RIGA GRADUATE SCHOOL OF LAW

Application of the Article 28 (3) of the General Data Protection Regulation in contemporary Software as a Service ("SaaS") business.

MASTER'S THESIS

AUTHOR: ĪLAJS LIJS
LL.M 2018/2019 year student
Student number: M015091

SUPERVISOR: Edvijs Zandars
LL.M

DECLARATION OF HONOUR:

I declare that this thesis is my own work, and that all references to, or quotations from, the work of others are fully and correctly cited.

……

RIGA, 2019

SUMMARY

On 25 May 2018 the General Data Protection Regulation ("GDPR") came into force in the European Union. Inspired by the rapidly growing technologies, the regulation aims to formalize and reinforce the already existent data protection framework established by Directive 95/46/EC and clarified by the EU case law. One of the requirements being subject to improvement is reflected in the Article 29 (3) of the GDPR which requires processing to be based on the legally binding "*legal act or contract*" between processor and controller that governs the processing of personal data on behalf of controller ("DPA"). Moreover, GDPR has introduced the variety of specific content requirements that parties must include in their DPA's.

The contemporary software market is swiftly transforming its software delivery strategy into *Software as a Service* model which entails the complex multi-role (processor, controller, joint controllers, sub-processors), "*multi-tenant*" software delivery model which typically involves processing of personal data on a large scale.

Therefore, for the purposes of this thesis, regulatory requirements associated with DPA are subject to interpretation in context of SaaS delivery models widely adopted by prominent SaaS providers. In addition, the author argues that, multiple parties processing personal data leads to problems in determining the correct processing role. Thereby, parties may struggle in meeting the requirements of the Article 28 (3) of the GDPR. Failure to ensure that processing is covered by the proper DPA is regarded as infringement of the GDPR. For that reason, thesis seeks to stress out complications associated with structuring DPA's and provides recommendations on how to structure DPA's according to the selected model.

ABBREVIATIONS

Art 29. WP	Article 29 Data Protection Working Party
BP	Business Process
CJEU	Court of Justice of the European Union
CRM	Customer-relationship management
DPA	Data Processing Agreement or "contract or other legal act" referred to in the Article 28 (3) of the GDPR
ERP	Enterprise resource planning
EU	European Union
EULA	End-User License Agreement
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
IS	Information Security
IP	Internet Protocol
OSV	Original Software Vendor
PIA	Privacy Impact Assessment
SaaS	Software as a Service
SLA	Service Level Agreement
T&C	Terms and Conditions
TFEU	Treaty of the Functioning of the European Union
VAR	Value Added Reseller

Table of Content

1. INTRODUCTION

We live in an age of information and digital technologies. The age in which information technologies have found its application in nearly all aspects of our lives. Information technologies are designed to improve the quality of our lives by automating processes, reducing costs, increasing productivity and developing user experience. According to the Oxford Dictionary, Information Technology is the "*study or use of systems (especially computers and telecommunications) for storing, retrieving, and sending information.*"[1] Therefore, the evolution of information technologies leads to significant changes in data processing environment. For the past twenty years, the capacity of data processing hardware and software[2] has grown substantially, overcoming all traditional boundaries in distribution of data.[3] That resulted in the evolution of information technologies that is manifested by the rapid technological development and widespread use of online services, such as social networking, ecommerce platforms, online banking, "*Internet of Things*" and "*XaaS*" ("*X as a Service*" or "*Anything as a Service*").

The rapid growth is especially vivid in the *SaaS* delivery model that is built on the "*multi-tenant*", "*one-to many*" principles and involves provision of software along with underlining infrastructure by SaaS provider via Internet.[4] Provision of SaaS can be administered almost instantly, after customer subscribes for the respective SaaS product. As a result, SaaS providers are having huge customer reach, given that provision of SaaS is not confined to specific location and has little or no technical requirements. However, the nature of SaaS requires SaaS providers to aggregate and process massive amount of data, including personal data, which inevitably leads to information security and trust issues.

Gartner, one of the leading research companies, predicts that SaaS revenues will reach $85 billion in 2019[5] and by 2020, 90% of all the software will be provided on a subscription-based business model. Transformation of software business will eventually result in SaaS companies seeking to increase their competitiveness by adding more features and functionality which inevitably increases the processing scope.

By offering easily accessible, constantly maintained, and supported solutions, SaaS providers are gaining more trust from customers. The trust is signified by customers entrusting their data and allowing SaaS companies to manage their BP. However, such trust must not be betrayed. Large scale processing creates many challenges ensued from the limited control over data in addition to various information security risks. The latter may cause harm data subjects and online market in general, unless appropriate measures are taken.

---

[1] Oxford Living Dictionaries, available on: https://en.oxforddictionaries.com/definition/information_technology. Accessed May 2, 2019.
[2] Mariusz Krzysztofek, *GDPR: General Data Protection Regulation (EU) 2016/679 Post-Reform Personal Data Protection in the European Union*, 2016, Available on: Wolters Kluwer Digital Book Platform. Accessed April 12, 2019. p. 3.
[3] Ziccardi G. Resistance, Liberation Technology and Human Rights in the Digital Age. Dordrecht: Springer Netherlands, 2013, p. 29.
[4] Gartner IT Glossary, available on: https://www.gartner.com/it-glossary/software-as-a-service-saas/. Accessed May 2, 2019.
[5] Gartner SaaS Forecast, available on: https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019. Accessed May 2, 2019.

As a result, not only that creates obstacles for *European Digital Single Market* objectives but poses a threat to the right to privacy, which has been generally recognized by EU as fundamental right.[6]

Even a glimpse to the evolving technologies and corresponding challenges was enough for European Commission to conclude that Directive 95/46/EC, that had been drafted in the early nineties, simply failed to match challenges posed by the "*Digital Age*". As a result, on 6th of April 2016 European Commission adopted a data protection reform package[7] that included the GDPR.

GDPR is in effect as of 25th of May 2018, and consequently, the existing data protection laws and regulations of EU member states implementing Directive 95/46/EC are being repealed or amended. According to the Article 288 of the TFEU, regulations have direct application to all Member States without the need to be implemented. Hence, GDPR denotes an important step towards the unification of data protection rules in the European Union and beyond.

The unified framework of data protection laws within the EU benefits the businesses operating internationally[8] and increases legal certainty. Taking into consideration the extended territorial reach of the GDPR[9], more businesses will be forced to adapt the same level of data protection standards if they wish to operate within the EU[10]. As Brad Smith, Microsoft's president and chief legal officer stated:

> "*We believe privacy is a fundamental human right. GDPR is an important step forward for people in Europe and around the world*".[11]

SaaS providers that happen to process massive amount of personal data are enjoying the free movement of personal data between the EU member states and have easier access to the European single market. Another benefit is that GDPR is regarded as a stand-alone legal act that is binding and can be invoked directly[12] without resorting to any of the national laws of EU member states. Nevertheless, businesses should bear in mind that GDPR allows member states to possess the autonomy in adapting their national data protection laws. However, autonomy is

---

[6] *Fuster, Gloria Gonzalez, Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer, 2014. P. 232.,* see. Article 16 (1) of the TFEU and Article 8(1) of the Charter of Fundamental Rights of the European Union.

[7] European Commission, General Data Protection Regulation enters into application, available on: https://ec.europa.eu/commission/news/general-data-protection-regulation-enters-application-2018-may-25_en. Accessed May 4, 2019.

[8] Mariusz Krzysztofek, *GDPR: General Data Protection Regulation (EU) 2016/679 Post-Reform Personal Data Protection in the European Union*, 2016, Available on: Wolters Kluwer Digital Book Platform. Accessed April 12, 2019. p 3.

[9] Article 3 of the GDPR.

[10] EU Commission. *The GDPR: new opportunities, new obligations. What every business needs to know about the EU's General Data Protection Regulation*. Luxembourg: Publications Office of the European Union, 2018. Page 2, available on: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf. Accessed May 8, 2019.

[11] Microsoft IT Security, available on: https://www.microsoft.com/en-mt/rethink-IT-security/gdpr.aspx. Accessed May 8, 2019.

[12] Article 99 (2) of the GDPR.

limited to certain areas provided in the GDPR[13] and to the extent there is no conflict with the EU law.[14]

GDPR emphasizes that, apart from contributing to "*accomplishment of an area of freedom, security and justice*" it also focuses on "*economic and social progress*" and "*strengthening and the convergence of the economies within the internal market*"[15]. This can be interpreted as intention to facilitate the economic processes at the same time avoiding application of measures to block or restrict businesses. Instead, GDPR aims to bring clarity in terms of obligations to protect fundamental rights to privacy. The unified system of rules pertaining to IS benefits businesses by forcing them to adapt a unified data protection compliance strategy across EU. By doing so, businesses can avoid costs in evaluating a national law of EU member states they want to operate[16] in. At the same time, processing of data in a secured, transparent, and controlled manner results in gaining more trust among consumers.

Whereas GDPR introduced a range of new rights and obligations pertaining to processing of personal data in a "*Digital Age*" (e.g. *right to portability*[17]), the core data protection principles were already defined in the Directive 95/46/EC and are currently incorporated in the GDPR. One important feature that must be emphasized is that GDPR imposes very harsh administrative fines of amounting "up to *20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher*[18]*"*. Perhaps one of the reasons for such measures is to address international corporations that process data on a large scale. Before now, such corporations were generally unaffected by the fixed fines imposed under the previous data protection framework. However, the turnover based fines, applied to the entire company group will most definitely incentivize businesses to regard incompliance with data protection laws not only as serious reputational risk but indeed a huge variable in their financial risk management matrix.

Any compliance obligations supported by the harsh administrative fines forces companies to adapt new rules, and, in some cases, even re-design their compliance strategy to achieve compliance. ISO Survey reveals that number of entities certified for ISO 27001 Information Security Management has increased to 20% in the 2016[19] (prior to GDPR entry into force) which indicates that companies have been widely preparing for the GDPR.

One of the obligations that was originally included in the Directive 95/46/EC but was reinforced by GDPR is Article 28 (3) of the GDPR. Article 28 (3) lays down specific content

---

[13] Recital 8 of the GDPR

[14] Judgment of the Court of Justice of the European Union (CJEU) of 15 July 1964 in Case 6/64 Costa v E.N.E.L., http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:61964CJ0006, and the CJEU judgment of 10 December 1969 in joined Cases 6 and 11-69 Commission of the European Communities v French Republic http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:61969CJ0006.

[15] Recital 2 of the GDPR.

[16] Of course, the interpretation of norms and application penalties in individual member states may differ. For example, in application of fines. On 3rd October 2017 Art.29.WP adopted the "Guidelines on the application and setting of administrative fines for the purposes of the GDPR". These guidelines should serve as a basis for application of administrative fines. Thereafter, individual member states are creating their own guidelines.

[17] Article 20 of the GDPR

[18] Article 83 (5) of the GDPR

[19] ISO 27001 certification figures, available on: https://www.itgovernance.co.uk/blog/iso-27001-certification-figures-increase-by-20 Accessed on May 9, 2019.

requirements that must be included in DPA between controller and processor. Nevertheless, these requirements are quite flexible and thereby enable parties to individualize DPA to fit the specific processing operations. However, the interpretational flexibility most probably lead to unclarity as to how to adjust these content requirements to the particular service or product.

The prerequisite for drafting an effective DPA is a clear understanding of the nature of processing and an ability to determine the role prior to engaging in processing. This becomes complicated in terms of SaaS delivery model which usually involves multiple parties (including but not limited to SaaS provider, VAR, SaaS vendor, data storage provider) performing, and, in some cases, controlling different processing operations.

Therefore, the thesis seeks to address these complications and provide guidelines for assisting parties in creating an effective DPA, which is designed to outline the rights and obligations of the parties, raise information security awareness, and strengthen the right to privacy.

1.1. Hypothesis and Research Questions

The aim of the thesis is to outline and clarify the challenges in interpreting and structuring DPA's in light of the complex multi-party SaaS delivery contracts. The following questions are being addressed:

1) Why the multi-party SaaS product delivery model require a detailed analysis of the processing to determine and assign the processing role (Art.4(7); Art.4(8); Art.28(2)) in a DPA? What are the factors determining the processing role in the SaaS contract?
2) How companies are dealing with execution of DPA's? What is the common practice in international, scalable business model? What are solutions used by large vendors, such as Microsoft and Amazon?
3) How to interpret and fill in the DPA content requirements set forth in the Article 28 (3) in the perspective of multi-party SaaS delivery model? Under which circumstances the purpose of DPA can be obstructed?

The thesis will seek to expound the problems associated with structuring DPA's according to the assigned processing role. Therefore, the author sets forth the following hypotheses:

a) Having regards to the (i) multi-party agreement structure common to the SaaS product delivery; (ii) flexibility in interpreting and adjusting content requirements pursuant to the Article 28 (3) of the GDPR; (iii) absence of detailed guidance issued by Data Protection Authorities pertaining to interpretation of Article 28 (3), SaaS providers are experiencing problems in the proper fulfilment of the DPA requirements according to the GDPR objectives. Therefore, current regulatory framework is of need of a clear guidance on structuring DPA's in the multi-role SaaS delivery models.
b) Regardless of the SaaS agreement structure, DPA must be entered into by the factual processor and controller.

1.2. Research Methods and Sources

The reasoning outlined in this thesis chiefly relies on the interpretation of the Article 28 (3) and related provisions of the GDPR while taking into account specifics of the SaaS technology. That is why, the text of the GDPR will serve as the primary source for this thesis, whereas well respected and renown IT research companies will provide insight on SaaS technology and its legal aspects.

For the purposes of providing guidance on structuring DPA's, thesis will contain the description of processing roles that is based on interpreting GDPR as a primary source and Art.29.WP guidelines as secondary source. The CJEU case law is used to demonstrate the issues related to interpretation of the types of personal data.

For interpretation of the DPA content requirements outlined in the Article 28 (3) of the GDPR, author will apply teleological method to illustrate the "spirit" of the article and the intention of the legislators in requiring parties to engage in a DPA. Furthermore, in the interpretation of the content requirements, the secondary sources, such as guidelines issues by Data Protection Authorities are examined. The systemic analysis will be applied to demonstrate the interaction between the Article 28 (3) and other provisions of the GDPR. In so doing, thesis will demonstrate the correlation between content requirements and the general principles of the GDPR.

The thesis will not only focus on underlining the problems in application of Article 28 (3) in SaaS but provide some guidance in drafting the standard data processing agreements in different processing scenarios. For that reason, the thesis will rely on the GDPR as the primary source for determining the mandatory provisions of the DPA and the general principles of contract law to suggest the alternative provisions the parties may consider for inclusion in a draft DPA.

2. INTRODUCTION TO SAAS TECHNOLOGY

The key feature of the SaaS delivery model is that software is delivered via Internet[20] and is managed, maintained and supported by SaaS provider and/or its suppliers. Customer, in this regard is responsible only for configuring user-specific parameters and managing its users, whereas SaaS provider is responsible for all the infrastructure[21], network, servers, operating systems, storage, and individual application capabilities[22]. The examples of SaaS products are ERP, CRM, service desk management, human resource management tools. According to the G2 research, the largest companies applying SaaS models include Google, Adobe, Slack, Microsoft, ServiceNow and Salesforce.[23]

To better illustrate the nature of the SaaS delivery model, the key difference between the traditional "*on-premise*" model and SaaS model must be illustrated. The main difference between "*on-premis*e" software delivery and SaaS is that delivery of on-premise software is a transaction in which software license (copy of a software) is delivered to a customer. Consequently, customer is responsible for obtain the hardware and expertise to install, maintain and support an infrastructure necessary to run a software, while taking account of appropriate information security. Typically, such model involves greater costs comparing to SaaS products, especially for small and medium sized businesses.

By comparison, the essence of the SaaS transaction is the grant of access to a software via Internet.[24] Subsequently, software is not tied to a specific access point and is available across different platforms while entirely managed, updated, supported and deployed by a SaaS provider (provided however, that customer is paying the recurring fee, payable in multiple models, i.e. pay-as-you-go and subscription based). Evidently, the SaaS business is growing rapidly and expanding to incorporate more BP functionality.

