing the risks associated with new technology. It is an open question, whether legal professionals in particular and other data controllers, who are not primarily active in the technological sphere, are fully equipped to assess the data privacy impact. In connection to that, who will hold responsibility for the damage to rights and freedoms of data subjects or data breaches that could have been avoided if not for incorrect data privacy impact assessment?

Some of the risks that DPIA for cloud based technologies and cloud storage will have to address include shared resources between subscribers who are unknown to each other, increased system complexity which provides more surface for vulnerabilities to arise, delivery of data via internet

[82] *Ibid*, art. 35, p 7.
[83] Tancock, D. et al (2010) A Privacy Impact Assessment Tool for Cloud Computing. - *2nd IEEE International Conference on Cloud Computing Technology and Science*, USA, 30 Nov.-3 Dec. 2010, (Eds.) Judy Qiu, Gansen Zhao, and Chunming Rong, Los Alamitos, CA : IEEE Computer Society, 667.
[84] Binns, R.(2017) Data protection impact assessments: a meta-regulatory approach. - *International Data Privacy Law*, Vol. 7, No. 1, p 22, 28-30.
[85] *Ibid*, 32.

exposing data to potential interception and delegation of security control to the cloud service provider.[86] The burden of obligations and associated risks may appear daunting. One of the technical measures that may serve as a safeguard is encryption, in particular zero-knowledge cloud storage, which may be helpful, but should not be treated as be-all and end-all.[87] In addition to PIA tools, specific GDPR compliance tools for the use of company compliance officers are available.[88]

With regards to professional secrecy and its impact on the GDPR compliance, as already mentioned, the GDPR makes a special mention of professional secrecy obligations and urges for special set of rules for supervisory authorities with regards to controllers and processors under professional secrecy obligations.[89] The GDPR also expresses respect for professional secrecy obligations and wishes to reconcile them with data protection rights where necessary, as can be seen from the recital 168.[90] More specific guidance shall be sought from the rules on supervisory authorities adopted by the Member States. The fact that the GDPR treats professional secrecy favorably is not the end of the discussion, as shown by the facts on the interference and breaches of legal professional privilege by state authorities laid out in the CCBE statement on legal professional privilege.[91] Therefore, legal professionals should still carefully evaluate data requests from the supervisory authorities and attempt to reconcile obligation to assist supervisory authorities stemming from the GDPR and professional secrecy obligation.

Notion of appropriateness in the GDPR is tied to its understanding of risk and risk-based approach taken by the Regulation. It is an obvious issue that the GDPR compliance requires huge resources, which is why tick-box compliance would have been a very burdensome approach. As such, risk based approach allows obliged parties under the GDPR assess their circumstances and tailor their obligations to the circumstance.[92] However, this approach leaves uncertain when the compliance will be considered 'appropriate' and it is also impossible to point out which legal norms are indispensable and which can be 'sacrificed' when part of supervisory functions is delegated to the

[86] King, N.J., Raja, V.T. (2012) *supra nota*, 309.
[87] Crowley, M.G et al (2016) Protecting corporate intellectual property: legal and technological approach. - *Business Horizons*, Vol 59, 627-628.
[88] Weber, R. H., Staiger, D. (2017) Transatlantic data protection in practice. Berlin: Springer-Verlag GmbH, 11.
[89] Regulation (EU) No 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, 4.5.2016, p 1-88 4.5.2016, art. 90, p 1.
[90] *Ibid,* recital 168.
[91]CCBE (2017) *CCBE Statement of professional secrecy/Legal professional privilege(LLP)*. Accessible: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_Postion_Papers/EN_DEON_20170915_Statement-on-professional-secrecy_LPP.pdf, 16 March 2019.
[78]Quelle, C. (2018) Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach. – *European Journal on Risk Regulation*, Vol. 9, 508

controllers and processors themselves[93]. This will most likely be cleared up when the first GDPR non-compliance cases will be brought to the EUCJ.

Another discussion point that would perhaps be interesting to discover is the application of data protection processes to the everyday work of a legal professional. The GDPR urges to take appropriate measures in order to prevent data from identifying the data subject which is expected to be achieved through anonymization or pseudonymization processes. It also requires setting limits on the data retention. Those measures may not be always suitable for the activities of a legal professional, depending on the area of practice, particular circumstances of the case and other factors, especially considering that many clients rely on legal professionals in documentation storage. This is where appropriateness and risk-based approach of the GDPR are extremely beneficial, allowing legal professionals to adapt the compliance processes to their particular activities. With regards to the anonymization, encrypted data in electronic processing such as cloud computing will be equated to the anonymized data, so it could be a better option for legal professionals.[94]

However, this is also the very reason why the GDPR compliance is an arduous task and should not be underestimated. It becomes even more burdensome, as the number of technologies in employ of a legal professional or a law firm increases. Although appropriateness may allow more leeway with compliance, it is not possible to avoid DPIAs for novel technologies employed by a legal professional in course of professional activity. Even though many services used may have similar underlying technologies, they might involve different risks depending on other factors. DPIA in any case a very useful tool that will give legal professionals better understanding of the implications of the technology, that is used in everyday professional activities, and thus an opportunity to safeguard it from potential breaches of confidentiality obligations, accidental waiving of professional secrecy and breaches of rights and freedoms of data subjects.

This sub-chapter had presented a rather brief overview of obligations of data controller under the GDPR, concepts of note that are important to understand in evaluating the GDPR compliance and specific position of a legal professional with regards to data protection obligations. It is necessary to have an understanding of the full framework of obligations, that legal professionals are subject to with regards to data protection regime. It is also important to highlight that it is not inconceivable

[93] *Ibid,* 525-526.
[94] Zanfir, G. (2012) The right to Data Portability in the context of the EU data protection reform. - *International Data Privacy Law*, Vol. 2, No. 3, 152.

that confidentiality obligations of a legal professional stemming from professional secrecy requirement may come in conflict with the obligations of a legal professional under the GDPR as a data processor, in particular where requests of data protection supervisory authority are referred to a legal professional.

3.2.Client As A Data Subject

Chapter 3 that contains Articles from 12-23 describes the rights of the data subject[95], who is the client of a legal professional in the case of this paper. In order to compile recommendations for legal professionals that would take into account data protection obligations and confidentiality obligation stemming from the legal professional privilege, it is necessary to provide a short overview of the data rights and freedoms of the client that are to be safeguarded by the legal professional in handling the clients' data in the course of professional activities.

Under the principle of transparency[96], legal professional as a data controller should inform the client of the purposes of processing the data and recipients of personal data if applicable.[97] It is a valid presumption that the client will be aware of the identity and contact details of the legal professional. Where legal professional obtains personal data not from the client with clients consent, it is obligatory to provide the identity, contact details, purpose of processing, category or categories of personal data concerned, recipients of personal data.[98] Additionally, where such data is transferred cross-border in the country of absent Commission adequacy decision, reference to appropriate safeguards is to be made[99], which is important to keep in mind for the purpose of cross-border data transfers.