The benefits of the SaaS model are leading to greater popularity and corresponding shift to SaaS model by many software vendors, including software market giants such as Microsoft.[25] As a result, the traditional "*on-premise*" software will no longer be a viable option for customers.

Consequently, customers will have to deal with challenges associated with the new software delivery model. Of course, SaaS is a double-edged sword. Automatic, multi-tenant, cloud-based service provisioning implies less control over customer data. And the growing trend and capability of SaaS businesses to undertake more technical and business processes will cause greater risk to the business critical and sensitive data categories, e.g. payroll data, confidential information, social security numbers, individual key performance indicator (KPI) models.

---

[20] Marioara Maxim, The Rights and Obligations of the Main Stakeholders in Cloud Computing Services, 4 Persp. Bus. L.J. 190 (2015) page 192.

[21] Michael J. Kavis, *Architecting the Cloud, Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)*, Wiley, p. 51.

[22] Ibid. p.52.

[23] Best Software companies, available on: https://www.g2.com/best-software-companies. Accessed May 10, 2019.

[24] David W.Tollen, *The Tech Contracts Handbook, Second Edition, Cloud Computing Agreements, Software Licenses, and Other IT Contracts for Lawyers and Businesspeople*. Part 1, Location 218 of 5176. Amazon Kindle Version.

[25] Microsoft as a Service, available on: https://www.pcmag.com/article/346287/microsoft-as-a-service-and-the-slow-death-of-on-premises-sof. Accessed May 9, 2019.

Customer's inability to apply most of information security controls to the SaaS environment, besides basic customer-tailored security customization will not relieve customers from being ultimately responsible for the security of their data. As being qualified as data controllers, customers are obliged to "*use only processors providing sufficient guarantees to implement appropriate technical and organisational measures"* [26] to meet the GDPR requirements.

On that account, GDPR has pressured companies to invest in information security with a forecast of $124 Billion in 2019.[27] GDPR also creates opportunities for growth in the information security product sector. Accordingly, customers are not tending to select the most suitable SaaS provider by the means of IS due-diligence process. IS due diligence is used to compare the IS strategy and commitment undertaken by potential SaaS providers.

Consequently, SaaS providers are being forced to employ up-to-date security measures in order to fulfil the new market standard associated with IS. It is true to say that being GDPR compliant has been a good sales opportunity and part of the value proposition among various SaaS providers that are now labelling their services as "*GDPR-compliant*" and thereby gaining competitive advantage in the market.

Sometimes, customers are misled by perception that SaaS provider is the sole entity carrying out the processing of personal data of their behalf. In fact, customer must be aware that it is quite common for SaaS product to integrate multiple elements within its offering that are, in fact, being delivered by its sub-contractors. That eventually creates a supply chain composed of entities responsible for different processing activities, and therefore exposed to the different security risks.

When customer is signing an agreement with SaaS provider or VAR as a main data processor, the data processing functions are often being delegated to multiple parties. That is why, data processing flow and corresponding contractual structure must be carefully considered in carrying out pre-contractual IS due diligence for conducting proper security risk assessment in relation to SaaS products.

The section 4 of this thesis describe the role of each party within the processing of personal data and accordingly will provide recommendations concerning the structuring the contractual relationship to secure the objectives of the GDPR.

[26] Article 28 (1) of the GDPR.
[27] Gartner on security spending, available on: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019. Accessed May 19, 2019.

3. INTRODUCTION TO THE ARTICLE 28 (3) OF THE GDPR

The obligation to enter into a DPA between controller and processor for the processing of personal data is not entirely new. Article 17 (3) of the Directive 95/46/EC required processing to "*be governed by a contract or legal act binding the processor to the controller*". That contract would stipulate that processing is carried out according to the instructions from the controller and obliged processor to take appropriate measures to keep the personal data secure.

Assuming that prior to GDPR entry into force, controllers and processors have already established a baseline for compliance with Directive and their respective national law, the Article 28 (3) of the GDPR has been tailored to extend the requirement of Article 17(3) of the Directive 95/46/EC to include more concrete content requirements.

That means that processing must have been already supported by a written contract stipulating terms for processing of personal data between controller and processor. One of the objectives of the GDPR is to facilitate the progress and economic growth[28] which implies the lack of substantial administrative burden. Therefore, companies were supposed to review and amend their existing contracts[29] and establish the correct contractual framework throughout the processing supply chain. [30]

3.1. Legal Background of the Data Processing Agreement

A contract is the formalization of rights and obligations of parties with respect to particular lawful action or omission.

Contractual law provides that one of the vital principles of the contemporary civil law is freedom of contract. Freedom of contract is the main and most used aspect of the principle of private autonomy. It is an essential part of the free market, which ensures effective exchange of goods based on relevant supply and demand.[31]

On the other hand, unrestricted freedom of contract might be incompatible with others civil law basic principles, such as good faith, equivalence or fairness. History of law provides a lot of examples how such unrestricted freedom could actually be harmful. In the 19th century civil law theory postulated unrestricted and absolute freedom of contract. It could be explained with legal assumption of those times, that contractual parties are equal. Obviously, such an approach led to disproportionality in contractual relationships, which forced legislators to intervene in contractual affairs of the private parties and make some amendments.[32]

Article 1:102 of the Principles of the European Contract Law states - parties are free to enter into a contract and to determine its contents, subject to the requirements of good faith and fair dealing,

---

[28] Recital 2 of the GDPR.
[29] Paul Voigt, Axel von dem Bussche. *The EU General Data Protection Regulation (GDPR). A Practical guide. Germany*, 2017. P. 82.
[30] Nick Pantlin, Claire Wiseman, Mariam Everett, *Supply chain arrangements: The ABC to GDPR compliance – A spotlight on emerging market practice in supplier contracts in light of the GDPR*. Harbert Smith Freehills LP, London, UK, P. 2.
[31] Torgans K., Kārkliņš J., Bitāns A., Līgumu un deliktu problēmas Eiropas Savienībā un Latvijā. Prof. K.Torgāna zinātniskā redakcijā. Rīga: Tiesu namu aģentūra, 2017, 45. lpp.
[32] K. Balodis. Ievads Civiltiesībās. Rīga: Zvaigzne ABC, 2007, 178. lpp.

and the mandatory rules established by these Principles.[33] It is clear, that with all due respect to the freedom of contract, authors of the Principles of the European Contract Law also recognized necessity to restrict this freedom in order to comply imperative legal norms, which, mostly, are called upon in order to protect vital goods and freedoms of the state and society.

One may argue that, according to the general principles of European contract law, the contract is concluded if the following vital elements are in place: (i) the parties intend to be legally bound[34]; and (ii) parties reach a sufficient agreement.[35] In presence of the aforesaid two elements contracting parties possess contractual autonomy to reach an agreement on the chosen terms and have intention to be bound by Data Processing Agreement to subsequently abide its terms.

In contrast, GDPR obliges controller and processors to enter into a written[36] contract or legal act and provides its mandatory content. On top of that, unlike the Directive 95/46/EC, GDPR outlines the specific obligations pertaining to processor with respect to controller, that might be regarded as limiting the contractual freedom of the parties.[37]

Having regard to the fact that DPA's content requirements are consistent with other provisions of the GDPR (which are directly binding to processor), and as further argued are derived from the principles of processing[38], processor that processes personal data in compliance with GDPR, must be, by default, capable to conform to the minimum content requirements of Article 28 (3) of the GDPR. Another aspect to consider is that intention of providing service or product which complies with the data protection law is presumed to be reasonably expected from the service provider. Therefore, the author argues that content requirements of DPA are proportionate and parties entering into a DPA are in possession of the vital elements defined in the Principles of European Contract Law.

3.2. Purpose of the Data Processing Agreement

It is quite common for the commercial contract to include terms that already are governed by applicable law, e.g. force majeure, hardship and "good faith". They have little practical meaning besides being a source of information, evidencing party's awareness of the terms, serving to reference upon their invocation and, sometimes, permitted alterations. The logical question is why the written DPA is required between controller and processor, since legislators could have simply transformed the processor's obligations under a DPA into the direct statutory

[33] The Principles of European Contract Law. Available: https://www.trans-lex.org/400200/_/pecl/#head_4.
[34] Section 1, Article 2:101 (1) (a) – Conditions for the Conclusion of a Contract, The Principles of European Contract Law 2002.
[35] Ibid, (1) (b).
[36] Article 28 (9) of the GDPR.
[37] Jenna Lindqvist, *PERSONAL DATA PROTECTION ON THE INTERNET OF THINGS AN EU PERSPECTIVE, 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?,* Doctoral dissertation to be presented for public examination, by due permission of the Faculty of Law at the University of Helsinki, December 15, 2018. P. 66.
[38] Article 5 of the GDPR.

requirements applicable to processor? For instance, Article 32 (1) of the GDPR, unlike the Article 17 (1) of the Directive 95/46/EC governing the security of processing are now directly applicable to processors.

The DPA is designed to establish rules for processing of the personal data by a processor. The author asserts that, whereas GDPR contains the direct statutory requirements for processors, requirement for having a DPA is not rudimentary element that would be deemed redundant should the GDPR contain the direct responsibilities of processor in all aspects of processing. Instead, DPA aims to fulfil the important functions, as follows:

a) **Legal Certainty and Awareness**: to ensure that parties participating in processing are aware of their role and their respective rights and obligations;

b) **Enforcement, Individualization:** to provide instruments for enforcing a contract and negotiate more specific (individualized) technical, organizational and legal measures appropriate for the respective processing.

c) **Strengthening of Data Subject's Rights:** to ensure that processors and their sub-processors (if applicable), undertaking the DPA obligations**,** are continuously applying the appropriate organizational and security measures while maintaining the processes for timely response to data subject's requests. By doing so, data subjects remain confident that their data remains secured in all stages of processing.

3.2.1. Legal certainty and awareness

The principle of legal certainty is one of the fundamental principles of the EU legal system. The concept is broadly used by CJEU in various cases in order to evaluate the legality of the legislation and actions of the public administration.[39] This principle, in its nature requires all laws to be clear, stabile, intelligible and predictable, in order to ensure ability of the addressees of the law to foresee all legal consequences and to base their conduct on that notion.[40] The principle of legal certainty is also called upon to clarify obligations between the subjects of private law.

Lack of the legal certainty can cause market instability. For example, the report of the Stockholm School of Economics in 2015 explains that unpredictability of the legal regulation and lack of clarity in the legislative framework has a negative impact on business activity in Latvia.[41] Thus, clear and stable legal regulation is a prerequisite for stable commercial environment and economic growth. This is why Article 28 (3) of the GDPR is important from the perspective of the legal certainty – it is not only stating that relations between the processor and the controller must be regulated, but also implying that those relations must be governed by a private contract.

While it is beyond any doubts that any conduct must go in line with applicable law, not all companies have the sufficient capacity and expertise to determine what laws and regulations are

[39] Von Dawitz Thomas. Europäisches Verwaltungsrecht. Berlin: Springer, 2008, S. 575.
[40] Paunio E. Legal Certainty in Multilingual EU Law : Language, Discourse and Reasoning at the European Court of Justice. Surrey: Ashgate Publishing Limited, 2013, p. 51.
[41] Sauka A. The investment Climate in Latvia: the Viewpoint of Foregoing Investors. FICIL Sentiment Index 2015. Available on: https://www.ficil.lv/wp-content/uploads/2017/04/FICIL-Sentiment-Index-Report-2015.pdf. Accessed May 15, 2019.P.14.

applicable to their operations. The DPA renders another mechanism which offers an alternative source of information regarding the rights and responsibilities pertaining to the processing of personal data. Further, DPA seeks to prevent misunderstanding by clearly stipulating the processing details. Thereby, by having a correct[42] DPA in place, parties are minimizing the risk of disputes arising from misinterpretation of processing components. Furthermore, should the opinion be requested from the Data Protection Authorities, DPA services as detailed source of controller's intentions for governing the specific type of processing.

Another aspect is that DPA is a personified document that includes the name of contracting parties and therefore assigns specific rights and obligations. By doing so, parties are becoming bound by the clear set of commitments, that can be invoked by the party exercising its rights under a DPA. However, the naming of the roles must correspond with the nature of processing. According to the Article 28 (10) of the GDPR, if a processor exceeds the instructions of controller by assigning the purpose and means on its own, processor would become a controller for that particular processing, and therefore be subject to accountability in accordance with the Article 5 (2) of the GDPR.

Moreover, the process of fulfilling the formal requirements for entering into DPA require companies to be aware of the details of their processing. In order to do that, parties must agree on "*subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller*"[43]. The clarity in identification of the aforesaid categories is important for demonstrating the controller's intention to select the processor which provides "*sufficient guarantees"* [44] in terms of the Article 28 (1) of the GDPR.

In other words, the risk-based assessment of "*technical and organizational measures*" [45] would be impossible without determining the processing details (including the type of data processed and for what purposes).

In any event, imperative wording of the Article 28 (3) of the GDPR leads to much stable and legal relations. Legal certainty is not exclusively public law principle, it is correlates with the private law. Thus, all private relations also should have a high degree of legal certainty. By setting the very strict and widely regulated rules on contractual obligation between the processor and the controllers, EU legislators guaranteed legal certainty both un public and private law field: on the one hand subject of the private law can emphasize necessary provisions of the contract in the wording of the Article 28 (3) of the GDPR, on the other hand, the processor and the controller are aware of their legal relations have an interpretation means, which GDPR itself and all related acts and documents, including case-law.

Therefore, author concludes, that Article 28 (3) of the GDPR guarantees legal certainty in application of the legal norm and clarifying the nature of the legal relations.

---

[42] By using the term "correct" author means the DPA that is precisely outlining processing details along with being compliant with formal requirements of the Article 28 (3) of the GDPR.
[43] Article 28 (3) of the GDPR.
[44] Article 28 (1) of the GDPR.
[45] Ibid.

3.2.2. Enforcement and individualization

Article 28 (1) of the GDPR requires controllers to use processors that are applying the appropriate measures to guarantee that processing complies with the GDPR. Accordingly, controllers are apt to select the processors that have adopted the IS compliance strategy that include, but are not limited to the following measures:

a) Lawfulness, Fairness, Transparency

a) Obtaining and keeping appropriate legal basis;[46]

b) Informing individuals about the details of processing prior to commencement of processing;[47]

c) Keeping Records of personal data;[48]

d) Contributing in fulfilment of data subject's requests;[49]

e) Identifying role in processing and entering into DPA, if appropriate.[50]

b) Security, Purpose and Storage Limitation

a) Understanding the nature and details of processing;

b) Keeping information accurate and up to date;[51]

c) Introducing data minimization routines;[52]

d) Implementing security awareness routines;

e) Securing data confidentiality;[53]

f) Implementing the processes for data breach notification;[54]

g) Carrying out Privacy Impact Assessments;[55]

h) Applying appropriate information security controls.[56]

DPA itself represents a commitment for parties to ensure that processing is based on the compliance with applicable laws, including GDPR. Therefore, the author believes that, should the processor comply with directly applicable provisions of the GDPR (other than those set forth in the Article 28 (3) of the GDPR), such processor should, by default, be capable to conform to most of the obligations imposed on the processor pursuant to the Article 28 (3) of the GDPR.

Essentially, the obligations undertaken by one contracting party entitle other party to claim the respective performance. DPA may include both, mandatory and non-mandatory rights

[46] Article 6 of the GDPR.
[47] Article 12, 13, of the GPDR.
[48] Article 30 of the GDPR.
[49] Chapter III of the GDPR.
[50] Article 28 (3) of the GDPR.
[51] Article 5 (1) (d) of the GPDR.
[52] Article 5(1) (c) of the GDPR.
[53] Article 5 (1) (f).
[54] Article 33, 34, of the GPDR.
[55] Article 35 of the GDPR.
[56] Article 32 of the GDPR.

of controller. Controller will benefit from having a legal instrument which represents the source of controller's rights and corresponding commitments from processor. As a result, clear commitment from the processor expressed in the enforceable legal instrument will enable controller to exercise its rights more effectively.