Data subjects also have a right of access that allows to obtain information from the controller whether his or her personal data is being processed,[100] right to rectification that allows to correct inaccurate data about the data subject[101], right to erasure that in certain circumstances allows the data subject to ask for erasure of his or her personal data[102], right to restriction of processing that

[95] Regulation (EU) No 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, 4.5.2016, p 1-88 4.5.2016, art. 12-23.
[96] *Ibid*, art 12.
[97] *Ibid*, art 13.
[98] *Ibid*, art.14, p 1.
[99] *Ibid*, art.14, p 1(f).
[100] *Ibid*, art.15, p 1.
[101] *Ibid*, art.16, p 1.
[102] *Ibid*, art.17, p 1.

allows the data subject to obtain an injunction of sorts on restriction of personal data processing by data controller from the supervisory authority in certain circumstances[103], right to data portability that allows data subject to move personal data to another controller in certain circumstances and receive a copy of his or her data[104], right to object to processing of personal data concerning data subject.

Now, how does it affect data processing activities of the legal professional as a data controller? The more impactful rights with regards to the data of clientele will likely be right to erasure, right to restriction of processing, right to data portability and right to object. It is in the interests of both parties in the lawyer-client relationship to have the correct data and to be aware of the circumstances of processing. Interestingly, CCBE guidelines had recommended already in 2012 that in case of processing through cloud technology, clients should be aware of that for the sake of transparency.[105]

Right to erasure, right to restriction of processing, right to data portability and right to object will very likely come in the light when conflict arises between the legal professional and the client. For example, how far would the limits to data portability go – would it be appropriate for the client to require a legal professional to store their data with a different cloud service provider? The right essentially allows to change a data controller. In the situation where data is stored in a cloud service, cloud service provider may be also considered a data controller jointly with a legal professional in the circumstances where data processing conditions are determined jointly by the legal professional and cloud service provider. It is not possible to respond to that issue without appropriate court practice, but it is something to consider in the situations where a legal professional is a joint controller with a service provider. As legal professionals need personal data provided by the data subject in its original form normally in order to be able to provide services, they do not fall under inferred data exception that is available with regards to data research[106]. As the data portability only extends to the data provided by the data subject itself, it does not extend to the data otherwise obtained by the legal professional,[107] but it is an unlikely circumstance to rely on.

[103] *Ibid*, art.18, p 1.
[104] *Ibid*, art.20, p 1.
[105] Council of Bars and Law Societies of Europe (2012) CCBE Guidelines On The Use Of Cloud Computing Services By Lawyers. Brussels: CCBE.
[106] Ursic, H. (2018) Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control. - SCRIPTed, Vol. 15, No. 11, 55.
[107] *Ibid*, 55.

With regards to data erasure, in choosing the cloud service provider, a legal professional must be aware of the difficulties that exist in truly removing data and should assess relevant capacities and policies of the cloud service provider. The rights and freedoms of data subject are not all encompassing and some limitations to them are already included in the Regulation. Nevertheless, legal professional must be especially aware that those rights apply to all of his or her clients whose personal data he or she stores when the data is stored with a third party. With regards to the choice of a service provider, it is particularly difficult to balance rights of the clients as data subjects and responsibilities of the data controller, as it seems that certain measures of ensuring privacy by design tend to undermine the rights of the data subjects.[108]

In different circumstances, depending on particular case, processing of the clients' data can fall under different legal bases for processing under the GDPR. Most likely the legal bases for processing the client's data under the Article 6.1 of the GDPR in case of law firms would be paragraphs 6.1.a, 6.1.b, 6.1.c and 6.1.f that refer to the processing of the personal data on the basis of consent, necessity for the performance of the contract, necessity for compliance with legal obligation and legitimate interests of the controller or third party.[109] The relationship between the client and the legal professional is normally based on an agreement, be it oral or written. In case of written agreement, legal basis for processing would be the contractual relationship, whereas the oral agreement would likely invoke consent as legal basis for processing. In some cases, where a relationship between a legal professional and a client is long standing, the contractual relationship may have its limits and in this case necessity for compliance with legal obligations will likely be the legal basis for personal data processing where necessary to fill in contractual gaps.

However, it is rather hard to imagine that a legal professional in his or her professional activities will not be able to process personal data of the client due to the lack of legal basis for processing. Personal data of the thirds parties to the relationship between the legal professional and the client is where the problems really may arise. It is very likely that legitimate interest of the third party, who would be the client, or the controller, who would most likely be the legal professional, would be the basis for processing the personal data of a person, who is not the client. However, it is not a bullet-proof solution and it should not be assumed that such basis would exist in the case of any third person.

---

[108] Veale, M. et al (2018) When data protection by design and data subject rights clash. – *International Data Privacy Law,* Vol. 8, No.2, 107.

[109] Regulation (EU) No 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, 4.5.2016, p 1-88 4.5.2016, art. 6.

Moreover, as the data must be 'processed lawfully, fairly and in transparent manner'[110], legal basis of the processing is not the guarantee for compliance with regards to the processing of the data. Article 5 of the GDPR sets outs general principles for the processing of the data, whereas Article 6 of the GDPR only expands on the lawfulness of processing. It is nevertheless prudent to approach a choice or rather discovery of an applicable legal basis with case, as different legal grounds will give rise to different sets of rights of the data subject.[111] For example, legitimate interest of a third party or a data controller would exclude application of the right to data portability, but neither right to object, nor right to erasure,[112] therefore, a third party would be within their right to raise their objections to the processing despite a legitimate interest of the client.

3.3.Rights And Obligations Of Service Providers

Storage of data falls under the definition of processing under the GDPR. Service providers may find themselves in a dual situation, as although in majority of the cases where the data is stored by a legal professional on a cloud service, service providers will be data processors, it may also happen that service providers in some circumstances will be considered data controllers jointly with the legal professional. Some aspects that will be helpful in analyzing whether service provider is a data processor or a joint controller are the level of prior instruction, the level of monitoring by data controller, then visibility of the service provider and the level of parties' expertise.[113] However, as different sub-chapter had already covered in brief responsibilities of the controller and the case of joint control will most likely be quite rare, this sub-chapter will presuppose that cloud service provider will be mainly a data processor rather than data controller.

The GDPR provides, that data controller must only use processors, that provide sufficient compliance guarantees with regards to appropriate technical and organizational measures that will allow the processor to meet the GDPR standards.[114] Legal professional in engaging a cloud service provider should only do so on a contractual basis, where the contract outlines subject matter,

[110] *Ibid*, art. 5, p 1.a.
[111] Gonzalez, E.G, De Hert, P. (2019) Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles. – *ERA Forum*, Vol. 19, 599.
[112] *Ibid,* 599.
[113] Lindquist, J. (2018) New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things? - *International Journal of Law and Information Technology*, Vol. 26, 48-49.
[114] Regulation (EU) No 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, 4.5.2016, p 1-88 4.5.2016, art. 28, p 1.

duration, purpose and nature of processing, types of personal data, categories of data subjects and rights and obligations of the controller.[115] Processor is also obliged to ensure appropriate level of security[116], notify the controller in case of a data breach[117] and designate a DPO[118].

Despite the type of the cloud service, all service providers will have available standard terms of service. Not all legal professionals will be able to propose their own, their bargaining position may not necessarily be strong, especially in a business-to-business environment where contracts are often proposed in 'take it or leave it' manner due to imbalance of the stakeholders[119]. Even in using zero-knowledge cloud service, a legal professional must be careful in using the cloud service, as the service provider may collect the data of the law firm itself, including device types, browsers, unique identifiers and IP-addresses.[120] Many legal professionals often work overtime or outside the office and may use their own devices and therefore need to be aware of the terms of the cloud data storage services they use in the course of their professional activities.

Another issue to look out for in choosing a service provider as a legal practitioner would be the specific language used by the provider in their terms of service. Those security standards have to correlate somehow with the standard set by the GDPR. Vagueness of the terms used in the contract and variety of the specific standards used by different service providers may be understandable, as the standards of the industry will change over time,[121] but the data controller nevertheless must ensure that the security standards of the data processor are sufficient for the purpose of the GDPR compliance, as data security is a shared responsibility under the GDPR[122]. The stringent security standards obligations are a consequence of the consumer focus of the EU legislative framework,[123] consumer in the circumstances of this paper being a data subject. It had been a topic of discussion whether public legislative regulation is sufficient for providing sufficient security standards, especially in cloud computing, where one of most significant regulatory pieces had emerged from the International Standards Organization.[124]

---

[115] *Ibid*, art. 28, p 3.
[116] *Ibid*, art. 32, p 1.
[117] *Ibid*, art. 33, p 2.
[118] *Ibid*, art. 37, p 1.
[119] Lindquist, J. (2018) *supra nota*, 50.
[120] Kamarinou, D., Milliard, C., Kuan Hon, W. (2016) Cloud privacy: an empirical study of 20 cloud providers' terms and privacy policies - Part I. - *International Data Privacy Law*, Vol. 6, No. 2, 88.
[121] Kamarinou, D., Milliard, C., Kuan Hon, W. (2016) Cloud privacy: an empirical study of 20 cloud providers' terms and privacy policies - Part II. - *International Data Privacy Law*, Vol. 6, No. 3, 179.
[122] Wolters, P.T.J. (2017) The security of personal data under the GDPR: a harmonized duty or a shared responsibility? - *International Data Privacy Law*, Vol. 7, No. 3, 177.
[123] McGillivray, K. (2016) A right too far? Requiring cloud service providers to deliver adequate data security to consumers. - *International Journal of Law and Information Technology*, Vol. 25, 25.
[124] de Hert, P., Papakonstantinou, V., Kamara, I. (2016) The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection. - *Computer law and security review*, Vol. 32, 16.

Again, the technology is still constantly being improved and it is plainly unlikely that governmental organizations will keep pace, which is why the GDPR risk-based approach that obliges to 'ensure' security and apply 'appropriate' measures was taken. With regards to the compliance aspects that data controllers must ensure, such mechanisms as privacy seals might be useful, although it should not be considered a panacea, it will make compliance burden with regards to cross-border environment and processor-controller interactions just a bit easier.[125]

To conclude, for a data controller such as a legal practitioner, it is crucial to be careful in choosing a data processor due to the burden of the GDPR compliance. It is also crucial to understand the interaction between data controller and data processor for the better GDPR compliance and application.[126] It is important to carry out appropriate research as per CCBE recommendations and evaluate terms of service, procedures and services that will affect the GDPR compliance of the data processor. Due to the nature of cloud services, it is also important for legal practitioners to implement in-house security procedures with regards to their own personal data as they find appropriate.

Additionally, taking into account confidentiality obligations to which most legal professionals are subject to, it is prudent to evaluate use of zero-knowledge cloud services, as the data will be encrypted at the customer level, which will make compliance with confidentiality obligations a bit easier as well as appear a more suitable anonymization method not only due to particular circumstances of using personal data in legal work but also due to difficulty of anonymizing and pseudonymizing data in the cloud. Retraceable pseudonymization may still remain personal data due to re-identification methods and traceability of pseudonymization and strength of pseudonymization itself will depend on the anti-identification methods used.[127]

However, zero-knowledge cloud service is not an be-all and end-all approach, as re-identification methods become increasingly more available and as such full data anonymization is not possible.[128] Therefore, it is essential to combine it with other measures prescribed and recommended by the GDPR, such as data minimization[129]. More guidance specifically on ensuring

[125] Rodrigues, R. et al (2016) The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR. - *International Review of Law, Computers & Technology*, Vol.30, No. 3, 249.
[126] Lindquist, J. (2018) *supra nota*, 46.
[127] Kuan Hon, W., Milliard, C., Walden, I. (2011) The problem of 'personal data' in cloud computing: what information is regulated?—the cloud of unknowing. - *Internationasl Data Privacy Law*, Vol. 1, No. 4, 217.
[128] *Ibid,* 227.
[129] *Ibid,* 227

security of data in the cloud is offered by the CIRRUS project that is co-funded by the European Commission and researches internationalization, certification and standardization in the cloud, result of this research being a Green Paper on security and data privacy protection.[130]

This sub-chapter had presented a brief outline of the legal regime concerning data processors. It was necessary to describe those circumstances in order to have a better understanding of the full picture surrounding legal professional as a data controller within the framework of the data protection. As shown in this sub-chapter, roles of data processor and data controller are inter-related, sharing many responsibilities. Additionally, performance of the data processor will likely affect performance of the data controller with regards to the GDPR compliance.

3.4.Cross-Border Data Disclosure In The Cloud

It is not inconceivable to suggest that legal professionals in the course of their professional activities will sometimes come across cases that require involvement with third country entities, as such international transfers are akin to a routine, especially in the context of a cloud[131]. In order to respect their confidentiality obligations and obligations as a data controller, it is prudent to evaluate all circumstances connected to the cross-border data transfer. It is also important to note that third country lawyers are not considered beneficiaries of the legal professional privilege based on the EU jurisprudence, which interprets legal professional privilege very narrowly.[132] Another circumstance to be taken into account is the treatment of cross-border transfers by the GDPR. Generally, such transfers are permitted if the country to which personal data is transferred is subject to a Commission adequacy decision.[133] At the moment in addition to EEA countries Andorra, commercial organizations in Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and USA are subject to Commission adequacy decision.[134]

However, in case of absence of an adequacy decision, data controller or data processor must provide an evaluation of existence of appropriate safeguards for data protection in the third country

[130] Kennedy, E., Millard, C. (2016) Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU Member States. - *Computer law and security review*, Vol. 32, 103.
[131] Zanfir, G. (2012) *supra nota*, 161.
[132] Gonzales-Diaz, F.E., Stuart, P. (2017) supra *nota*, 59.
[133] Regulation (EU) No 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, 4.5.2016, p 1-88 4.5.2016, art. 45.
[134] European Commission (2019) *Adequacy decisions*. Accessible: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en, 20 March 2019.

where data will be transferred.[135] If the evaluation finds that there are no appropriate safeguards, then the transfer of personal data to that third-country can not be done. This is also an important issue to keep in mind in the use of cloud storage services considering potential lack of understanding where the data actually is. Is the place of the data transfer considered to be the server location or place of establishment of the service provider or place of head office of the cloud provider or an evaluation ought to consider data privacy regulations in all of those locations? Internet jurisdiction comes back to haunt once again.