Since controller is ultimately accountable for demonstrating compliance with the GDPR[57], another purpose of DPA is to envisage controller with more control over the processing by enabling controller to negotiate additional and perhaps more specific legal terms. As a result, contracting parties might individualize their DPA to reflect the terms most relevant to the agreed processing.

For example, controller requires processor to process special categories of personal data on its behalf. In this case, controllers should be interested in requiring processor to apply highest IS controls associated with the data at hand. It is likely that controllers will attempt to govern what access management and operations security controls must be applied, as minimum, given the sensitivity of the personal data. In addition, controller may require processor to obtain certificates issued by certification bodies referred to in the Article 43 of the GDPR or other certificates warranting the processor's compliance with information security standards, such as ISO 27001, or ISO 27017. Another option is to oblige processor to obtain cyber insurance coverage to hedge against cyber risks.

Controller may also consider including the liability section that outlines the concrete liability of processor for breaching DPA terms. Since the damages incurred by unauthorized access, disclosure or loss of data may be hard to prove, let alone estimate, controllers might be keen in including fixed penalties for each event of breach. Finally, it is quite common that a DPA is incorporated in a main agreement as an annex. Consequently, controller may stipulate that any breach of DPA (e.g. failure to apply certain security measures or contribute to security audit) would constitute a material breach of the main agreement and allow controller to terminate an agreement unilaterally (sometimes - effective immediately). That remedy may be especially useful in the recurring annual contracts with no advance payments made. Therefore, besides the obligations directly applicable to processor under the GDPR, processors are now held contractually liable for breach of variety of obligations undertaken under a DPA. In such a way, compliance is ensured at all levels of processing.

However, controllers are often in a position in which they do not have enough bargaining power to impose their own terms.[58] Especially in SaaS, in which SaaS providers not typically accepting customer's version of DPA, unless a controller is an enterprise customer or public entity awarding a public contract. This approach stems from the nature of SaaS delivery model as based to *one-to-many* principle. SaaS requires standardization of its delivery infrastructure with only few permitted customizations, such as security settings selected by controller via software interface. Therefore, only on very rare occasions SaaS providers are applying additional security controls and measures exceeding their standard controls generally applicable to all customers. As

[57] Article 5 (2) of the GDPR.

[58] Jenna Lindqvist, *PERSONAL DATA PROTECTION ON THE INTERNET OF THINGS AN EU PERSPECTIVE, 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?,* Doctoral dissertation to be presented for public examination, by due permission of the Faculty of Law at the University of Helsinki, December 15, 2018. P. 66.

a result, SaaS providers are relying on their standard agreement templates with little or no derogations acceptable.

There can be argued that controller is the one that must define the purpose and nature of processing and have the control over adapting a DPA accordingly to the selected purpose. However virtually any SaaS business implies that customers are merely accepting the nature and purpose of processing already defined by a SaaS provider. That does not diminish the authority of controller pursuant to the GDPR, since controller is ultimately authorized to select the processor that is offering the processing conditions and corresponding contractual terms matching that of the controller. Given that SaaS market is becoming more and more competitive, the choice of the most suitable processor should not be a difficult task.

Another reason for standardization of DPA's by SaaS providers is related to the fact that customer often lacks proper expertise to recognize the intricate structure of the SaaS delivery model and therefore, potential security threats. Having a limited knowledge about the processing environment would create significant obstacles in creating an effective DPA. In fact, knowledge of the technical environment and SaaS delivery framework allows SaaS provider to map the flow of data and therefore be proactive in identifying and applying the appropriate measures. Therefore, in most of the SaaS contracts, controller would be simply verifying whether the DPA provided by SaaS provider meets the GDPR requirements.[59]

Despite the impracticalities in forcing the controller's version of DPA to a SaaS provider, by the virtue of Article 5(2) of the GDPR controller remains accountable for demonstrating compliance with the principles of GDPR[60], and hence, the responsibility to oversee the compliance with Article 28 (3) is in line with the Article 5(2) of the GDPR – accountability principle. The ICO guidance on "Contracts and liabilities between controllers and processors" confirm the controller's responsibility for initiating DPA signing process towards its processors by emphasizing the consequences of non-compliance with this requirement, which are now extended to processors as well.[61]

Unlike the Directive 95/46/EC, GDPR provides that processors are now having a direct responsibilities and obligations under the GDPR, outside the terms of DPA. Processors can be held directly responsible for non-compliance with these obligations and may be subject to administrative fines. That is why, prior to GDPR entering into force on 25th of May 2018, virtually any multinational SaaS vendor has been launching their GDPR-ready programmes which included "*re-papering*" their existing contracts.

In addition, the processor's refusal to enter into a DPA would constitute a breach of applicable laws and thereby breach of a main contract. Some contract provides that incompliance with applicable law is deemed as "*material breach of a contract*". Failure to cure the breach within the certain time would allow controller to terminate an agreement. Having an "opt out"

---

[59] Mariusz Krzysztofek, *GDPR: General Data Protection Regulation (EU) 2016/679 Post-Reform Personal Data Protection in the European Union*, 2016, Available on: Wolters Kluwer Digital Book Platform. Accessed April 12, 2019. P. 187.

[60] Article 5 (2) of the GDPR

[61] Information Commissioner's Office GDPR guidance: Contracts and liabilities between controllers and processors, available on: https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf. Accessed May 19, 2019. P. 6.

option may bring some leverage to controller in setting out DPA and perhaps customizing some of its terms.

Finally, as being a source of information on processing details DPA will facilitate any dispute by providing the court and/or Data Protection Authority with information of what parties agreed in terms of processing. That will relieve claimant from the need to collect evidence to prove the agreed details of processing, let alone the fact of processing.

3.2.3. Strengthening of Data Subjects Rights

Without any doubt, protection of the right to privacy is a cornerstone of GDPR and is being its primary objective. That is why, when examining the provisions aiming to protect data subjects are easily spotted throughout the DPA content requirements laid down in the Article 28 (3) of the GDPR.

Recital 81 of the GDPR emphasizes that in agreeing the DPA, "*the risk to the rights and freedoms of the data subjects must be taken into account*". One way to interpret this is that selection of processor requires controller to carry out prior privacy risk analysis.

In doing so, even prior to entering into a DPA, controller needs to verify if it has sufficient legal ground to outsource the processing to a third-party processor. Next, is to identify the processing details, including determining the purpose, nature of processing and types of personal data[62] and to confirm the nature of processing is justifying the purpose of processing. Matching the processing details with the purpose is particularly important in applying purpose limitation principle, according to which, controller is required to assess if the personal data is processed only to the extent required for fulfilling the purpose of processing[63]. Lastly, the controller mandates processor to guarantee implementation of technical and organizational measures[64] appropriate to the processing. In some cases, controller may require processor to carry out PIA.[65] An obligation to apply "appropriate" measures means that processor must always keep such measures in line with changes in processing and then-current IS risks.

Finally, according to the Article 28 (3) (e) processor will need to assist controller in fulfilling data subject's rights. Thus, a contractual commitment will force processors to align their processes and systems to enable effective and timely response to data subject's requests. By doing so, the DPA serves the function of ensuring the protection of data subject's rights at all levels of processing.

3.3. Form of a DPA

According to the Article 28 (9) of the GDPR, the legally binding "*contract or the other legal act*" must be in writing, including in electronic form. That means that oral agreements or agreements that cannot be evidenced in writing cannot be compliant with formal requirements of

[62] Article 28 (3) of the GDPR.
[63] Article 5 (1) (b) of the GDPR.
[64] Article 28 (1) of the GDPR.
[65] Article 35 (3) of the GDPR.

the Article 28. Whereas that is limiting the company's contractual autonomy, it is a proportional and reasonable requirement given that controller's obligations to demonstrate compliance would involve collecting evidence about controller's informative choice in selecting the trustworthy processor. To substantiate that claim, there must be a proper arrangement for processing of personal data with processor. A document expressed in writing is the only reliable tool controller can use in order to prove conformity with the Article 28 (3) of the GDPR.

Unlike the Article 17 (4) of the Directive 95/46/EC that required a DPA to be in "writing or in another equivalent form" the Article 28 (9) brought more clarity by stating that a "*contract or the other legal act*" can be concluded in "*electronic form*". Ability to enter into a DPA electronically is vital for SaaS businesses, since scalability and growth of their products is dependent of a complete automation of the contract lifecycle management and swift signing process. Thus, in most cases, given that no installation or integration of SaaS product is required, most SaaS companies are having a "*sign up*" functions on their websites.

Upon "*signing up*" customers are automatically agreeing to the standard T&C of a SaaS provider along with its DPA. The use of SaaS product is conditioned upon assent of such standard T&C, since no registration process is completed prior to accepting such T&C. If a purchase order is used, a standard DPA is usually included by reference in that purchase order. Hence, by signing a purchase order, customer automatically adheres to the standard DPA. It is crucial for SaaS provider to allow modifications of its standard T&C, including DPA, from time to time, to reflect changes in the system which may lead to changes in its processing environment.

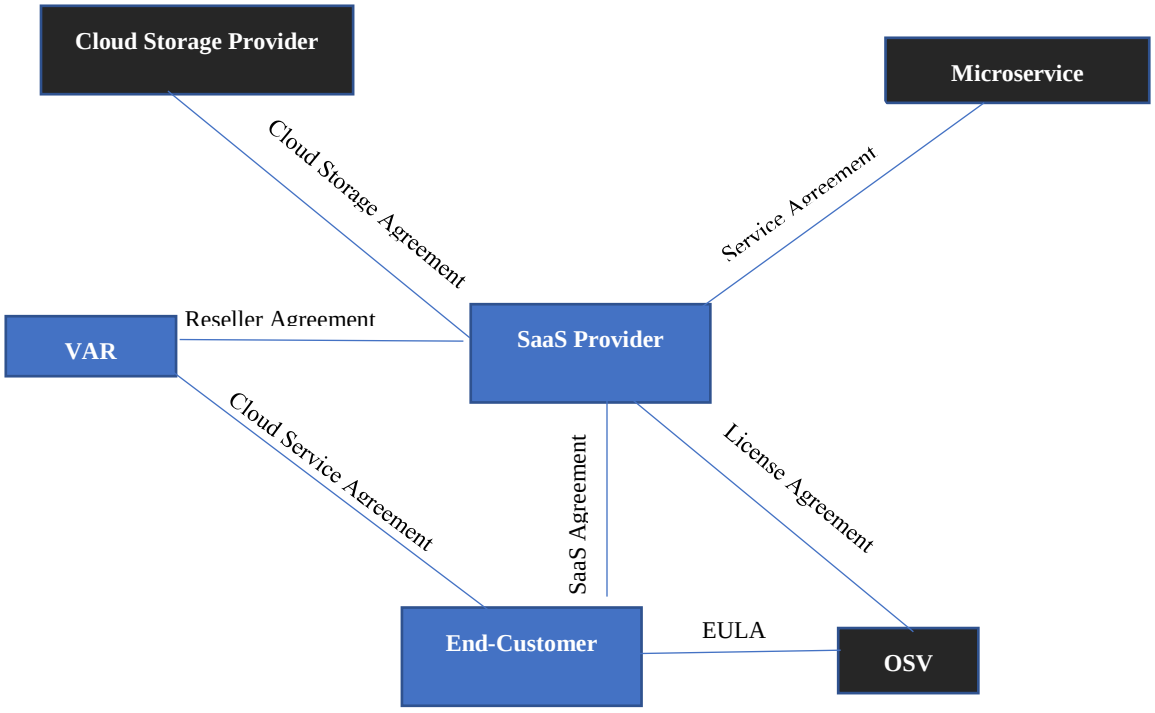
Another SaaS providers are allowing controllers to fill in the processing details before accepting DPA, such as "*types of personal data and categories of data subjects*"[66] whereas other terms remain standard. That is usually done when SaaS product embodies data management function and thereby does not confine its product to specific personal data foreseen by SaaS provider. Allowing controller to modify a DPA is an indication of "*good faith"* and "*good industry practice*". In so doing, SaaS provider is entitled to claim that controller had the ability to alter the terms according to its desire. However, both parties must be aware that if controller fails to fill in the appropriate processing details, or if processing exceeds the scope defined in the DPA, processing of such data will not be governed by that DPA. In turn, processing of that data is rendered non-compliant with the GDPR. Therefore, whereas the standard DPA might be permitted to be amended from time to time unilaterally by a SaaS provider the processing details needs to be constantly monitored by controller.

[66] Article 28 (3) of the GDPR.

4. DETERMINING YOUR ROLE IN SAAS CONTRACTS

The further chapters will illustrate various interaction models commonly adopted among SaaS providers and provide guidance for structuring DPA's in accordance with the roles assigned to each party within the SaaS contractual framework. SaaS product delivery model typically involves multiple parties simultaneously processing personal data on behalf of controller for different purpose. However, it is crucial to determine the applicable roles for the correct assignment of roles and responsibilities of the parties.[67] That is why, the thesis will provide guidance for determining the processing roles of the contractual parties participating in SaaS delivery model by interpreting the terms: controller, processor, other processor ("sub-processor") pursuant to the Article 4 and Article 28 of the GDPR, examining the Opinion 1/2010 of the Art.29.WP and analysis of functions undertaken by different parties within SaaS delivery model.

The possible interaction between parties of SaaS contract is represented in the chart below.[68] Please note that the list is not complete, however author sought to outline the parties that are normally appearing in SaaS contracts. Entities such as Internet and network providers, as well as actors that themselves become controllers or joint controllers (and are therefore not contracting parties to a DPA), are intentionally excluded. The DPA impact on data subjects is discussed in the sub-sections 3.2.3 and 6.9. sections of the thesis.



[67] Vidovic, Marina Skrinjar, *EU Data Protection Reform: Challenges for Cloud Computing*, Croatian Yearbook of European Law and Policy 12, No. 12 (2016). Doi:10.3935/cyelp.12.2016.252, P.176.

[68] Natālija Lazukina, *Programmatūras kā pakalpojuma nodrošināšanas līguma normatīvais regulējums un problēmas*, Latvijas Universitāte Juridiskā Fakultāte Civiltiesisko Zinātņu Katedra, 2010. Section 2.1. SaaS pakalpojuma juridiska shema. Para. 23.

4.1. Personal Data Controller

The role of personal data controller is defined in the Article 4 (7) of the GDPR and characterized as a person, regardless of the legal form, that "*alone or jointly with others*", determines the "*purposes and means of the processing*" of personal data.[69]

Art.29.WP in its opinion suggested that the key element of distinguishing controller from other actors is to determine if that entity exercises control over personal data by determining "*the purpose and the means of processing of personal data*".[70] Therefore, controller is not regarded as person that actually processes the personal data, but rather a decision maker that assigns the "*purpose and means*" of processing.

Assigning a purpose of processing can be construed as controller's decision whether to process personal data for achieving the specific objectives. To ensure that processing conforms with the purpose limitation principle and lawfulness of processing, the purpose must match the legal basis under which the personal data has been collected in a first place.

For example, bank is processing data its customer's data and uses data storage provider. In this setup, bank, as a personal data controller, is relying on its contracts with customers[71] (data subjects) as well as has some direct legal obligations[72] to process personal data, including using third-party processors to store such data on its behalf. However, if bank wishes to diversify its earning strategy by adding another product, and therefore engages in direct marketing, bank must find another legal ground for processing, e.g. legitimate interest[73]. Thereafter, only after carrying out "*legitimate interest balancing test*" confirming that interests of the bank override the rights and freedoms of data subject[74] and subject to fulfilment of transparency obligations, bank can engage in direct marketing based on the newly acquired legal basis. The use of processors for the purposes of providing, for instance, digital marketing tools and services, must be considered within the "*legitimate interest balancing test*"[75].

Assigning the means of processing relates to deciding the manner of processing, including technical and organizational means[76]. In other words, deciding on how the data is to be processed to reach the purpose of processing. In the aforesaid example, the storage of personal data constitutes one of the means of processing on behalf of controller. Moreover, bank may be interested in confining storage of personal data to specific territory (e.g. within European Union) and subjecting such data to selected IS controls. By requiring processor to apply such measures, controller is deciding the means of processing of personal data.