Such cross-border transfers may take place with regards to various stakeholders, not only private parties, international organizations and other legal professionals but with regards to the judiciary, quasi-judiciary or another state authority of a third country. Transfers of data to foreign court, tribunal or regulator must be based on an international agreement, such as Mutual Legal Assistance Treaty.[136] Legal industry had already expressed concerns over Privacy Shield due to the *Schrems* case from the EUCJ, that effectively cancelled Safe Harbour.[137] Practical recommendations over data protection regime with regards to regulatory requests propose evaluating whether there is an obligation to respond, seek further information to establish the purpose of the request, negotiate the scope of the request, anonymize data or minimize it, notify the data subject or obtain his or her consent and evaluate whether requested data may be transferred on the basis of mutual legal assistance treaty or through domestic state authority.[138]

Long arms of the GDPR have imposed a harmonization move on the international actors and stakeholders especially where it comes to cross-border transfers.[139] The voice of dissent to the GDPR strict regulation due to a concern that its long arms may prompt international actors and other states to restrict dealings with the EU, which may have very undesirable consequences. One of the consequences of compliance with the GDPR with regards to cross-border issues may be emergence of Europe-only services, EU excluding international companies and international companies and third countries excluding EU due to the compliance burden. For example, the idea of Europe-only cloud predates the Snowden revelations, but might just get the push forward from

[135] Regulation (EU) No 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, 4.5.2016, p 1-88 4.5.2016, art. 46.
[136] *Ibid*, art. 48.
[137] Parker, N. et al (2017) *GDPR and data protection issues in cross-border regulatory investigations.* Accessible: www.allenovery.com/publications/en-gb/lrrfs/continental%20europe/Pages/GDPR-and-data-protection-issues-in-cross-border-regulatory-investigations.aspx, 8 October 2018.
[138] *Ibid.*
[139] Sullivan, C. (2014) Protecting digital identity in the cloud: Regulating cross-border data disclosure. - *Computer law and security review*, Vol. 30, 148.

the GDPR.[140] This will definitely have an impact on competition law, intra-European trade and potentially free movement of services,[141] potentially a rather negative impact. In the context of the Digital Single Market and data-based economy direction that EU had taken in the recent years, rather restrictive approach on the right to use data taken by the GDPR may put it in an unfavorable position in the global market with regards to building an information economy.[142]

It could be argued that territorial scope of the GDPR does not cover all cross-border situations where data subject is in the EU and a controller or a processor is outside the EU, as it requires processing of the personal data to relate to provision of services or goods to data subject in the EU or monitoring of the behavior of those data subjects.[143] However, it is likely that jurisprudence will interpret non-EU specific worldwide targeting as falling under the scope of the Regulation nevertheless in accordance with teleological approach as otherwise it would be all too easy to escape the GDPR, be it as it may against the wording of the Article 3(2)(a).[144]

A particular issue that is a matter of cross-border data transfer, would be a foreign court order requesting the personal data of a EU data subject, as the GDPR does not provide the basis for questioning or refusing such order, although such concerns were presented in the initial draft of the Regulation.[145] It is a circumstance that legal professionals should be aware of and ready to deal with if need be.

Another matter in the cross-border effect of the GDPR is e-discovery. It is yet unclear what effect will the GDPR have on the data collected through internet[146], but some regard might be had to digital evidence regulation. It is possible, that upcoming digital evidence regulation will sufficiently compliment the GDPR and clarify the matter of e-discovery, but its scope is limited to the EU and criminal matters[147].

---

[140] Kuan Hon, W. et al (2016) Policy, legal and regulatory implications of a Europe-only cloud. - *International Journal of Law and Information Technology*, Vol. 24, 254.
[141] Ibid, 277.
[142] Zech, H. (2016) A legal framework for a data economy in the European Digital Single Market: rights to use data. - *Journal of Intellectual Property Law and Practice*, Vol. 11, No. 6, 470.
[143] Taka, A-M. (2017) Cross-Border Application of EU's General Data Protection Regulation (GDPR) - A private international law study on third state implications. (Master's thesis) University of Uppsala, Department of Law, Uppsala, 88.
[144] Ibid, 88-89
[145] Kulesza, J. (2014) Transboundary data protection and international business compliance. - *International Data Privacy Law*, Vol. 4, No. 4, 303.
[146] Ryz, L. et al (2016) A new era in data protection. – *Computer Fraud and Security*, Vol. 2016, No. 3, 19.
[147] European Commission (2019) *E-evidence – cross-border access to electronic evidence.* Accessible: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en#internaleurulesproposaloneevidence, 7 May 2019.

To conclude, this sub-chapter had outlined legal and compliance issues concerning cross-border data transfers in general and specific to the situations of cloud transfers and data transfers by legal professionals. Trends of the EU jurisprudence that had gradually expanded EU competence and European nanny state tradition based on faithful loyalty and trust to the state had laid the foundation for the current situation. The EU absorbs more control from the states, whereas the states take away control from the individuals in a misguided attempt to shield them from harm. However, this is the consequence of choices made by individuals in a free democracy.

Nevertheless, despite all the benefits of the GDPR, it has some gaps and difficulties associated with it, the chief issue being its potential to affect international trade due to the restrictive long arm approach that the Regulation had taken. At the moment, after the GDPR had entered in force in spring of last year, the backlash had been widespread but mild. However, it would not be beneficial to seclude the trade to Europe-only supply of goods and services. Nevertheless, the foundation had been laid and the effects of the undertaken course of action will soon follow. With regards to the issue at hand, it had been outlined very briefly what potential issues a legal professional ought to pay attention to and be extremely mindful about in the cross-border data transfers.

In summary, an overview was provided for the data privacy issues connected with the General Data Protection Regulation, that a legal professional practicing in the field of law would have to be aware of in the context of his or her professional activities, being a data controller him- or herself. It is a second of three main legal aspects of this paper, the first being confidentiality obligation under legal professional privilege and the effect of using cloud storage by a legal professional on that obligation; and the third aspect being the liability for breaching confidentiality obligation and obligations under the GDPR as well as liability of other parties to the circumstance of data storage and transmission to the cloud. After outlining those issues in a sufficient manner, it will be possible to conduct a proper analysis of whether the hypothesis, that was proposed in the introduction to this paper, is true or false.

Before addressing next chapter that will start pulling together the strings and discussion points addressed up to this moment, it is useful to reiterate the supposition that forms the hypothesis of this paper: use of cloud storage and online cloud-based tools by law firms in the course of their work for the purposes of storing documentation wholly or partially compromises data rights and freedoms of their clients and undermines confidentiality between a legal professional and a client. This chapter had provided the basis for addressing a significant part of the hypothesis: the

obligations of the data controller, who is a legal professional in the circumstances of the hypothesis, and rights and freedoms of the data subject, who is a client of a legal professional. As the prior chapter had provided the analysis of the legal professional privilege within the EU and effects of cloud storage on the compliance with confidentiality obligation, the foundation for more analytical part of the paper and putting together problematic issues and their counters had been laid.