---

[69] Article 4 (7) of the GDPR.
[70] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010, page 1.
[71] Article 6 (1) (b) of the GDPR.
[72] Article 6 (1) (c) of the GDPR.
[73] Article 6 (1) (f) of the GDPR.
[74] Ibid.
[75] Ibid.
[76] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010, P. 14.

However, the Art.29.WP acknowledges that, in some circumstances it is permissible for processor to determine the technical and organizational measures without being qualified as controller.[77] As mentioned before, scalability of SaaS model requires standardization of purpose and means of processing, whereby controllers are exercising its control by selecting the processor that offers the purpose and means of processing matching the intentions of controller. Processor's authorization to decide on the means of processing must be, nonetheless, accompanied by controller's ability to oversee, in some cases, interfere with selected means[78] via controller's instructions.

In the contractual framework presented above, Customer will be regarded as "Controller".

4.1.1. Customer

For the purposes of this thesis, customer is referred to as an entity that is using SaaS products, such as cloud-based ERP, to outsource its processing to SaaS provider. Even though, greater leverage of SaaS companies allows them to use "*take it or leave it*" agreements, customer remains responsible for acquiring and maintaining the legal basis for processing and are responsible for deciding whether to use a SaaS company or not. In other words, even if SaaS company is making their product to fit for specific purpose, (e.g. customer data management), and employing the means of processing by selecting the technical and organization measures[79] that does not constitute controlling personal data. SaaS company would be acing within the scope of agreement with Customer that must thereafter assess whether the purpose and means offered by a SaaS company comply with theirs. If not, SaaS company may withdraw from using SaaS entity.

Defining purpose and means of processing is often manifested as giving instructions to a processor. As a result, in determining with whom there must be a DPA in place, customers are required to identify its processor by determining which entity is responsible for directly responding to the instructions from controller.

4.2. Personal Data Processor

GDPR defines processor as person, that regardless of its legal form, processes personal data on behalf of controller[80], according to its documented instructions.[81] Whereas controller is responsible for determining the "*purpose and means*" of processing, the actual processing of personal data is not a prerequisite for being a controller. Controller is entitled to use processors to process data on their behalf, however, if the processing carried out by processor exceeds the controller's instruction, the processing is unlawful unless processor has a legal basis for the

[77] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010, P. 14.
[78] Handbook on European data protection law. Luxembourg: Publication Office of the European Union, 2018, p. 108.
[79] Mariusz Krzysztofek, *GDPR: General Data Protection Regulation (EU) 2016/679 Post-Reform Personal Data Protection in the European Union*, 2016, Available on: Wolters Kluwer Digital Book Platform. Accessed April 12, 2019. p. 181.
[80] Article 4(8) of the GDPR.
[81] Article 28(3) (a) of the GDPR.

processing and is therefore empowered to assign a purpose. In such as case, processor becomes joint controller or data controller itself pursuant to the Article 28 (10) of the GDPR.

In SaaS contractual framework provided in the section 4 of this thesis, Value Added Reseller (and optionally - SaaS provider)[82] is regarded as personal data processor.

4.2.1. Value Added Reseller

The term VAR is hereby used to refer to an entity that is acting as reseller of SaaS product, usually under a reseller agreement with SaaS Provider. Reseller agreement is granting VAR a right to sell SaaS product either as an independent solution or in conjunction with VAR's or its suppliers own services. The value-added services provided by VAR may are aimed to enhance the value of a SaaS product and may include support services, integration, consultation and bundling the SaaS product together with other products and services. Reseller agreement also allows VAR to govern the business terms between VAR and customer, including, prices, payment terms, liability, etc. Subsequently, VAR is entering into a "SaaS purchase agreement" and/or service agreement with Customers.

A lot of IT giants are operating through the distribution channels that involve VAR's that abide to specific partner programmes. Such programmes typically require VAR's to act as customer facing party and maintain the qualified marketing, sales and support personnel. For instance, according to the Microsoft Cloud Reseller Agreement[83], VAR undertakes to provide continuous customer support. In exchange, vendors are providing discounts and are working closely with VAR's to improve their expertise by providing sales/marketing materials and training. By doing so, vendors are enhancing the sales capacity of VAR.

4.2.2. SaaS Provider

SaaS provider is used to describe the provider of a Software as a Service to customer. The important distinction must be made between a SaaS contract and a software license agreement. The essence of the software license agreement is transfer of rights to use the software for the specific period of time. Consequently, software is installed on a controller's hardware and is usually accessible in an offline mode. However, SaaS contract is essentially the service agreement, where SaaS provider is providing an access to the cloud-based infrastructure together with the software.

That requires closer cooperation between SaaS provider and customer, since any changes in the cloud computing environment or software must be communicated to customer. By providing a cloud computing environment and enabling continuous software management and updates SaaS provider can operate either through a model in which it acts as sub-contractor for VAR or to have a direct agreement with a customer. It is true to say that many SaaS vendors, while using VAR as a distribution channel, are entering into direct agreements with its customer.

---

[82] See. Model No.2. page 29 of this thesis.

[83] Microsoft Cloud Reseller Agreement, available on: https://docs.microsoft.com/en-us/partner-center/csp-documents-and-learning-resources#cloud-solution-provider-program-guide , Art. 6. (a). Accessed May 9, 2019.

As a result, even though the SaaS product is purchased from VAR, and perhaps is part of a services bundle, customer is to be bound by both (i) agreement with VAR governing the business terms and value-added services provided by VAR, and direct agreement with one or more SaaS providers governing the delivery of the respective SaaS products.

4.3. Personal Data Sub-Processor

Upon receipt of an authorization from controller, processor may use another processor to process personal data on its behalf[84]. The term "*other processor*" may be interpreted as a person, regardless of its legal form, that, upon authorization from controller, process personal data on behalf of processor.

In its opinion on cloud computing services Art.29.WP used the term "sub-processor" when stating that "Cloud computing services may entail the involvement of a number of contracted parties who act as processors. It is also common for processors to subcontract additional sub-processors which then gain access to personal data."[85] In other opinion Working party agreed, that – "Nothing in the Directive prevents that on account of organizational requirements, several entities may be designated as data processors or (sub-)processors also by subdividing the relevant tasks."[86]

There is no limitation to the number of sub-processors, although appointment of sub-processors is subject to controller's authorization. However, Art.29.WP. emphasized that "*one should avoid a chain of (sub-)processors that would dilute or even prevent effective control and clear responsibility for processing activities, unless the responsibilities of the various parties in the chain are clearly established*."[87]

The essential element of SaaS products is the continuous provision of a set of services to customer under a unified SaaS framework. SaaS offering may also include multiple types of microservices and professional services. It would be quite rare that SaaS company possessed the sufficient resources to develop all the SaaS components themselves. That requires substantial amount of time and resources to build their own data centre, employ a support personnel while saving time for research and development, which would mean a long-term investment. Instead software companies are often utilizing ancillary products, such as cloud commerce platforms, data hosting companies and different microservices that are taking care of the individual features and are integrated in the main SaaS product. That relieves SaaS companies from spending time on resolving matters other than improving and development of their core product. Such supplementary products are provided on "*as a service*" basis to SaaS companies, and if they are used to process personal data on behalf of SaaS provider, companies supplying such products are becoming personal data sub-processors.

In SaaS contractual framework provided above, Microservices Provider and Data Storage Provider are regarded as personal data sub-processors.

---

[84] Article 28 (2) of the GDPR.
[85] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing (01037/12/EN WP 196), p. 9.
[86] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (00264/10/EN WP 169), p. 27.
[87] Ibid.

4.3.1. Microservices Provider

Originally, the term "*Microservices*" is used to refer to the method of architecting software applications in cloud. By using the "*microservices approach*" software is built from the multiple independent components.[88] For the purposes of this thesis, microservices are SaaS product components that are provided by microservices providers and are involved in the processing of customer's personal data on behalf of SaaS provider. The use of microservices can vary from seemingly simple functions, such as log-in, to analytics or set of more complex functions provided by the cloud commerce platforms.

Microservices are aimed to increase value proposition of the SaaS product and allows SaaS provider to focus on its core product rather than developing a software component which can be provided by microservices provider at relatively cheaper cost and better quality.

Microservices can be provided as a white labelled solution, in which certain functions are integrated in SaaS product but, in fact, are provided by microservices provider themselves. It is important to emphasize that, unlike the sale of tangible goods, that may be assembled from third-party materials, microservices used in SaaS products are usually provided on a continuous basis. Therefore, the contract between microservices provider and SaaS provider is usually not a purchase agreement, but (i) "*Service Agreement*" by which SaaS provider outsources part of its technical or business processes to microservices provider; or (ii) "*Reseller Agreement*" by which SaaS provider gains a license to sell a microservice as an add-on to its SaaS product. Both of these models require microservices provider to be continuously involved in the processing of customer's personal data, should the nature of microservice require to do so. Therefore, microservices provider becomes personal data sub-processor or, in some cases, processor.

In addition, both VAR and SaaS provider can resort to outsourcing of their processes, including, but not limited to support, research & development, managed services, shared services, invoicing, dunning, quality assurance, to third parties.

Sometimes, the companies within the same company group can be used for that purpose. However, it must be kept in mind that, even if companies are belonging to the same group, they are regarded as separate entities, and thereby separate actors within the processing.

In terms of processing, it is crucial to determine whether the such third-party qualifies as processor for the customer, for SaaS provider (or VAR) or becomes controller itself. For example, SaaS company is using third party performing development function. Development features may require third party to have access to the database of SaaS provider. And unless the database is encrypted or pseudonymized, or otherwise does not contain personal data, the access to that database constitutes data processing according to the Article 4 (2) of the GDPR. It can be argued that development carried out with intention to improve SaaS product is consistent with the purpose assigned by controller. However, in this case, SaaS company is determining the purpose

[88] Microservices definition, available on: https://www.ibm.com/blogs/cloud-computing/2016/05/04/what-are-microserverices/ Accessed 13 May, 2019.

and selects the means of processing. Therefore, SaaS company becomes controller[89] and is accountable for demonstrating compliance with principles relating to personal data,[90] whilst third-party provider becomes processor.

4.3.2. Cloud Storage Provider

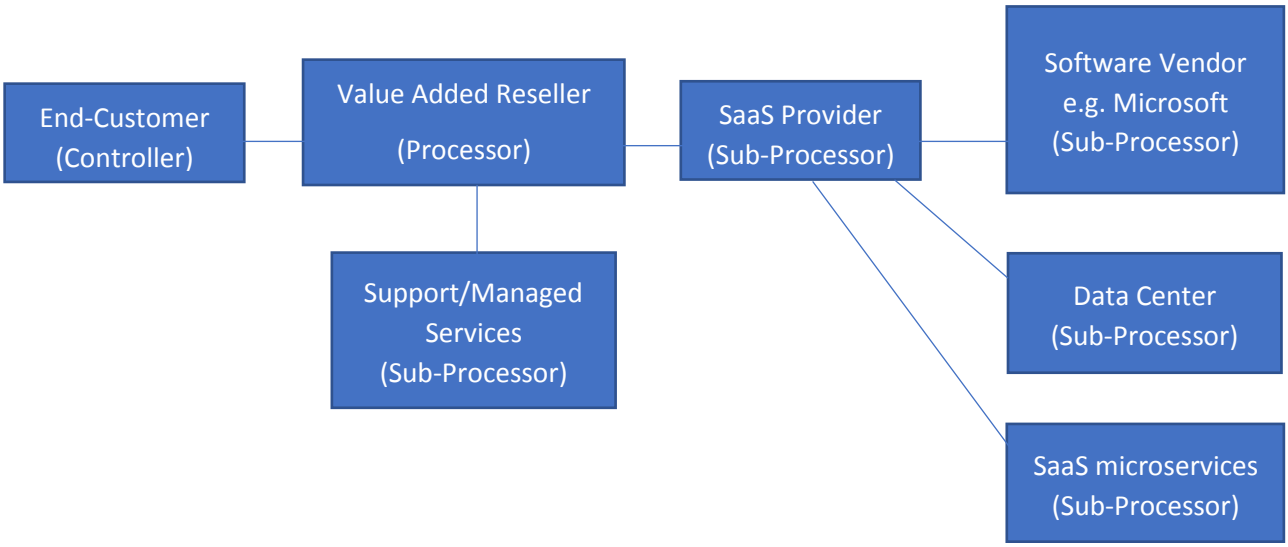
Cloud storage is an essential part of the SaaS outsourcing strategy in which the data is hosted by a third-party. Third party cloud storage provider becomes responsible for the physical environment, including hardware to render the data available to SaaS provider and its customers according to the specific SLA. Using cloud storage has many benefits, such as avoidance of purchasing and maintaining physical data centres while paying only for the limited storage capacity. In terms of data security, cloud storage provider is responsible for ensuring IS security of its data centres, including physical security.

Usually, the cloud storage is rendered to the SaaS provider under a "*cloud storage agreement*". The storage of personal data constitutes the "*processing*" pursuant to the Article 4 (2) of the GDPR. Provided that cloud storage is used to store customer's data, cloud storage provider becomes qualified sub-processors of the SaaS provider.

[89] Mariusz Krzysztofek, *GDPR: General Data Protection Regulation (EU) 2016/679 Post-Reform Personal Data Protection in the European Union*, 2016, Available on: Wolters Kluwer Digital Book Platform. Accessed April 12, 2019. p. 183.
[90] Article 5(2) of the GDPR

5. SAAS DPA SCENARIOS

5.1. Model No.1



The Model No.1 represents the contractual framework in which provision of software is governed by the direct agreement between customer and VAR. In this case, VAR is owning customer relationship and act as customer facing party in all aspects of SaaS delivery. In this way, VAR would commit to delivery of SaaS product to customer, while outsourcing that function to SaaS provider. In this regard, most of the contracts between VAR and SaaS provider would state that SaaS provider fully indemnifies the reseller if SaaS product is not compliant with the technical documentation.

Adding an extra contractual layer does not relieve from liability to conclude a DPA between processor and controller. The solution commonly used by VAR is to sign a DPA with customer, in which VAR is formally qualified as processor, while its suppliers are recognized as sub-processors. From a DPA perspective, the lack of participation of VAR in SaaS delivery means that fulfilment of DPA is ensured by VAR redirecting the customer's processing instructions reflected in the DPA among its providers.

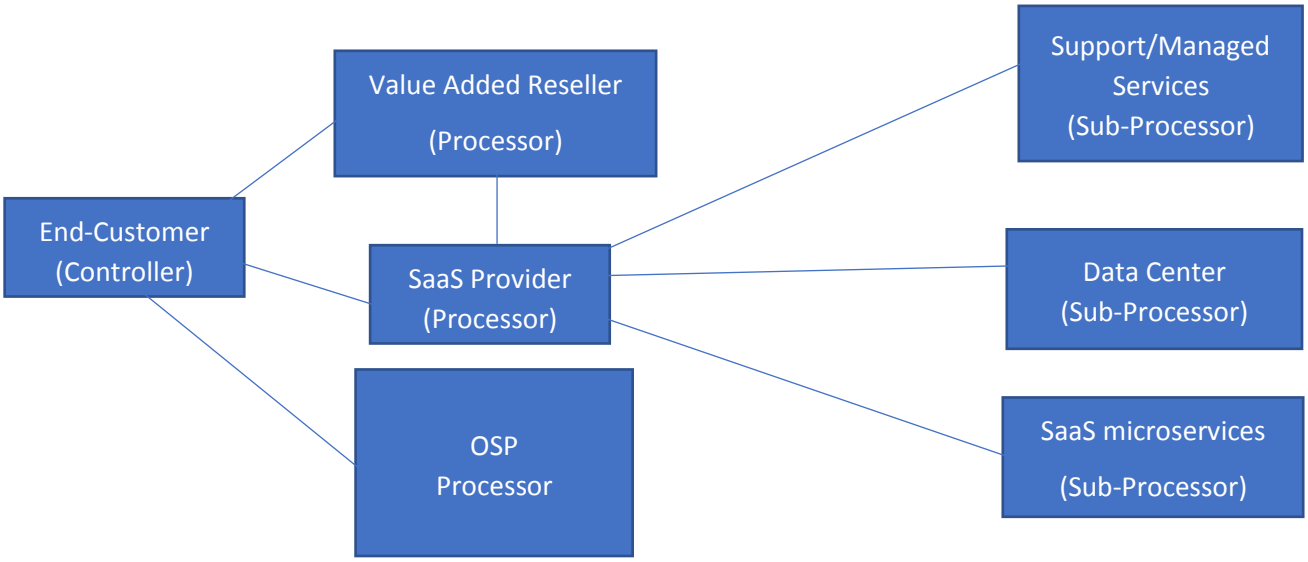
Even if there is no direct conflict in GDPR that would restrict the use of this model, it is not entirely free of flaws. The essential characteristic of controller is the ability to give processing instructions to processor. The instructions are the means of communicating the changes in processing details to processor. However, SaaS delivery typically entails closer cooperation between SaaS provider and customer, thereby SaaS product functionality allows customer to carry out changes to its personal data via SaaS interface. Such actions would imply circumvention of the DPA with VAR and issuing direct instructions to the sub-processor.

It may be claimed thought, that fulfilment of customer's instructions is carried out by SaaS provider under the general instruction of VAR. However, the author believes that the absence of processing function would conflict with the definition of "processor" as a person that processes the personal data upon instructions from controller. This is the case when VAR acts solely as "middleman", re-selling SaaS product, and does not process any customer's personal

data except for sales and marketing purposes or when engaging in provision of its value-added services.

Nevertheless, going forwards, VAR may consider including GDPR coordination function as a part of its value proposition e.g. automation of GDPR related processes for targeting start-up companies.

5.2. Model No.2



The Model No.2 provides that the use of SaaS product is conditioned upon execution of two or more agreements simultaneously. Each of these agreements only covers the scope of products or services provided by the respective party.

Firstly, customer enters into a service agreement with VAR that governs business terms and delivery of value-added services. Regardless of direct agreements between customer and SaaS provider, SaaS sales go through VAR sales channel, thus, VAR remains responsible for price management under its cloud reseller agreement with SaaS provider. That means that VAR determines the price of SaaS product and is responsible for bearing credit risk. VAR is typically bundling SaaS products with additional services and/or products to increase the value of its SaaS product offering. Provided that VAR is exercising direct control over these "value-adds", the direct contract between VAR and customer will reflect the terms of delivery of such additional services of products.

Secondly, customer is entering into a direct SaaS agreement with SaaS provider that governs the delivery of SaaS product. SaaS agreement is usually limited to the technical T&C pertaining to delivery of SaaS product e.g. scope of SaaS, technical specifications, SLA, update schedule and obligations related to security and return of data.

From the DPA perspective, this model seems very intuitive, since, both SaaS provider and VAR are qualified as separate processors. Essentially, this model goes in line with the nature of SaaS delivery model. The SaaS providers are not granting VAR a license to re-sell software

licenses, instead, VAR is selling the subscription right to a software which is continuously provided by a SaaS provider.[91] This distinction requires SaaS provider to be qualified as processor, since any changes to the processing details are taken care of by SaaS provider upon direct instructions from a customer.

Another scenario that is worth mentioning is when SaaS provider is not an OSP but is hosting its application on another cloud product. This option is supported by various vendors, such as Microsoft[92] and Cisco[93]. In this case, product of SaaS provider could be regarded as add-on or integrated solution with other vendor product and therefore, its delivery is conditioned upon customer obtaining a license from OSP. From the customer's perspective, this model is similar as that between VAR and SaaS, in which customer is bound by either (i) one agreement with SaaS provider (or VAR) which outlines the sale and delivery of OSP software together with SaaS product; or (ii) two agreements, one governing the delivery of SaaS product and another the delivery of product license from OSP. It may be the case, that customer is already using OSP product and purchases SaaS product as ancillary solution. In this case, parties typically resort to the latter second scenario.

The model No.2 is beneficial for VAR that becomes exempt from requirements to satisfy controller's processing instructions. This scenario is particularly important if VAR's strategy is confined to managing the sales channel by re-selling individual SaaS products or SaaS bundles containing multiple SaaS products. In such an event, VAR is not responsible for managing the SaaS providers as its sub-processors and requiring them to maintain the same security guarantees as those required by customer from VAR. That is arguably reasonable considering that VAR may have limited knowledge on actual functionality of individual SaaS products.

In addition, customer may benefit from being contractually entitled to claim damages from SaaS providers directly, in cases the SaaS product is not compliant with technical T&C or if SaaS provider commits data breach. The benefit is however very arbitrary and dependent on the financial standing of the SaaS provider and contractual provisions of SaaS contract. On this instance, customer should estimate its chances of claiming damages by examining the SaaS contract in terms of governing law and limitation of liability. Most of the SaaS providers, let alone OSP's are not so keen in balancing the terms of liability and require customer to accept the governing law and jurisdiction of their domicile. Therefore, customers may, on the contrary, benefit from commencing legal action against reseller that is usually located in the same region as customer (for better sales reach, language considerations, support). Thereafter, if damages are awarded, VAR may resort to the indemnity clauses stipulating that SaaS provider reimburses all damages incurred by VAR due to SaaS provider's breach of its technical commitment.

Nevertheless, having a separate contract with each processor require customers to be advanced in maintaining processes for exercising controller's rights with respect to each processor individually. For example, customer has purchases from VAR the CRM from SaaS

---

[91] David W.Tollen, *The Tech Contracts Handbook, Second Edition, Cloud Computing Agreements, Software Licenses, and Other IT Contracts for Lawyers and Businesspeople*. Part 1, Sec E (2) Cloud Resale. Amazon Kindle Version.

[92] Microsoft Partner Program, available at: https://azure.microsoft.com/en-us/. Accessed May 9, 2019.

[93] Cisco Partner Program, available at: https://www.cisco.com/c/en/us/partners/partner-with-cisco/solution-partner-program-spp.html. Accessed May 9, 2019.

provider X, cloud storage from SaaS provider Y. Data subject is using its "*right to be forgotten*"[94] for complete erasure of its data. Provided that customer is not having another legal basis for storing personal data, customer is required to locate where the data resides within its own systems and third-party processors. Thereafter, customers must rely on the DPA[95] with each processor separately i.e. X and Y, to ensure the erasure of data by either using the SaaS product functionality or directly requesting processor to erase the data in question. Another aspect is that, in this model, customer is owed to carry out IS due diligence with regards to each SaaS provider to determine if SaaS provider offers the sufficient guarantees of compliance with the GDPR,[96] which ultimately benefits the data subject with having a risk analysis carried out in all layers of processing, however leads to customer incurring costs.

The model No.2 has been widely applied by large vendors such as Microsoft, that are operating largely through reseller channels. According to the clause 4 (a) Cloud Reseller Agreement[97] Microsoft requires its resellers to procure that its customers accept the direct agreement between Microsoft and customer. Reseller is liable for any damages resulting from reseller's failure to establish a legally binding agreement between Microsoft and customer.

Therefore, any reseller that re-sells Microsoft could products, besides its own agreement is obliged to ensure customer's acceptance of Microsoft's customer agreement. Even prior to GDPR entry into force Microsoft worked closely with the Art.29.WP to have its cloud computing agreement compliant, including its DPA formally approved by the Art.29.WP[98]. The current Microsoft Customer Agreement[99], by reference includes Product Terms[100] containing DPA[101]. Since, DPA is an integral part of customer agreement, acceptance of customer agreement means acceptance of DPA as well. However, the acceptance process has not been properly controlled and resulted in problems in proving customer's acceptance of the terms. As a response to the growing privacy obligations, Microsoft has adopted new processes requiring VAR to confirm that their customer have accepted terms of Microsoft cloud agreement. Microsoft argues that such measures are necessary for assisting its partners to meet its compliance obligations while ensuring transparency.[102]

---

[94] Article 17 (1) of the GDPR.
[95] Article 28 (3) (e) of the GDPR.
[96] Article 28 (1) of the GDPR.
[97] CSP program guide, available on: https://docs.microsoft.com/en-us/partner-center/csp-documents-and-learning-resources#cloud-solution-provider-program-guide. Art 6. (a). Accessed May 9, 2019.
[98] W. Gregory Voss; Katherine H. Woodcock; Cecil Saehoon Chung; Kyoung Yeon Kim; Jai Lee; Doil Son, Privacy, E-Commerce, and Data Security, 49 Int'l Law. 97 (2015), P 102.
[99] Microsoft Customer Agreement, available on: https://www.microsoft.com/licensing/docs/customeragreement. Accessed May 9, 2019.
[100] Microsoft Docs, available on: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31
[101] Ibid. p.8. Accessed May 9, 2019.
[102] Microsoft cloud agreement attestation, available on: https://docs.microsoft.com/en-us/partner-center/confirm-consent-faq. Accessed May 9, 2019.

6. MINIMUM DPA CONTENT REQUIREMENTS

The Recital 81 to the GDPR clarifies that the fulfilment of the formal content requirements associated with a DPA must be based on the "*specific tasks and responsibilities of processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject"*. The author believes that the agreement between controller and processor which precisely addresses the processing details and responsibilities of processor is a prerequisite for claiming that controller has selected the processor that is providing "*sufficient guarantees*" pursuant to the Article 28 (1), and has considered the impact on a data subject prior to commencement of processing.

The ICO guidance on "Contracts and liabilities between controllers and processors" guidelines provide that DPA needs to be very clear about the scope of processing, and no "*catch all*" contract terms can be used. [103] Even though it is crucial for SaaS providers to have a standardized DPA's, the indication of all possible types of personal data by, for example, adding reference to the Article 4 of the GDPR, or defining purpose of processing as any "*contract related activities*" (without describing the functions) is not compliant with the GDPR. It is argued that, along with strengthening controller's rights by providing the processing control mechanism, DPA is the vital peace of information on processing details and, as asserted further, is deemed as documented evidence of controller's compliance with the principles of processing.[104]

6.1. Processing Details: Subject Matter, Nature and Purpose of Processing

Prior to 25th of May 2018, companies have been largely engaging in "re-papering" of their existing contracts to include the DPA content requirements. While their efforts were based on the interpretation of the Article 28 (3) of the GDPR, the term "*subject-matter*" has been received by many as to reflect the purpose of the processing. And whereas the purpose of processing may reflect the subject-matter of the processing, author finds these two concepts to have a different purpose.

Both Microsoft[105] and Amazon[106] define "*subject-matter*" as processing of customer related personal data within the scope of the GDPR. By doing so, parties are agreeing that the object which undergo processing is personal data. While author agrees with the approach taken by Microsoft and Amazon, author believes that "*subject-matter*" of processing should include the general objective or task, performance of which requires processing of personal data.

---

[103] Information Commissioner's Office GDPR guidance: Contracts and liabilities between controllers and processors, available on: https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf. Accessed May 19, 2019. P. 13.

[104] Article 5 of the GDPR.

[105] Microsoft Online Terms, available on: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31 p.8. Accessed May 19, 2019.

[106] Amazon Data Processing Addendum, available on: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf. Accessed May 2, 2019.

Subsequently, a DPA would clarify what processing operations constitute the nature of processing and assigns purpose to one or all of the named processing operations. The author believes that not only the purpose of processing, but subject matter as well should justify engaging in processing. Subject matter should demonstrate the link between the processing and the main transaction (e.g. provision of software) between controller and processor.

Nature of processing can be construed as one or many processing operations performed with respect to personal data (e.g. storage, erasure, use, etc.). DPA itself is an initial set of instructions for processor, containing the authorization for the use of processing operations carried out with respect to the defined personal data. Identifying the nature of processing is paramount in performing a privacy risk assessment to identify and manage privacy risks.[107]

Purpose of processing describes why parties engage in processing of personal data. It is important to link the nature of processing with the specific purpose parties pursue. For the convenience, some companies are providing the general link to the main agreement, stating that the purpose of processing is "*fulfilment of contractual obligations with customer*". The author believes that this vagueness does not meet the GDPR requirements. The purpose of processing needs be essentially consistent with the scope of legal basis relied by controller. For example, controller is using a SaaS ERP for accounting purposes. Let us assume that controller is acting within its employment contract with a data subject and has informed the data subject of its intention to use a third-party processor. Whereas, employment agreement is a valid legal basis under the Article 6 of the GDPR, it is confined to the set of specific functions required for controller to fulfil its obligations as employer. Therefore, employer is entitled to use SaaS ERP product to calculate payroll and manage resources. These functions, that are in line with the legal basis, must be reflected in a DPA and match the actual processing operations performed by processor. If, for example the scope of processing operations contains operations that exceed, the named purposes e.g. behavioural analytics, the controller must verify if it possesses the appropriate legal basis.

It is true that some SaaS providers are employing the same processing operations among all of their products and therefore, the indication of particular purpose is not principal. However, parties must acknowledge that failure to recognize the concrete purpose of processing would mean inability to verify whether the processing operations are required at all. If processing operations cannot be justified, such processing would be contrary to the purpose limitation principle[108]. That is why, when defining the purpose of processing, parties should indicate the precisely what products and services require processing operations included in the "*nature of processing*" and "*types of personal data*" and "*categories of data subjects*" included further in a DPA.

Clarity of these processing details is essential in ensuring timely response to data subject's access request according to the Article 15 of the GDPR without resorting to the controller's rights described in the Article 28 (3) (e) of the GDPR.

[107] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 p.6.
[108] Article 5 (1) (b) of the GDPR

Depending on the complexity, it is suggested that functionality the microservices used in the processing is used as purpose of processing. As a result, purpose of processing will not state a general purpose that is often copying the subject-matter of the main contract, but explicitly state what purposes are served by the processing.

To avoid any interpretation, purpose of processing can be linked with other processing details. For example, when indicating the purpose of processing, such purpose can be liked with specific type of personal data and processing means. For example, controller and processor agree that one of the purposes of processing is support ticket registration. That information can be supplemented by indicating the processing operations, (e.g. "storage", "registration", "disclosure"), as well as types of personal data, (e.g. first name, last name, company, title) and data subject's categories (e.g. controller's employees). Other services provided under the same agreement can be represented in the same manner. The benefit of that model is to assist controller in ensuring the transparency of processing, and data minimization principle as both parties would consider whether the processing details tied to a specific purpose are adequate and entail additional risk to the data subjects.

6.2. Duration of Processing

The duration of processing is an agreement between controller and processor with regards to the time period in which processor processes personal data, including storage. Article 5(1)(e) of the GDPR states that storage of personal data is permitted for as long as necessary for the legitimate purpose of processing. Upon completion of the purpose, or if the purpose is no longer legitimate, personal data must be minimized (erased, destroyed) or anonymized. For that reason, controller must be aware of the systems where the personal data is kept.

The duration of processing is dependent on the purpose of processing. If a contact specifies multiple purposes, when one of purposes is achieved, the data relevant with that purpose must be erased or anonymized. That is another argument in favour of the model in which purpose is linked to the other processing details. In most of the SaaS contracts, the duration of processing of data is linked to the subscription term, i.e. the processor processes personal data to the extent required by the agreement with controller. If that subscription is terminated or expired, the legal basis for processing is void. Accordingly, processors are required to construct its technical environment and internal processes to manage erasure of personal data from all systems (including backup copies)[109] upon termination, early expiry of the subscription, or when specific purpose identified in the DPA ceases to exist.

6.3. Types of personal data

According to the Article 28(3) of the GDPR, DPA must reflect the type of personal data and categories of data subjects whose data is required for processing on behalf of controller. That requires identification of the entire set of personal data that will be available to processor.