It is undeniable, that the compliance burden of the controller is very significant and utmost caution must be exercised by the controller in the data processing activities concerning personal data. This statement has even more weight, when applied to the data controller who is legal professional, as demonstrated in this chapter. Additionally, this chapter had given pointers to compliance and responsibilities specifically concerning storage of personal data in the cloud alongside the discussion on the general GDPR compliance. It could have been a more detailed discussion on the topic of the GDPR compliance, but the focus of this paper is the effect of the cloud storage use on the compliance of legal professionals. With regards to cloud data storage, it seems to have several significant issues that affect compliance methods that data controller must evaluate using in the context of the GDPR compliance, cloud data storage and transmitting data to that cloud storage. Hopefully, this chapter had sufficiently covered the topic in order to conduct an analysis necessary to answer as to the truthfulness of the hypothesis in the conclusion of this paper.

4.Liability In The Cloud

4.1.Law Firm

The GDPR in the Article 5.2 provides for the accountability of the data processor for the compliance with the general principles of processing.[148] Therefore, law firm undoubtedly is liable for non-compliance with the provisions of the GDPR, including its general principles and specific obligations based on those principles. Most importantly, data controller must be able to demonstrate the compliance with the GDPR on the basis of the Article 5.2.[149] In some rare cases legal professional may have liability of the data processor, but as those are the minority of cases, it is prudent to accept more stringent requirements as default and act accordingly.

Therefore, legal professional will still have most of the compliance liability in the processing of data, as accountability is the principal obligation of the processor[150], and should be aware of that fact in the choice of the service provider. This is further exacerbated by the wider liability for potential damages, that applies to data controllers under the GDPR. Under the Article 82, any data controller shall be liable for the damage caused by processing that is in breach of the GDPR,[151] unless controller is able to prove that he was not in any way responsible for the event giving rise to the damages[152].

This puts even more stress on the choice of service provider for a law firm. Not all service providers are created equal. In American case *Harleysville Insurance Company v Holding Funeral Home Inc* Dropbox was already considered a 'digital equivalent of leaving the documentation on a park bench'.[153] It is possible to suggest, that European jurisprudence will take a similar position, especially considering rising significance of cyber security and data protection in the EU.

[148] Regulation (EU) No 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, 4.5.2016, p 1-88 4.5.2016, art. 5.2.
[149] *Ibid,* art. 5.2
[150] Lindquist, J. (2018) *supra nota*, 58.
[151] Regulation (EU) No 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, 4.5.2016, p 1-88 4.5.2016, art. 82.2.
[152] *Ibid*, art 82.3.
[153] Harleysville Insurance Company v Holding Funeral Home Inc., No. 1:15 cv 00057, 2017 U.S. Dist. LEXIS 18714 (W.D. Va. Feb. 9, 2017).

Liability for law firms in the cloud is not much different from that of their clients, who are also considered data processors under the GDPR. However, the question of confidentiality obligation under legal professional privilege is layered on the data protection obligations under the GDPR. From one side, it makes the compliance question much more significant, from the other side, as the obligations overlap, compliance related activities decrease.

4.2.Controller-processor Agreement Aspects

Even though a law firm would be a principal responsible party, service provider will also bear some responsibility, either as a joint controller or a data processor, depending on the particular agreement between the service provider and the law firm. From the law firm's point of view, it is crucial to understand liability of the service provider in order to choose an appropriate one. In the choice of a service provider, law firms will have different bargaining positions, not all law firms will be able to negotiate the contracts with the service providers, even though it is the primary responsibility of the processor to allocate responsibility[154]. Understanding the question of liability of the service provider, who would likely be a data processor as discussed prior, will allow to evaluate terms of service in order to choose a provider.

Firstly, for the controller's obligations to be appropriately fulfilled, there must be a link between the accountability obligation of the controller and measurability of processing due to the obligation of the controller to be able to demonstrate compliance.[155] Processing can be measured through right to audit, where right to audit can contain right to audit location of the servers, the algorithms or security measures.[156] In practice, it can be complicated to implement due to a variety of reasons. Big digital companies will have too many clients to the point where it would not be possible to allow each of them to inspect physical location of the servers, servers can be located far away from the client. This is especially true for cloud service providers. It is up to the contracting parties, whether to include right to audit or not. Additionally, it is possible to limit, simplify or standardize audit in order to make it accessible for both data processor and data controller. In any case, processors are obliged to make available all the necessary data for demonstrating controller's compliance with the GDPR.[157]

[154] Lindquist, J. (2018) *supra nota*, 61.
[155] *Ibid*, 58.
[156] *Ibid*, 58.
[157] Regulation (EU) No 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, 4.5.2016, p 1-88 4.5.2016, art.23.

Secondly, the contract between the law firm and service provider shall make the question of accountability very clear, as data processors are not liable for the failure to apply the principle of accountability, unless appropriately instructed by the data controller.[158] Law firm as data controller shall take utmost care in either drafting a contract or evaluating standard terms of service, as data processor is liable for damage caused by the breach of the obligations under the GDPR where it had acted outside of lawful instruction of the controller or where the GDPR obligations, that are specifically directed at the controller, were breached.[159] Therefore, the contract between the data controller and data processor must outline such instructions, as data controller will bear principal liability for damages, which might be further exacerbated by deficiencies of the contract.

The contract between the data processor and data controller must further clarify the question of the sub-contracting. It is possible to restrict sub-contracting in the controller-processor agreement,[160] however, if a processor intends to rely on sub-contracting, he must remember, that legal responsibility to the controller in case of the breach by the sub-processor will lie with the initial processor.[161]

This is of course not the full list of the matters, that must be outlines in the controller-processor contract in order to comply with the GDPR, but those are most crucial for understanding the liability of the parties and safeguarding against unfavorable outcome in case of the breach.

It is also interesting to mention an argument that cloud service providers are not data processors, as they only make available the resources that allows their customers carry out data processing activities.[162] However, although the argument makes sense from the technical perspective, as it is not yet practically possible for the client to install all necessary security procedures and measures and take all appropriate safeguard in the context of cloud services, it is doubtful, that this position will be assumed by the judiciaries of the EU and MS.

[158] Lindquist, J. (2018) *supra nota*, 58.
[159] *Ibid*, 60.
[160] Kuan Hon, W., Milliard, C., Walden, I. (2012) Who is responsible for 'personal data' in cloud computing? —the cloud of unknowing. - *International Data Privacy Law*, Vol. 2, No. 1, 5.
[161] Lindquist, J. (2018) *supra nota*, 60.
[162] Kuan Hon, W., Milliard, C., Walden, I. (2012) *supra nota*, 10.

4.3.Client

However unlikely, it is still possible that a client may bear some responsibility for the breach of the obligations under the GDPR. Joint controllership of the law firm and the client and breach, related to the data of the third party, are the pre-conditions for such liability. Those cases will likely be rare in practice, but theoretically it is possible for the circumstances to lead to such outcome.

With the existence of cloud computing tools, that facilitate data sharing, will a client, who shares employee's personal data via Dropbox or Google Drive, be liable in case of a breach? Depending in the circumstances of the case, the client can be considered a data controller in this case and as such bear responsibility for the breach. Who had offered such means of data processing, could the law office reject such submission and request a different delivery method – those factors may help the establish controllership. Another question is whether it is the responsibility of the law office to safeguard their clients from such accidental joint controllership. It is up to each law office, whether it is considered necessary, however, in the interest of good faith and preservation of client-attorney relationship, it may be prudent to advise the client with regards to appropriateness of the methods used to deliver the required data.

5.Recommendations

On the basis of the discussion brought up in this paper, it is possible to address existing guidelines for the cloud use by lawyers and propose some recommendations for the regulatory bodies that had drafted those guidelines initially. As the circumstances had changed and the cloud usage became more widespread since such guidelines were drafted, not in the least due to being facilitator for other technologies. There is no need to change the backbone of the recommendations that is expressed in the guiding principles, as principles of data protection legislation are very much in line with core principles of legal profession.[163]

The main changes are the precariously vague status of legal professional privilege in European Union law, new data protection regulation, increased reliance on and use of the cloud in the professional activities of the law companies. With regards to that, CCBE guidelines on the use of online platforms by lawyers from 2018 are more up to date and provide a comprehensive and multifaceted analysis of issues involved in the use of online platforms by lawyers.[164] This type of analysis would be also appropriate in addressing cloud computing use by lawyers, but the existing CCBE guidelines on cloud use are not quite as thorough.

It can not be denied that CCBE had been rather thoughtful in their submissions and publications with regards to cloud computing. CCBE response regarding the European Commission public consultation on cloud computing had pinpointed concerns related to the ethical duty of lawyers to preserve and protect clients' data and rightfully called for an update on Data Protection Directive.[165] As such an update to the data protection regime took place, it is also prudent to revisit the existing CCBE cloud computing guidelines in order to address changed circumstance.

However, on the basis of the analysis carried out in the previous chapter, the first recommendation that stems from this paper is the recommendation to stress the necessity for clarity with regards to the liability. Such clarity must include not only the analysis of the liability of the law firm itself, but attention to liability aspects of the controller-processor contract and appropriate consultation

[163] CCBE (2013) Charter of core principles of the European legal profession and Code of conduct for European lawyers. Brussels: CCBE.
[164] Council of Bars and Law Societies of Europe (2018) CCBE Guide On Lawyers' Use Of Online Legal Platforms. Brussels: CCBE.
[165] CCBE (2011) *CCBE response regarding the European Commission public consultation on cloud computing.* Accessible: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20110909_CCBE_Response_on_Cloud_Computing.pdf, 7 May 2019.

to the client with regards to avoiding or managing joint controllership. Additionally, as GDPR had introduced more stringent obligations for data controllers, it would be prudent to revise the contractual precautions section of the guidelines, which contains essentially a list of things to which a legal professional should pay utmost attention in dealing with the service provider. The existing list of precautions already contains some of the relevant points, such as server location, right to audit and technical documentation, but it would be prudent to add a few more, such as aforementioned liability question, security procedures and measures and specific provisions on scope, retention, time limits, legal basis of processing and so on.

Another important question, that was not covered in the 2012 CCBE guidelines is cross-border data access. Cloud computing and cloud data storage can additionally be used by cooperating law firms as a data sharing tool, thereby touching on questions on e-discovery and cross-border data sharing in such guidelines would be prudent.

Furthermore, there is a serious downside to the guidelines are purposefully vague. The attempt to make the guidelines relevant through avoiding specific measures is understandable, however, an update is already required due to changes in circumstance. Additionally, law firms are not cyber security specialists and often may not be aware of specific measures or type of measures that may be employed to fulfil their obligations. People-Process-Technology is the standard evaluation matrix in cyber security strategy that can be an appropriate recommendation for evaluation of both inhouse and outhouse security measures.[166] In this context, it may be beneficial for the industry, if some soft law regulation proposes certain generalised but specific technical recommendations.

It is possible to break down the topic of the cloud computing use for lawyers in subsections or separate guidelines, in order to keep the ethical part more lasting and at the same time to provide more guidance regarding specific compliance measures. A package of guidelines will also allow to easily amend those parts, that will need updating with time, which is inevitable.

To sum up, it would make it easier for a regulatory body to break up the topic of cloud computing into several parts in order to address cloud computing use by lawyers in most efficient and resilient manner – ethical; specific legal questions, including, but not limited to data protection,

[166] Kao, D.-Y. (2015) Performing an APT Investigation: Using People-Process-Technology-Strategy Model in Digital Triage Forensics. – *39th IEEE International Computers, Software & Applications Conference,* Taiwan, 1-5 Jul. 2015, (Eds.) Sheikh Iqbal Ahamed, Carl K. Chang, William Chu, Ivica Crnkovic, Pao-Ann Hsiung, Gang Huang, and Jingwei Yang, Los Alamitos, CA : IEEE Computer Society.

confidentiality obligations, cross-border data sharing and e-discovery, liability under data protection, contractual precautions; and technical aspects, including, but not limited to risk assessment, measure recommendations on in-house security, recommendations on evaluating security measures and procedures of service providers.

Conclusion

In order to summarize the findings of this paper, it is prudent to revisit the hypothesis. As stated in the introduction to this paper, the initial hypothesis of this paper is that the use of the cloud storage and online cloud-based tools by law firms in the course of their work for the purposes of storing documentation wholly or partially compromises the data rights and freedoms of their clients and undermines the confidentiality between a legal professional and a client.

It is now possible to answer that cloud data storage creates a rather severe risk of compromising the clients' data. The control over the data is largely being surrendered to the service provider, but the responsibility mainly lays with the law firm. The cloud technology itself in the opinion of the industry had not finished its development, therefore, there is the risk of unknown exploits with unknown protections. This risk can be mitigated by employing security procedures inhouse, taking all necessary precautions, including contractual precautions, in choosing the provider and monitoring the service provider with regards to security procedures and measures, however, it can not be fully eliminated due to the technology itself not having reached its maturity yet.

Legal professional in this context ends up balancing in a very precarious position – professional obligations such as professional secrecy, role of the data controller and oversight to be exercised over the clients and service providers are bound to become rather difficult. Major stress of the compliance is on the law firm as the data controller, therefore it is crucial for a legal professional or a law firm not only to fulfil their own obligations as data controllers impeccably, but also to be very cautious in dealing with service providers, as improperly drafted controller-processor agreement may lead to liability for breaches of the GDPR resting almost solely on data controller's shoulders.

Even though the argument with regards to cloud storage providers being quite removed from the data, as they essentially only provide the means of processing,[167] is quite reasonable in its own right, whoever uses those services is far from being fully in control in using them. This allows to suggest, that cloud service providers will remain data processors in the eyes of the judiciary for the reasons of enforceability.

Nevertheless, it was additionally important to describe the data protection in general, as it is necessary for a legal professional or a law firm to be fully aware of the rights of their clients in

[167] Kuan Hon, W., Milliard, C., Walden, I. (2012) *supra nota*, 10.

order to be able to appropriately respond to them and provide appropriate guidance to their conduct in order to safeguard not only the clientele but also themselves.