[109] Mariusz Krzysztofek, *GDPR: General Data Protection Regulation (EU) 2016/679 Post-Reform Personal Data Protection in the European Union,* 2016, Available on: Wolters Kluwer Digital Book Platform. Accessed April 12, 2019. p 70

Article 4 (1) of the GDPR defines personal data as any information by which a person can be identified, directly or indirectly by a reference to a specific identifier. The Directive 95/46/EC provided the similar definition of personal data, however the definition provided in the GDPR also emphasized that identifiers include also the "*online identifier*". GDPR provides examples of online identifies, which includes IP address, cookie identifiers[110] or other identifiers which, combining with other unique identifiers can be used to identify a natural person. It may also include the behaviour traits online as a consumer or regular Internet user.[111] Even subjecting data to "pseudonymisation" is merely a measure to "reduce the risks to the data subjects"[112] and remains a personal data, since the pseudonymisation process is reversible.[113]

According to Recital 26 of the GDPR, any identifier that can be used to identify a natural person by a reasonable means. To assess whether the means are reasonable the factors, such as costs, the amount of time required for identification, and available technology are considered.

Hence, if a processor possesses such reasonable means of using an identifier to directly or indirectly identify a person, such identifier is deemed as personal data and must incorporated in a DPA. Furthermore, when there is a substantial change in business rendering the reasonable means of identifying a person by available identifiers such data can become a personal data[114] and therefore must be covered by a DPA.

In the Case C-582/14 Patrick Breyer v.Bundesrepublik Deutschland[115], CJEU confirmed that IP address can be regarded as personal data. If a company possesses additional information that, in combination with a dynamic IP address can help to identify a natural person, such dynamic IP addresses that are valid only for the duration of the internet connection is regarded as personal data. But if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant', such identifiers are not regarded as personal data[116]. Therefore, such identifiers should not necessarily be included in a DPA. Inclusion of any personal data into a DPA results in assessing whether the applies IS means are adequate for security of that data.

It is evident that the list of identifiers included in the GDPR is far from exhaustive and the concept of indirectly identifiable person must be kept in mind when identifying what data will be accessible to a processor. Therefore, a SaaS provider needs to conduct an assessment which consists of identifying what type of information it processes and evaluate its technical and financial capacity in rendering such data personal.

---

[110] Recital 30 of the GDPR
[111] Recital 30 of the GDPR
[112] Recital 28 of the GDPR
[113] Recital 29 of the GDPR
[114] Mariusz Krzysztofek, *GDPR: General Data Protection Regulation (EU) 2016/679 Post-Reform Personal Data Protection in the European Union,* 2016, Available on: Wolters Kluwer Digital Book Platform. Accessed April 12, 2019. p 44.
[115] Judgment of 19 October 2016 in Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, CELEX: 62014CJ0582.
[116] Judgment of 19 October 2016 in Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, CELEX: 62014CJ0582, Para 46.

Some data can be regarded as personal by the party possessing the means of accessing it. For example, SaaS provider is delivering a cloud storage, such as Amazon S3, Microsoft OneDrive to customer. Provided that data is encrypted or pseudonymized would mean that customer is in possession of a means of making the data personal. In such a case, the data will remain personal with respect to the customer, whereas in absence of decryption key or pseudonymisation reversal key or other reasonable means available to processor, such data would be non-personal.[117]

Another question is whether there must be a DPA between a cloud storage provider as a processor and customer as controller. It is obvious that data hosting constitutes a processing according to the Art 4 (2) of the GDPR. However, if a database is encrypted, pseudonymized and such cloud storage provider is not in possession of reasonable means of rendering that data personal, it is unclear whether a DPA needs to be signed as the transferred data may not be considered personal.

However, the teleological analysis of the Article 28 (3) suggests that there must be a DPA between a cloud storage provider and customer, since the encrypted or pseudonymized data base can under some circumstances become personal data, and if such data base is compromised due to inadequate security measures taken by processor, another entity with the encryption key or otherwise possessing means of accessing that data would harm data subjects. That is why DPA must outline the types and categories of data subjects that such data base is going to contain. That will allow data processors to apply the measures appropriate for security, confidentiality and integrity of a cloud database. Another option would be to specifically exclude some types of data, such as special categories of personal data processed according to the Article 9 of the GDPR ("*Sensitive Data*"), and thereby allocate responsibility in a way that processor is responsible only for security of non-sensitive data.

It is crucial for SaaS companies to have a unified DPA applicable to multiple services which involve processing. The self-service and the lack of complex processes requiring verification of each agreement separately is a prerequisite for any scalable product.

For example, AWS GDPR Data Processing Addendum[118] used by Amazon defines type of personal data as "*Customer Data uploaded to the Services under Customer's AWS accounts*[119]". Further, the term "*Customer Data*" not defined. Another example is a Data Processing Addendum of the cloud storage provider – Exoscale which states that "*Type of personal data: personal data uploaded to the Services under Client's Exoscale accounts*". [120] However, the generalized scope of processing details that does not clearly specify what types of personal data is in scope should not be compliant with the GDPR.

Possible interpretation is that personal data processed by processor may include any personal data defined in the Article 4 (a) of the GDPR. It is true that cloud storage provider may

---

[117] Mariusz Krzysztofek, *GDPR: General Data Protection Regulation (EU) 2016/679 Post-Reform Personal Data Protection in the European Union*, 2016, Available on: Wolters Kluwer Digital Book Platform. Accessed April 12, 2019. p 49.

[118] Amazon Data Processing Addendum, available on: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf. Accessed May 2, 2019.

[119] Amazon Service Agreement, available on: https://aws.amazon.com/agreement/. Accessed May 2, 2019.

[120] Exoscale DPA, available on: https://www.exoscale.com/dpa/, Section 2. Accessed May 2, 2019.

have limited knowledge of what types of personal data are being processed (e.g. cloud storage provider) and therefore resort to the vague terms. In addition, fine-driven pressure applied by GDPR and supported by growing concern from customers has made processors to apply highest information security standards that are enabling controller to process virtually any type of data in the relatively secured manner. Another scenario used by cloud providers is to create a non-exhaustive list of types of personal data and categories of personal data subjects. For example, company might state that personal data processed under a DPA "*might include*" or "*includes but is not limited to*" certain types and categories of personal data. By doing so, the DPA would apply to any data processed, whereby processor remains liable for obligations of Article 28 (3) of the GDPR with respect to that data.

Identification of what types of personal data is involved in the processing is vital for both parties to comply with the "*Purpose Limitation*" principle defined in the Article 5(1)(b) of the GDPR. According to this principle, personal data must be processed to the extent necessary for achieving the specific processing purpose. Controller must be aware what data is processed in order to make a reasonable judgement whether this data is not exceeding the processing purpose. SaaS providers, in designing a new service needs to create a data flow architecture to define a minimum data required to enable the functionality. If SaaS provider concludes that functionality can be retained when only relying to pseudonymised data rather than personal data, then the use of personal data is breaching the data minimisation principle.[121]

For example, SaaS service requires creation of the end user profile by using an email or login. The email is sufficient to enable the log-in function and is clearly matching the purpose. However, if the nature of SaaS product implies managing of sensitive or confidential data, SaaS provider may consider increasing the level of security by adding two-factor authentication, user and/or device authentication.[122] Application of such measures may require additional information, such as geographical location, IP of a device, or phone number. This feature is consistent with the market demand of secure SaaS service (which becomes additional purpose of processing) and collecting of additional types of data is justified.

Another question is whether data that is required by processor to comply with its legal obligation should be included in the DPA. Processor may become itself controller for data that it collects for purposes of compliance with laws, such as Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. Adherence to such laws require company to create a "*Know your client*" and have an "*Anti-Money Laundering"* processes that involve identification of person my ID and other identifiers. In addition, processor may be interested in storing customer's contact data for other purposes, e.g. contact persons from accountant and legal departments for collection of accounts receivable. Interpretation of Article 28 (3) of the GDPR suggests that DPA is entered into between controller and processor. Therefore, should SaaS provider carry out processing which exceeds the purposes assigned by

[121] Mariusz Krzysztofek, *GDPR: General Data Protection Regulation (EU) 2016/679 Post-Reform Personal Data Protection in the European Union,* 2016, Available on: Wolters Kluwer Digital Book Platform. Accessed April 12, 2019. p 61

[122] Bladford, Richard, *Information Security in the Cloud,* Network Security 2011, No.4 (2011): 15-17. Doi:10.1016/s1353-4858(11)70040-x, P. 16.

customer, SaaS provider becomes controller of personal data, and thus is not required to enter into DPA with customer to govern the processing performed under the purpose defined by that SaaS provider.

Moreover, Recital 14 of the GDPR makes an important clarification that contact details of legal persons including the name and the form of the legal person and the contact details of the legal person is not covered by the requirements of the GDPR. That means that such data can be freely processed in any manner chosen by a person, for as long as processing of that data do not violate other laws and regulations. Therefore, even if a company name consists of personal data identifiers and details of signatories are included in the agreement, there is no need to enter into a DPA to regulate the processing of that data, since this data is not covered by the GDPR.

Further question is whether any end-user using SaaS product is regarded as "*company representative*" in terms of Recital 14 of the GDPR. Author believes that GDPR does not intend to create obstacles for companies to engage in business activity which require customer identification and subsequent processing of company related data. Therefore, while a signatory of the company may act as end-user of SaaS product, the user management functionality allowing to add or remove other users is regarded as processing of personal data (provided however that end-user data contain personal data) and must be covered by a DPA. Otherwise, all customer's employees, added as users, would be exempt from the requirement of the GDPR, regardless of the scope.

Another issue is related to whether processor recognizes individual end-user data categories as personal data. For example, if a user is created by one identifier, e.g. email address. One can argue that, even if an email is composed from a fist and last name of a person, including a company domain, it is not necessarily a personal data, since there can be multiple persons within a company with a same name.[123] However, unless an email is purely of general nature, such as info@company.com. Author advises to include that email address in a DPA, since SaaS company would probably possess additional information such as IP address and be able to identify a person.[124] The email are used more and more to substitute traditional mail, therefore more and more systems would add sources to link the email with a specific person.[125] The same goes for a phone number, which has been proven to be a standalone sufficient to identify a person. The experiment conducted by Jonathan Mayer and Patrick Mutchler of Stanford University revealed that by having solely a phone number of a person, more than 90% of persons can be identified by using a social media channels such as Facebook, Yelp, Intelius and Google Places[126]. Therefore, if there is end-user management functionality within the SaaS product, DPA is required.

---

[123] Mariusz Krzysztofek, *GDPR: General Data Protection Regulation (EU) 2016/679 Post-Reform Personal Data Protection in the European Union,* 2016, Available on: Wolters Kluwer Digital Book Platform. Accessed April 12, 2019. P. 46.
[124] Ibid.
[125] Ibid. P. 47.
[126] R.J. Rosen, 'Stanford Researchers: It Is Trivially Easy to Match Metadata to Real People', The Atlantic, available on:http://www.theatlantic.com/technology/archive/2013/12/stanford-researchers-it-is-trivially-easy-to-match-metadata-to-real-people/282642/. Accessed May 7, 2019.

Having regards to the fact that some data may become personal by the use of other data or reasonable means in processors possession, it is recommended to include all types of data that is being processed with respect to a data subject. Even if such data is kept separately.

Such additional identifiers may include:

a) **Account data,** including username (even nicknames)[127], user behaviour (preferences, feedback and the information about the ways a product or service is used).

b) **Technical data,** including IP address, location data, operating system and its version, information about devices used to access the service, cookies, time zone settings, browser plug-ins, radio frequency identification (RFID) tags, and other online identifiers[128];

c) **Financial and transaction data**, including payment details and details on purchased goods and services.

6.4. Categories of data subjects

By indicating categories of data subjects, the parties are agreeing on what classes of data subjects that are going to be affected by the processing. Understanding the scope of affected data subjects is vital for the proper risk management and application of the appropriate technical and organizational measures for keeping the data secured.

Determining the types of personal data is not enough to recognize the possible harm inflicted on the data subject should the personal data be subject to unauthorized disclosure, alteration or destruction. For example, billing software, provided by SaaS provider, aggregates data on transaction history of multiple data subjects. If such product is provided to a hospital, DPA must reflect that data subject categories may include patient data, and not just types of data which does not, in this case, fully reflect the sensitivity of that data.

On the other hand, if patients are included as data subjects, controller has communicated this information to processor and therefore expect processor to take appropriate actions for safeguarding this data. Otherwise, processor might claim that deficit of information of the processing details resulted to application of the insufficient security controls that would have been otherwise applied should the processor possess that knowledge. Therefore, it is highly recommended to explicitly include all classes of data subjects that are going to be affected by the processing. Even if processing is carried out with respect to limited data, e.g. only IP address, the data subject categories whose IP address is collected must be included.

Of course, this task is quite difficult for storage and hosting providers that often have no real access to the data. However, even considering the ultimate responsibility of controller, DPA must include the preliminary list of data subject's categories that controller intends to include in a

[127] Mariusz Krzysztofek, *GDPR: General Data Protection Regulation (EU) 2016/679 Post-Reform Personal Data Protection in the European Union*, 2016, Available on: Wolters Kluwer Digital Book Platform. Accessed April 12, 2019. P. 46.
[128] See. Recital 30 of the GDPR.

database. Another option would be for processor to impose limitations on permitted types of personal data and categories of data subjects. In this case, controller would be in a breach of contract and no consequences related to insufficient technical and organizational measure would be attributed to processor. The examples of categories of data subjects include the following categories: employees, agents, partners, customers, suppliers, consultants, users. In addition, each category may be defined as well. E.g. "*user*" may be defined as any person that is using service or product on behalf of the controller.

6.5. Documented Instructions from Controller

According to the Article 28(3)(a) of the GDPR, processing by processor must be based solely on the documented instructions from the controller, insofar there are local laws that require processor to transfer personal data. In this case, processor is obliged to informs controller prior to carrying out the transfer.

This principle entitles controller to remain in control of the processing of personal data by ensuring that the processing is guided by the means of instructions from controller. At the same time, processor is acting solely within the boundaries set by controller and, in order to comply with this provision, must have the evidence, proving the connection between its processing records and controller's instructions. In absence of such evidence, processor may be found as acting beyond controller instructions, and therefore itself be qualified as controller[129] for some processing operations which exceeds the controller's instructions, or, in some cases, the processing may be regarded as unlawful in its entirety.

For this reason, GDPR requires such instructions to be documented, although, GDPR does not lay down requirements for documenting instructions. Parties may resort to any means of documenting instructions, insofar as such instructions can be proven to exist and reflect the details of the processing that can be reasonably understood.

The instruction is the instrument of communicating the details of processing to the processor. For that reason, the DPA, per se, serves as the set of processing instructions. By including a processing details in a DPA, the processor is subject to the initial instructions that clarify (i) what type of data is going to be processed; (ii) by what means; (iii) for what purpose; and (iv) what security measures must be applied. Going further, parties can agree on the process of issuing instructions, e.g. by amending an agreement, sending email, change request, or by using product functionality. Considering the pressure coming from controllers rigorously preparing for GDPR compliance, SaaS companies tend to keep the trend and implement functionality that allows for complete control of personal data within the SaaS product, e.g. create, alter, erase, export personal data. Author argues that implementation of such functionality is to be qualified as automation of controller's processing instructions, since, in fact, processing is carried out within processor's computing environment upon controller's instructions given via web user-interface.

While processing ought to be limited to controller's instructions, the nature of service may preclude processor from completing some of the given instructions. For example, if

[129] Article 28 (10) of the GDPR

controller is using a cloud storage provider to host its encrypted database, such cloud storage provider cannot be instructed to access or use the data without having an encryption key. That is why the Article 28 (3) (a) of the GDPR does not state that processor must adhere to the instructions, but only that instructions form a basis of processing by processor.

6.6. Confidentiality

Even though data breaches can be caused by different factors, the ICO report for 2018 revealed that human error remain the leading cause of data breaches.[130] Human error is usually an indication of inadequate process fulfilment controls and lack of privacy awareness. After all, and organization consists of individuals that must be aware of their responsibility in keeping the data secure. That is why the Article 28(3)(b) of the GDPR requires processor to ensure that its personnel authorized to process the personal data is bound by confidentiality or is under appropriate statutory obligation of confidentiality and is informed how to handle personal data.