In that context, existing guidelines on the European level are currently lacking not only specific guidance with regards technical measures to assist legal professionals with compliance, but also a number of legal issues due to changes circumstances. Hopefully, this paper provides enough cause for legal professionals and relevant regulatory bodies to adapt to new circumstances and update existing framework.

Bibliography

Books

1. Weber, R. H., Staiger, D. (2017) Transatlantic data protection in practice. Berlin: Springer-Verlag GmbH.

Articles

2. Ahmed, H. et al (2016) Data security issues in cloud computing: review. – *International Journal of Software Engineering and Computer Systems*, Vol 2, 58-65.

3. Binns, R.(2017) Data protection impact assessments: a meta-regulatory approach. - *International Data Privacy Law*, Vol. 7, No. 1, 22-35.

4. Crowley, M.G et al (2016) Protecting corporate intellectual property: legal and technological approach. - *Business Horizons*, Vol 59, 627-628.

5. D'Amore, F., Pirone, F (2018) Doctor 2.0. and i-Patient: information technologu in medicine and its influence on the physician-patient relationship. – *Italian Journal of Medicine*, Vol. 12, No. 1, 1-4.

6. Drotsky, G.A.P. et al (2005) The influence of information and communication technology on the selling activities of the professional sales representative. – *Acta Commercii*, Vol. 5, No. 1, 96-105.

7. Eva, E. (2015) Lawyers' legal professional privilege in Europe. - SEA - Practical Application of Science, Vol. 3, No. 1(7), 33-38.

8. Gibson, D.. et al (2018) Evolving Learning Paradigms: Re-Setting Baselines and Collection Methods of Information and Communication Technology in Education Statistics. – *Educational Technology and Society*, Vol 21, No. 2, 62-73.

9. Gonzalez, E.G, De Hert, P. (2019) Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles. – *ERA Forum*, Vol. 19, 597-621.

10. Gonzales-Diaz, F.E., Stuart, P. (2017) Legal professional privilege under EU law: current issue. – *Competition law and policy debate*, Vol. 3, No. 3, 56-65.

11. Graham, G. (2012) Lost in a Cloud: Overview of the legal obstacles to the growth of cloud computing. – Medijska Istrazivanja, Vol. 18, No. 2, 21-31.

12. de Hert, P., Papakonstantinou, V., Kamara, I. (2016) The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection. - *Computer law and security review*, Vol. 32, 16-30.

13. Holtz, J. (2013) Legal Professional Privilege in Europe: a Missed Policy Opportunity. - *Journal of European Competition Law & Practice*, Vol. 4, No. 5, 402-412.

14. Jayapandian, N. et al (2016) Improved Cloud Security Trust on Client Side Data Encryption using HASBE and Blowfish. - *Green Engineering and Technologies*, Coimbatore, India, 19 November 2016.

15. Jiang, Z.L. et al (2013) Maintaining Hard Disk Integrity With Digital Legal Professional Privilege (LPP) Data. – *IEEE Transactions on Information Forensics and Security*, Vol. 8, No. 5, 821-828.

16. Joint, A., Baker, E., Eccles, E. (2009) Hey, you, get off that cloud? - *Computer law and security review*, Vol. 25, 270-274.

17. Kamarinou, D., Milliard, C., Kuan Hon, W. (2016) Cloud privacy: an empirical study of 20 cloud providers' terms and privacy policies - Part I. - *International Data Privacy Law*, Vol. 6, No. 2, 79-101.

18. Kamarinou, D., Milliard, C., Kuan Hon, W. (2016) Cloud privacy: an empirical study of 20 cloud providers' terms and privacy policies - Part II. - *International Data Privacy Law*, Vol. 6, No. 3, 170-194.

19. Kao, D.-Y. (2015) Performing an APT Investigation: Using People-Process-Technology-Strategy Model in Digital Triage Forensics. – *39th IEEE International Computers, Software & Applications Conference,* Taiwan, 1-5 Jul. 2015, (Eds.) Sheikh Iqbal Ahamed, Carl K. Chang,

William Chu, Ivica Crnkovic, Pao-Ann Hsiung, Gang Huang, and Jingwei Yang, Los Alamitos, CA : IEEE Computer Society.

20. Kennedy, E., Millard, C. (2016) Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU Member States. - *Computer law and security review*, Vol. 32, 91-110.

21. King, N.J., Raja, V.T. (2012) Protecting the privacy and security of sensitive customer data in the cloud. - *Computer law and security review*, Vol. 28, 308-319.

22. Kuan Hon, W., Milliard, C., Walden, I. (2011) The problem of 'personal data' in cloud computing: what information is regulated?—the cloud of unknowing. - *Internationasl Data Privacy Law*, Vol. 1, No. 4, 211-228.

23. Kuan Hon, W., Milliard, C., Walden, I. (2012) Who is responsible for 'personal data' in cloud computing? —the cloud of unknowing. - *International Data Privacy Law*, Vol. 2, No. 1, 3-18.

24. Kuan Hon, W. et al (2016) Policy, legal and regulatory implications of a Europe-only cloud. - *International Journal of Law and Information Technology*, Vol. 24, 251-278.

25. Kulesza, J. (2014) Transboundary data protection and international business compliance. - *International Data Privacy Law*, Vol. 4, No. 4, 298-306.

26. Lindquist, J. (2018) New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things? - *International Journal of Law and Information Technology*, Vol. 26, 45-63.

27. Masur, M.J. (1999) Safety in Numbers: Revisiting the Risks to Client Confidences and Attorney-Client Privilege Posed by Internet Electronic Mail. - Berkeley Technology Law Journal, Vol. 14, No. 3, 1117-1162.

28. McGillivray, K. (2016) A right too far? Requiring cloud service providers to deliver adequate data security to consumers. - *International Journal of Law and Information Technology*, Vol. 25, 1-25.

29. Mikkonen, T. (2014) Perceptions of controllers on EU data protection reform: a Finnish perspective. - *Computer law and security review*, Vol. 30, 190-194.

30. Murphy, G.(2009)Is it time to rebrand legal professional privilege in EC competition law? An updated look. – *Commonwealth Law Bulletin*, Vol. 35, No. 3, 443-461.

31. Quelle, C. (2018) Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach. – *European Journal on Risk Regulation*, Vol. 9, 502-526.

32. Rodrigues, R. et al (2016) The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR. - *International Review of Law, Computers & Technology*, Vol.30, No. 3, 248-270.

33. Romanou, A. (2018) The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. - *Computer law and security review*, Vol. 34, 99-110.

34. Ryz, L. et al (2016) A new era in data protection. – *Computer Fraud and Security*, Vol. 2016, No. 3, 18-20.

35. Sullivan, C. (2014) Protecting digital identity in the cloud: Regulating cross-border data disclosure. - *Computer law and security review*, Vol. 30, 137-152.

36. Tancock, D. et al (2010) A Privacy Impact Assessment Tool for Cloud Computing. - *2nd IEEE International Conference on Cloud Computing Technology and Science*, USA, 30 Nov.-3 Dec. 2010, (Eds.) Judy Qiu, Gansen Zhao, and Chunming Rong, Los Alamitos, CA : IEEE Computer Society, 667-676.