Authorization to process personal data applies to all persons that are exposed to personal data, carry out any processing defined in the Article 4(2) of the GDPR, including having access to such personal data.

Therefore, comply with this requirement, processor must:

a) identify the persons within its organization that are authorized to process personal data under authority of a controller;

b) verify that these persons are bound by confidentiality obligations;

c) ensure that these persons are aware how to handle personal data.

The term "*personnel*" is used to refer to the entire processor's organization, including permanent and temporary employees. For SaaS providers, and IT in general, it is not uncommon to outsource software development and other functions to contractors, including "*freelancers*". Thereafter, some functions performed by external developers may requires access to the database, which constitutes the processing of personal data. Nevertheless, such contractors are not regarded as processor's personnel in the context of the Article 28(3)(b) of the GDPR. Even though, it can be argued that developing a new product functionality is consistent with purpose of processing defined by customer, the fact that contractor is instructed by SaaS provider that defines the "*purposes and means of processing*" indicate that contractor is acting as processor for SaaS provider rather than a sub-processor of customer pursuant to the Article 28 (3) (d). Therefore, the confidentiality obligations will not be applied to such contractors. Nevertheless, there is no prohibition in extending the term "*personnel*" to include sub-contractors of processor. Therefore, in drafting DPA controllers may specify that personnel mean any person (acting on the processor's instructions or otherwise) that is authorized to process personal data.

On the other hand, to ensure lawfulness of processing, SaaS provider would need to enter into a DPA with its contractors that are processing personal data. There are numerous ways for establishing confidentiality obligation for personnel. Perhaps the most popular ones are

[130] Information Commissioner's Office report on "Data Security Trends", available on: https://ico.org.uk/media/action-weve-taken/reports/2014675/data-security-trends-pdf.pdf. Accessed May 19, 2019.

incorporating confidentiality into the employment agreement, enforcing company policy documents, signing a "*Non-Disclosure Agreement*". However, the inclusion of confidentiality obligations must be done in careful consideration of the employment law. Application of fixed penalties for infringement of confidentiality obligations may not be valid under some jurisdictions.

The second part of the requirement is to ensure that processor's personnel is aware of how to handle personal data. That requires processor to introduce and maintain internal information security policies and procedures supported by security awareness training routines.

6.7. Ensuring Security of Processing (Article 28 (3) (c) of the GDPR)

The DPA must contain an obligation for processor to "*take all measures required pursuant to Article 32*".[131] Unlike the Article 28 (1) which requires processor to provide "*sufficient guarantees*" to meet the requirements of GDPR, Article 32 of the GDPR is more specific and contains direct statutory obligations requiring controller and processor to implement the "*appropriate technical and organisational measures*" to ensure the level of security of personal data appropriate to the risk and cost of implementation.

There can be no doubt that the wording of the article is vague and there is no precise formula to determine which technical and organizational measures are to be applied in which particular case. Hence, the interpretation of the "*appropriate measures*" is left for data protection authorities and courts[132] to clarify. Nevertheless, the author believes that broad interpretation is reasonable given the rapidly evolving technologies, expanding market of security products and growing capabilities of companies in applying information security controls.

Accordingly, processor must ensure the ongoing compliance requirements with adapting its *technical and organisational measures* according to its capabilities, then-current risk level entailed by the processing and changes to the processing environment.

In drafting a DPA, the author recommends retaining the term "*appropriate*" while including the minimum-security measures pertaining to the processing details. The appropriate means that processor is, at all times, responsible for matching its security controls with the risk level, by maintaining the process for regularly testing and assessing the effectiveness of its technical and organizational measures. By doing so, the processor will be required to tackle the changes in processing instructions by adapting its existing IS measures accordingly.

Nowadays, many controllers are widely applying IS due-diligence process before selecting the feasible processor. It is recommended to list the minimum technical requirements that are relevant to the processing.

Therefore, author advises parties to use the Article 32 of the GDPR along with other guidelines for implementing appropriate measures, in a form of processor's obligations, stating

[131] Article 28 (3) (c) of the GDPR
[132] Paul Voigt, Axel von dem Bussche. *The EU General Data Protection Regulation (GDPR). A Practical guide. Germany,* 2017. Page 64

that whereas appropriate, processor must implement appropriate technical and organizational measures, including:

a) protection of personal data against destruction, modification, unlawful dissemination, or unlawful access;

b) protection of personal data against all forms of unlawful processing;

c) pseudonymisation and encryption of personal data;

d) maintenance of ongoing confidentiality, integrity, availability and resilience of processing systems and services;

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

f) implementation of process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

g) having internal security policies, security awareness trainings, as well as implementing technical, physical security and access controls;

h) adhere to the principles of "Privacy by Design and Privacy by Default" when developing new product features[133];

i) use of Data Protection Officer to carry out assessment to determine whether the applied controls are appropriate to the security risks[134].

As mentioned throughout the thesis, the typical SaaS contract involves multiple parties processing personal data. Therefore, the customer facing DPA will be based on security commitments of all the processing chain, including VAR, SaaS provider, microservices provider and other parties. In other words, the DPA will resemble all controls applied by the main processor and its sub-processors.

Apparently, this may lead to unclarity whether these are the measures provided by the processor under a DPA, or processor guarantees that such measures are taken by its sub-processors. In that regard, author recommends linking the "*purpose and nature of processing*" with the security controls and clarify the responsible entity. It could be complicated to include the name of specific sub-processor, although the processor could clarify the function undertaken by such entity. For example, "*Physical Security is ensured at all level of processing, For the purposes of protection of personal data against unlawful access, disclosure, alteration and destruction, physical security controls are applied by SaaS Provider, VAR and all sub-processor included herein*". By doing so, customer will gain clarity and confidence regarding the applied measures. Otherwise, customer may be misled by DPA listing the applied solely by VAR, whereas the security measures applied by its supply chain will remain unclear, despite the fact that processor is obliged to impose the same obligations to its sub-processors.[135]

[133] Paul Voigt, Axel von dem Bussche. *The EU General Data Protection Regulation (GDPR). A Practical guide. Germany,* 2017. P. 38
[134] Ibid. P. 64
[135] Article 28 (4) of the GDPR.

The processor may demonstrate its compliance with Article 32 of the GDPR by adherence to the approved certification mechanism.[136] Therefore, as a means of ensuring the compliance with the Article 32 of the GDPR controllers may require processor to maintain certificates relating to its processing, such as such as ISO 27001 – Information Security Management System (or versions for cloud services - ISO 27017) ensuring that processor takes a risk based approach in securing its information[137], or Payment Card Industry Data Security Standard ("PCI DSS") in case processing concerns payment card and transaction data.

In addition, SaaS companies may increase the value of their product by offering additional security. Since the article 32 applies to both controller and processor, provision of minimum appropriate measures under the article 32 of the GDPR must be performed by default, without extra charge. However, nothing in the GDPR precludes processor to monetize on security add-ons which exceed the defined minimum.

6.8. Using another processor ("Sub-Processor")

As presented throughout the thesis, SaaS delivery model typically involves multiple parties engaged in processing of personal data on behalf of controller. SaaS provider or VAR may be using sub-processors, such as microservices provider. However, GDPR introduced very important change by empowering controller to exercise more control over the entire processing "*supply chain*". The control is established by the following means:

c) Processor must obtain controller's authorization prior to engaging sub-processor; In case of general written authorization, processor must inform controller each time the sub-processor is added or replaced, thereby giving the controller the opportunity to object.[138]

d) Processor must pass to sub-processor the same data protection obligations as those set forth in the DPA with controller.[139]

e) Processor remains fully liable for sub-processor's failure to ensure compliance with data protection obligations.[140]

GDPR allows parties to agree on the general authorization which typically allows processor to appoint sub-processor that are GDPR compliant, by providing a notice to the controller, or otherwise making that information available to the controller. The general authorization is the only viable solution with respect to SaaS delivery model, as it would be impractical for SaaS providers to obtain authorization from each of their customers every time SaaS provider intends to add or replace a microservice or other service managed by sub-processor. However, the second sentence of the Article 28 (2) provides that with respect to general authorization, controller must be given opportunity to object. Literal interpretation of this provision suggests that controller is allowed to abuse its right to object, by objecting to any sub-processor at its own discretion, without providing any reasoning supporting its decision.

---

[136] Article 40 to 43 of the GDPR

[137] *EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide*, Second edition, IT Governance Privacy Team, 2016, 2017, p. 64.

[138] Article 28 (2) of the GDPR

[139] Article 28 (4) of the GDPR.

[140] Ibid.

However, according to the author's interpretation "*opportunity to object*" [141] implies that the right to object may be subject to certain conditions agreed between controller and processor. For instance, SaaS provider may publish and maintain the list sub-processors. Subsequently, the list can be modified by SaaS provider upon providing a notification to customer that is entitled to object against any sub-processor, within the reasonable time period (e.g. 14 working days), by submitting the written document summarizing the reasons for objection. However, that takes an administrative burden, since publishing the potential sub-processors must be done prior to integration with a SaaS product given that any integration implies financial investment. That would create obstacles for making business and limit the SaaS company's ability to improve product or optimize its business costs. For that reason, general authorization entitling SaaS provider to appoint sub-processors and limitation of customer's right to object (to the extent such limitation is reasonable and is not contrary to the GDPR remains the preferred option.

The DPA between processor and sub-processor must encompass the same obligations imposed on sub-processor as those undertaken by processor under a DPA with controller. As a result, DPA will resemble the back-to-back agreement structure, in which sub-processor DPA (along with obligatory content requirements) will be defined by the obligations set out by controller. If processor allows controllers version of DPA to be used, adding a new controller would require processor to verify if its existing DPA with sub-processor conforms to controller's DPA. If not, the DPA with sub-processor should be modified to reflect processor's obligations. If this model is applied, it is recommended to create annexes to the main DPA between processor and sub-processor for each controller. Should the agreement with controller cease to exist, annex must be terminated accordingly. In addition, any fixed penalties applied to processor would probably need to be transposed to sub-processors, if applicable.

Even though, in theory, this can be automated, in practice, "*pushing down*" the exact terms of the controller's DPA may not be practical.[142] The SaaS product delivery model is very vulnerable to the issues that may block the swift product delivery strategy. Therefore, SaaS providers cannot afford in engaging into lengthy contract negotiations. Therefore, SaaS providers happen to apply the reverse scenario. Such scenario provides that DPA with controller is standardized, and compiles the commitment to security, data breach notification and data subject's rights request processing from sub-processors. In other words, when processor creates its DPA, processor links processing operations fulfilled by sub-processor with its commitments associated with this particular processing e.g. data storage provider ensures physical and environmental security of its servers.

Accordingly, the processor will indicate in its DPA with controller that nature of processing includes "*personal data storage*" and technical and organizational means include "physical and environmental security of personal data when stored". Therefore, the effective use multiple sub-processors are conditioned upon processor's ability to use its own version of DPA.

6.9. Protecting Data Subject's Rights

[141] Article 28 (2) of the GDPR

[142] Pieter Gryffroy, *Computer and Telecommunications Law Review 2018 Legal aspects of multi-cloud: more clouds, more problems?,* Sweet & Maxwell and its Contributor. C.T.L.R. 2018, p. 131.

Under the Directive 95/46/EC the controller mainly responsible for ensuring that data subject's ability to exercise their rights. However, the gaining popularity of outsourcing processing function and amount of shared functions made it clear that controller is struggling in fulfilling data subject's rights without the means of obtaining the support from across the processing chain. That is why Article 28(3) (e) of the GDPR requires processor to whenever possible, and considering the nature of the processing, to assist controller with fulfilment of controller's obligation to respond to requests for exercising the data subject's rights by applying technical and organizational measures.

Pursuant to the Chapter III of the GDPR, data subjects have the following rights:

a) **Right to be informed.** Data subject is entitled to obtain information on the processing of his or her data;[143]

b) **Right to access.** Data subject is entitled to get confirmation from controller regarding processing of his or her personal data[144] and receive a copy of such data in a commonly used electronic form[145];

c) **Right to rectification.** Data subject is entitled to request rectification of his or her personal data if such data is inaccurate;[146]

d) **Right to be forgotten.** Data subject is entitled to request erasure of his or her data[147];

e) **Right to object.** Data subject is entitled to restrict processing of his or her personal data[148], including the right to object to automated individual decision-making, profiling and direct marketing purposes[149];

f) **Right to portability.** Data subject is entitled to request its personal data to be provided in a structured, commonly used and machine-readable format and get such data transmitted to another controller[150].

The conformity with this obligation requires processor to establish the processes for communication, management, control and verification of data subject's requests among all of its sub-processors. For instance, controller receives the request for complete erasure of personal data from an identified data subject. Subsequently, controller notifies its processor, which, in turn, must delete the personal data from its own systems and procure that its sub-processors do the same. I may become complicated in the Model No.2 in which customer may purchase a bundle of different SaaS product from a VAR that is not itself acting as processor. In this case, customer is having a direct DPA with each of SaaS providers. That requires customer as personal data controller to notify its processors separately.

However, a lot of SaaS products nowadays integrate the functionality that enables automated fulfilment of requests related to data subject's rights. As a result, controllers can order processor

[143] Article 12–14 of the GDPR
[144] Article 15 (1) of the GDPR
[145] Article 15 (3) of the GDPR.
[146] Article 16 of the GDPR.
[147] Article 17 of the GDPR, see. also 116 C-131/12, Google Spain, 13 May 2014.
[148] Article 18 of the GDPR.
[149] Article 21–22 of the GDPR.
[150] Article 20 of the GDPR.

and its entire processing chain to carry out operations required to fulfil data subject's rights. For example. For example, Microsoft has implemented its compliance management functionality to manage and control data lifecycle to ensure timely response to data subject's rights.[151]

The wording of the Article 28(3) (e) of the GDPR suggests that processor must contribute to fulfilment of controller's obligation to respond to requests for exercising the data subject's rights, taking into account "*nature of the processing*" and "*insofar as this is possible*". GDPR acknowledges that processors are exempt from this obligation should the nature of processing limit the processor ability to apply the processors ability to fulfil data subject's requests.

The author believes that the concept "*nature of processing*" in this context cannot be construed as business reasoning that renders the fulfilment of data subject request expensive. Where the application of technical and organizational measures is reasonably possible, processor is obliged to employ them. When the cloud storage provider is used to store encrypted database on behalf of controller, the limited access to the personal data would preclude cloud storage providers from directly assisting controller in "*fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights*" according to the Article 28 (3) (e) of the GDPR. Nevertheless, the cloud storage provider can fulfil this requirement by implementing the functionality that enables controller to access a database and effectively carry out actions required for exercising data subject's requests.

6.10. Assisting controller in ensuring security of processing, data breach notification and PIA

In addition to being subject to direct requirements to ensure the security of processing[152], the processor is required to assist controller in ensuring security of processing. That can hardly be interpreted as processors obligation to implement information security controls within the controller's environment. Instead, author believes that assistance must be expressed in processor's compliance with the principle of secured processing and subsequent supply of information regarding the security functionality to controller.

This may include sharing with controller the results of PIA, furnishing information on potential risks, and being proactive in implementing security features based on controller's request/feedback. The continuous implementation of security controls and functionality for security customization can be indications of a good practice of contributing to controller's obligation related to secure processing.

In addition, processor must notify the controller without undue delay after becoming aware of a personal data breach.[153] Consequently, in order to assist controller's in notifying data protection authority[154], processor is required to, without undue delay, supply controller with information pursuant to the Article 33 (3) of the GDPR, should such information be accessible to processor. Controller may consider extending this obligation by requiring processor to investigate

[151] Microsoft compliance with the GDPR. https://techcommunity.microsoft.com/t5/Microsoft-OneDrive-Blog/GDPR-Compliancy-with-OneDrive-and-SharePoint/ba-p/191126. Accessed May 19, 2019. P. 17.
[152] Article 32 of the GDPR.
[153] Article 33 (2) of the GDPR.
[154] Article 33 (1) of the GDPR.

the breach, perform the root – cause analysis and assist controller in performing breach mitigation activities. The term "*without undue delay*" can be interpreted as immediately after processor becomes aware of breach and collects the basic information necessary for notifying controller. If a data breach involve potential harm to data subjects, the controller must notify data protection authorities within the 72 hours after becoming aware of the breach.[155] Accordingly, it is common to require processor to notify controller of any breach "*immediately, but no longer than within 48 hours"*. The author supports this approach, in spite the fact that the moment of becoming aware of the breach may be difficult to calibrate.

The processor's assistance in controller's obligations pursuant to Article 35 and 36 of the GDPR can be interpreted as follows: If controller determines that processing carried out by processor is "*likely to result in a high risk*" [156] to the data subjects, controller may either independently (by requesting information) or jointly with processor carry out PIA to assess the risks to data subjects associated with processing. If PIA confirms such risks, controller becomes obliged to consult with the supervisory authority prior to commencement of processing.[157] Processors contribution should be expressed in sharing details of PIA with controller.

6.11. Deletion of personal data

Besides the obligation to carry out processing based only on documented instructions from controller, Article 28 (3) emphasizes that, at the end of the service which requires processing and subject to controller's request, processor must return or delete all personal data, unless Union or Member State law requires storage of such data[158]. This provision requires automatic return or deletion of all personal data, whereas "*controller's request*" is referred to as decision whether to return or delete the data. The word "*return*" relates more to the physical copies of data, whereby returning physical copies may imply that processor is no longer possessing personal data. In SaaS product delivery model however, personal data must be automatically deleted, and if requested by controller, processor provides a copy of all personal data prior to deletion.

Naturally, such obligation is not extended to scenario in which SaaS provider keeps that portion of data, in relation to which processor is regarded as controller or keeps the records of fulfilment of data subject's request. The literal interpretation of this provision suggests that controller's request to have the personal data deleted means that processor should not merely anonymize this data but instead to follow the direct instruction to carry out deletion of personal data, as one of the processing operation defined in the Article 4 (2) of the GDPR.

6.12. Assisting controller in demonstrating compliance

[155] Article 33 (1) of the GDPR.
[156] Article 35 of the GDPR.
[157] Article 36 (1) of the GDPR.
[158] Article 28 (3) (g) of the GDPR.

Demonstrating compliance with the GDPR pursuant to the Article 5 (2) of the GDPR requires controller to be prepared to present documentation, records[159] and other evidence suggesting that processing has been performed in a secure, lawful and transparent manner, whereas the risk to the data subjects are being assessed and data subject's requests fulfilled. Furthermore, controller is selecting processor that provides "*sufficient guarantees*" by virtue of Article 28 (1) of the GDPR. Therefore, processor's compliance with DPA obligations becomes part of the controller's own compliance. Controller's failure to prove that its processors comply with the GDPR constitutes breach of Article 28 (1) of the GDPR. That is why DPA requires processor to:

a) make available to the controller all information necessary to demonstrate compliance with the GDPR;
b) contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

The wording "*demonstrate compliance*" opens a room for interpretation regarding whose compliance the information needs to be supplied. Apparently, processor has limited information about the controller's compliance, but since processor's compliance is interlinked with controller's, processor must make available information regarding its own compliance with the GDPR. If applicable, controller may request processor to explain how processor contributes to the controller's compliance with the GDPR. Answering on such request processor may include the following categories:

g) information about technical and organizational measures applied to keep personal data secured;
h) records of fulfilment of data subject's rights;
i) information about sub-processor's compliance;
j) results of PIA;
k) information about transfers of personal data outside EU;
l) information about personnel authorized by processor to process personal data.

For that matter, controller may oblige processor to keep the records of processing, despite the fact that processor might not be required to do so under the Article 30 of the GDPR.

Audits performed by controller or its auditors may include request of documentation or on-site inspections. However, nothing prohibits processor of limiting the scope and number of permitted audits. Processor may state that controller is not allowed to carry out audits for more than once per annum, unless controller has a reasonable evidence of processor's incompliance with the GDPR. Parties may also agree on who is responsible for covering expenses incurred in relation to an audit. It is unclear whether the Article 28 (4) providing that sub-processors are bound by the same obligations as processors, can be interpreted as controllers being able to directly audit sub-processors. The literal interpretation of this provision would suggest that processor is responsible for auditing sub-processor, although in practice, processor's audit will probably be based on that of controller. Therefore, for raising transparency and control, Model No.2, providing that controller can audit its processors directly is more beneficial.

[159] Information Commissioner's Office GDPR guidance: Contracts and liabilities between controllers and processors, available on: https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf. Accessed May 19, 2019. P. 17.

Lastly, processor must immediately inform controller if controller's instruction infringes GDPR or any other law. It is not specified in the GDPR whether suspicion of unlawful instruction entitles processor to suspend the processing. Having regard to the lawfulness of processing being one of the fundamental principles of GDPR[160], should the processor obtain information that instruction given by controller is unlawful, processor must immediately inform the controller and suspend fulfilment of the suspicious instruction until the matter at hand is resolved. Author advises SaaS providers and other processors to include the "*suspension clause*" which allows parties to temporary suspend the processing, in case processor reasonably suspects that controller's instructions are breaching GDPR or other laws.

[160] Article 5 (1) (a) of the GDPR.

7. CONCLUSION

It has been almost a year since GDPR entry into force and probably by now the companies have crystalized its approach with respect to the contractual structure for governing the processing of personal data.

It has been demonstrated that it is common for the complex structure of SaaS delivery model to involve processing of personal data by multiple parties responsible for their respective processing operations. The use of multiple parties entails additional information security risk and must be properly regulated. In the course of doing so, roles of each actor must be determined and reflected in the proper DPA.

Author encourages companies to regard DPA not just as another formality its GDPR compliance strategy, but an important instrument which brings clarity to the roles and responsibilities of each processing actor, empower controller in exercising control over personal data, and strengthens data subject's rights.

It is argued that failure to ensure an effective DPA would result in loss of control and inability to extend the such control down to the processing chain, thereby jeopardizing controller's compliance and causing harm to data subjects.

It has been confirmed that the current wording of the Article 28 (3) of the GDPR contains very broad concepts that ought to be adapted to the particular processing operations. Accordingly, author expects the crystallization of the term "non-compliant DPA" whereby courts or data protection authorities would find DPA failing to address the matters pertaining to the specific processing.

The following summary of benefits leads to the conclusion that, DPA should be signed between factual processor and controller, despite the fact that such DPA might circumvent the contractual structure of the main agreements.

Model No.1 – Customer is entering into DPA with VAR.

Pros	**Cons**
Customer is utilizing one centralized DPA.	Customer has no means of directly approaching SaaS provider. VAR must have a detailed knowledge of SaaS product and be responsible for abiding to customer's instructions. VAR role as processor is not justified, given that customer usually circumvents VAR by issuing direct instructions to SaaS provider. That may lead to SaaS provider being recognized as processor, whereas such processing would not be covered by a direct DPA and thereby deemed incompliant with the GDPR.

Model No.2.

Pros	Cons
VAR is relived from responsibility to enforce Customer's processing instructions, besides those concerning processing of personal data directly by VAR and/or its sub-processors. Customer can directly approach SaaS provider and issue processing instructions, which gives customer more access to its data. Processor's role is justified, and processing operations are described in individual DPA signed between customer and each SaaS provider. That results to increased awareness and more control over data.	Customer is bound by several DPA's thereby must maintain the means of issuing processing requirements directly to SaaS Provider which, in some cases may be problematic, e.g. SaaS providers, unlike VAR, are not providing local language support.

Further, in outlining the recommendations for filling in the content requirements and execution of DPA the thesis relies on the interpretation of the GDPR and analysis of the practice applied by large SaaS providers. Therefore, some portion of recommendations provided in this thesis might become redundant, since DPA must be adapted not only to the changes in contract law, contractual tradition, but changes in the ways the data is processed in within the current SaaS delivery model.

8. BIBLIOGRAPHY

Primary Sources

European Union Legislation

1. Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN. Accessed May 2, 2019.
2. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, OJ L 141, 5.6.2015. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849. Accessed May 19, 2019.
3. Directive 95/46/EC DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.95. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en. Accessed April 20, 2019.
4. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Accessed April 29, 2019.
5. Treaty on Functioning of the European Union, OJ C 326, 26.10.2012. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN. Accessed 1 May, 2019.

Case law

1. Judgement of 15 July 1964 in Costa v E.N.E.L, Case 6/64, CELEX: 61964CJ0006.
2. Judgment of 10 December 1969 in joined Cases 6 and 11-69 Commission of the European Communities v French Republic, CELEX: 61969CJ0006.
3. Judgement of 13 May 2016 in Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, CELEX: 62012CJ0131
4. Judgment of 19 October 2016 in Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, CELEX: 62014CJ0582

Secondary Sources

Books

1. Paul Voigt, Axel von dem Bussche. *The EU General Data Protection Regulation (GDPR). A Practical guide. Germany*, 2017.
2. *Fuster, Gloria Gonzalez, Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer, 2014.*
3. Mariusz Krzysztofek, *GDPR: General Data Protection Regulation (EU) 2016/679 Post-Reform Personal Data Protection in the European Union*, 2016, Available on: Wolters Kluwer Digital Book Platform. Accessed April 12, 2019.
4. Michael J. Kavis, *Architecting the Cloud, Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)*, Wiley & Sons, 2014.
5. David W.Tollen, *The Tech Contracts Handbook, Second Edition, Cloud Computing Agreements, Software Licenses, and Other IT Contracts for Lawyers and Businesspeople*.
6. Torgans K., Kārkliņš J., Bitāns A., Līgumu un deliktu problēmas Eiropas Savienībā un Latvijā. Prof. K.Torgāna zinātniskā redakcijā. Rīga: Tiesu namu aģentūra, 2017.
7. K. Balodis. Ievads Civiltiesībās. Rīga: Zvaigzne ABC, 2007.

8. Von Dawitz Thomas, *Europäisches Verwaltungsrecht* [European Administrative Law] Berlin: Springer, 2008.
9. Paunio E. Legal Certainty in Multilingual EU Law : Language, Discourse and Reasoning at the European Court of Justice. Surrey: Ashgate Publishing Limited, 2013.

Articles

1. Bladford, Richard, *Information Security in the Cloud,* Network Security 2011, No.4 (2011): 15-17. Doi:10.1016/s1353-4858(11)70040-x.
2. Jenna Lindqvist, *PERSONAL DATA PROTECTION ON THE INTERNET OF THINGS AN EU PERSPECTIVE, 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?,* Doctoral dissertation to be presented for public examination, by due permission of the Faculty of Law at the University of Helsinki, December 15, 2018.
3. Marioara Maxim, The Rights and Obligations of the Main Stakeholders in Cloud Computing Services, 4 Persp. Bus. L.J. 190 (2015).
4. Natālija Lazukina, *Programmatūras kā pakalpojuma nodrošināšanaslīguma normatīvais regulējums un problēmas*, Latvijas Universitāte Juridiskā Fakultāte Civiltiesisko Zinātņu Katedra, 2010.
5. Nick Pantlin, Claire Wiseman, Mariam Everett, *Supply chain arrangements: The ABC to GDPR compliance – A spotlight on emerging market practice in supplier contracts in light of the GDPR*. Harbert Smith Freehills LP, London, UK.
6. Pieter Gryffroy, *Computer and Telecommunications Law Review 2018 Legal aspects of multi-cloud: more clouds, more problems?,* Sweet & Maxwell and its Contributor. C.T.L.R. 2018.
7. Vidovic, Marina Skrinjar, *EU Data Protection Reform: Challenges for Cloud Computing*, Croatian Yearbook of European Law and Policy 12, No. 12 (2016). Doi:10.3935/cyelp.12.2016.252, P.176
8. W. Gregory Voss; Katherine H. Woodcock; Cecil Saehoon Chung; Kyoung Yeon Kim; Jai Lee; Doil Son, Privacy, E-Commerce, and Data Security, 49 Int'l Law. 97 (2015).

Electronic Sources

1. Amazon Data Processing Addendum, available on: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf. Accessed May 2, 2019.
2. Amazon Service Agreement, available on: https://aws.amazon.com/agreement/. Accessed May 2, 2019.
3. Best Software companies, available on: https://www.g2.com/best-software-companies. Accessed May 10, 2019.
4. Cisco Partner Program, available at: https://www.cisco.com/c/en/us/partners/partner-with-cisco/solution-partner-program-spp.html. Accessed May 9, 2019.
5. CSP program guide, available on: https://docs.microsoft.com/en-us/partner-center/csp-documents-and-learning-resources#cloud-solution-provider-program-guide. Accessed May 9, 2019.
6. EU Commission. *The GDPR: new opportunities, new obligations. What every business needs to know about the EU's General Data Protection Regulation*. Luxembourg: Publications Office of the European Union, 2018. on: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf. Accessed May 8, 2019.

7. Exoscale DPA, available on: https://www.exoscale.com/dpa/, Section 2. Accessed May 2, 2019.
8. Gartner on security spending, available on: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019. Accessed May 19, 2019.
9. ISO 27001 certification figures, available on: https://www.itgovernance.co.uk/blog/iso-27001-certification-figures-increase-by-20 Accessed on May 9, 2019.
10. Microservices definition, available on: https://www.ibm.com/blogs/cloud-computing/2016/05/04/what-are-microserverices/ Accessed 13 May, 2019.
11. Microsoft as a Service, available on: https://www.pcmag.com/article/346287/microsoft-as-a-service-and-the-slow-death-of-on-premises-sof. Accessed May 9, 2019.
12. Microsoft cloud agreement attestation, available on: https://docs.microsoft.com/en-us/partner-center/confirm-consent-faq. Accessed May 9, 2019.
13. Microsoft Cloud Reseller Agreement, available on: https://docs.microsoft.com/en-us/partner-center/csp-documents-and-learning-resources#cloud-solution-provider-program-guide. Accessed May 9, 2019.
14. Microsoft compliance with the GDPR. https://techcommunity.microsoft.com/t5/Microsoft-OneDrive-Blog/GDPR-Compliancy-with-OneDrive-and-SharePoint/ba-p/191126. Accessed May 19, 2019.
15. Microsoft Customer Agreement, available on: https://www.microsoft.com/licensing/docs/customeragreement. Accessed May 9, 2019.
16. Microsoft Docs, available on: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31. Accessed May 9, 2019.
17. Microsoft IT Security, available on: https://www.microsoft.com/en-mt/rethink-IT-security/gdpr.aspx. Accessed May 8, 2019.
18. Microsoft Online Terms, available on: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31. Accessed May 7, 2019.
19. Microsoft Partner Program, available at: https://azure.microsoft.com/en-us/. Accessed May 9, 2019.
20. R.J. Rosen, 'Stanford Researchers: It Is Trivially Easy to Match Metadata to Real People', The Atlantic, available on:http://www.theatlantic.com/technology/archive/2013/12/stanford-researchers-it-is-trivially-easy-to-match-metadata-to-real-people/282642/. Accessed May 7, 2019.

Other

1. Article 29 Data Protection Working Party, "Guidelines on the application and setting of administrative fines for the purposes of the GDPR".
2. Handbook on European data protection law. Luxembourg: Publication Office of the European Union, 2018.
3. Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing (01037/12/EN WP 196).
4. Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010.
5. *EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide*, Second edition, IT Governance Privacy Team, 2016, 2017.
6. Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

7. Information Commissioner's Office GDPR guidance: Contracts and liabilities between controllers and processors, available on: https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf. Accessed May 19, 2019. P. 6.

8. Information Commissioner's Office report on "Data Security Trends", available on: https://ico.org.uk/media/action-weve-taken/reports/2014675/data-security-trends-pdf.pdf. Accessed May 19, 2019.

9. Sauka A. The investment Climate in Latvia: The Viewpoint of Foregoing Investors. FICIL Sentiment Index 2015. Available on: https://www.ficil.lv/wp-content/uploads/2017/04/FICIL-Sentiment-Index-Report-2015.pdf. Accessed May 15, 2019.P.14.

10. The Principles of European Contract Law 2002. Available: https://www.trans-lex.org/400200/_/pecl/#head_4.