37. Ursic, H. (2018) Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control. - *SCRIPTed*, Vol. 15, No. 11, 42-69.

38. Veale, M. et al (2018) When data protection by design and data subject rights clash. – *International Data Privacy Law,* Vol. 8, No.2, 105-123.

39. Webley, L. (2016) Interception of communications and legal professional privilege and the rule of law. - *Legal Ethics*, Vol. 19, No.1, 173-176.

40. Wolters, P.T.J. (2017) The security of personal data under the GDPR: a harmonized duty or a shared responsibility? - *International Data Privacy Law*, Vol. 7, No. 3, 165-178.

41. Zanfir, G. (2012) The right to Data Portability in the context of the EU data protection reform. - *International Data Privacy Law*, Vol. 2, No. 3, 149-162.

42. Zech, H. (2016) A legal framework for a data economy in the European Digital Single Market: rights to use data. - *Journal of Intellectual Property Law and Practice*, Vol. 11, No. 6, 460-470.

Theses

43. Färjsjö, F., Stenberg, E. (2017)Ensuring Continuous Security in the Cloud and Compliance with GDPR. (Master's thesis) University of Uppsala, Department of Technology and natural sciences, Uppsala.

44. Taka, A-M. (2017) Cross-Border Application of EU's General Data Protection Regulation (GDPR) - A private international law study on third state implications. (Master's thesis) University of Uppsala, Department of Law, Uppsala.

Legislations

45. Regulation (EU) No 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, 4.5.2016, p 1-88 4.5.2016.

Case Law

46. Court decision, 14.09.2010, Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v European Commission, C-550/07, ECLI:EU:C:2010:512.

47. Court decision, 18.05.1982, AM & S Europe Limited v Commission of the European Communities, 155/79, ECLI:EU:C:1982:157.

48. Harleysville Insurance Company v Holding Funeral Home Inc., No. 1:15 cv 00057, 2017 U.S. Dist. LEXIS 18714 (W.D. Va. Feb. 9, 2017).

49. Court decision, 02.03.1994, Hilti AG v Commission of the European Communities, C-53/92 P, ECLI:EU:C:1994:77.

Other

50. Article 29 Data Protection Working Party (2010) *Opinion 1/2010 on the concepts of "controller" and "processor"*. Accessible: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf, 16 March 2019.

51. Black, N. (2017) *Significantly more lawyers using cloud computing in 2017*. Accessible: http://www.legalnews.com/washtenaw/1449844, 16 March 2019.

52. Clio (2017) *Why Law Firms are moving to the cloud.* Accessible: http://www.nysba.org/WorkArea/DownloadAsset.aspx?id=78979, 16 March 2019.

53. Council of Bars and Law Societies of Europe (2018) CCBE Guide On Lawyers' Use Of Online Legal Platforms. Brussels: CCBE.

54. Council of Bars and Law Societies of Europe (2012) CCBE Guidelines On The Use Of Cloud Computing Services By Lawyers. Brussels: CCBE.

55. CCBE (2016) *CCBE Recommendations on the protection of client confidentiality within the context of surveillance activities.* Accessible: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20160428_CCBE_recommendations_on_the_protection_of_client_confidentiality_within_the_context_of_surveillance_activities.pdf, 16 March 2019.

56. CCBE (2016) *CCBE response regarding the European Commission public consultation on cloud computing.* Accessible: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20110909_CCBE_Response_on_Cloud_Computing.pdf, 7 May 2019.

57. CCBE (2017) *CCBE Statement of professional secrecy/Legal professional privilege(LLP)*. Accessible: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_Postion_Papers/EN_DEON_20170915_Statement-on-professional-secrecy_LPP.pdf, 16 March 2019.

58. CCBE (2013) Charter of core principles of the European legal profession and Code of conduct for European lawyers. Brussels: CCBE.

59. CCBE (2004) *Regulated legal professionals and professional privilege within the European Union, the European Economic Area and Switzerland, and certain other European jurisdictions.* Accessible: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_Reports/EN_DEON_20040227_Fish_report.pdf, 16 March 2019.

60. CCBE (2003) *The professional secret, confidentiality and legal professional privilege in Europe.* Accessible: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_Reports/EN_DEON_20030930_Update_of_th_Edwards_report.pdf, 16 March 2019.

61. CCBE (1976) *The professional secret, confidentiality and legal professional privilege in the nine member states of the European community.* Accessible: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_Reports/EN_DEON_19761029_Edwards_report.pdf, 16 March 2019.

62. Clio (2019) *About Clio*. Accessible*:* https://www.clio.com/eu/, 16 March 2019.

63. Clio (2019) *About Clio.* Accessible: https://www.linkedin.com/company/clio---cloud-based-legal-technology/about/, 5 May 2019.

64. Cohen, M.A. (2017) *Global Legal Tech is Transforming Service Delivery.* Accessible: https://www.forbes.com/sites/markcohen1/2017/08/29/global-legal-tech-is-transforming-service-delivery/#57e0ac811346, 5 May 2019.

65. Committee on professional ethics of New York State Bar Association (2010) *Opinion 842*. Accessible: http://www.nysba.org/CustomTemplates/Content.aspx?id=1499, 16 March 2019.

66. Columbus, L. (2017) *2017 State of Cloud Adoption and Security.* Accessible: https://www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoption-and-security/, 5 May 2019.

67. Dimka, D. (2016) *The Zero-Paper Law Firm - The Ultimate Guide to Going Paperless.* Accessible: https://uptimelegalworks.com/resources#ebooks, 8 October 2018.

68. European Commission (2019) *Adequacy decisions.* Accessible: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en, 20 March 2019.

69. European Commission (2019) *E-evidence – cross-border access to electronic evidence.* Accessible: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en#internaleurulesproposaloneevidence, 7 May 2019.

70. ICO (2014) *Data controllers and data processors: what the difference is and what the governance implications are*. Accessible: https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf, 16 March 2019.

71. Kennedy, D. (2019) *Techreport 2018: Cloud computing.* Accessible:https://www.lawtechnologytoday.org/2019/01/techreport-2018-cloud-computing/, 5 May 2019.

72. Lim, R. (2017) *Cultivating Innovation in risk-averse legal industry*. Accessible: http://insight.thomsonreuters.com.au/posts/innovation-risk-averse-legal-industry, 5 May 2019.

73. Litify (2017) *10 Cloud Security Best Practices For Attorneys and Law Firms.* Accessible: https://www.litify.com/10-cloud-security-best-practices-attorneys-law-firms/, 16 March 2019.

74. Parker, N. et al (2017) *GDPR and data protection issues in cross-border regulatory investigations.* Accessible: www.allenovery.com/publications/en-gb/lrrfs/continental%20europe/Pages/GDPR-and-data-protection-issues-in-cross-border-regulatory-investigations.aspx, 8 October 2018.

75. Szabo, O. (2017) *The status of legal tech in Central Eastern Europe: 2017 in Retrospective*. Accessible: https://investcee.hu/status-of-legaltech-in-central-eastern-europe/ , 16 March 2019