DOI 10.5817/MUJLT2015-1-6

OFFICE 365 V. GOOGLE APPS: A DATA PROTECTION PERSPECTIVE

by

JAN TOMÍŠEK*

This article lists the requirements of European data protection law as regards the contents of a contract between cloud provider and cloud client. Based on these requirements the contracts for the provision of Google Apps for Work and Microsoft Office 365 for small and medium enterprises are evaluated and compared from the data protection perspective. The article also discusses the shortcomings of the current legal framework for data protection with regard to cloud computing, and analyses the possible improvements made by the General Data Protection Regulation.

A cloud client usually plays the role of a data controller, while the provider may be a data controller, data processor or may not fall under the scope of data protection law. The relationship between the client and cloud provider, as a data processor, must be governed by a contract stating that the provider is bound by the instructions of the client, and describing the security measures.

The contract for Microsoft Office 365 was found to be compliant with data protection law. The contract for Google Apps for Work suffers from several deficiencies that may cause a breach of data protection law.

The current data protection framework lacks unification, clarity, scalability and balance regarding liability. With the exception of unification, the General Data Protection Regulation is not expected to bring a substantial improvement if it is adopted using the proposed wording. To cope with the problems arising from the interaction of cloud contracts with current law, cloud clients and providers may use the Cloud Service Level Agreement Standardisation Guidelines.

* Mgr. Bc. Jan Tomíšek is graduate from Faculty of Law and Faculty of Informatics, Masaryk University, Brno, Czech Republic, and junior associate at ROWAN LEGAL, Czech-based law firm focusing on ICT law. Opinions expressed in this article do not represent the opinions of ROWAN LEGAL. jantomisek@gmail.com.

KEY WORDS
Data protection, cloud, SaaS, Google Apps, Office 365, data processing agreement, DPA

1. INTRODUCTION

The concept of cloud computing is not entirely new and there is no need to introduce it to the reader at length. Cloud computing may simply be defined as a set of hosted IT services delivered on a shared internet-based platform.[1] If a cloud client operates in the European Union (EU) and the data processed using the cloud service may serve to identify any physical person, the provision of the service may fall under the regime of Directive 95/46/EC on protection of individuals with regard to the processing of personal data (DPD). The DPD sets a number of requirements on the relationship between the cloud client and the cloud provider.

Cloud solutions should bring substantial efficiency improvements in particular to small and medium enterprises (SMEs) which can neither usually afford nor fully exploit large scale dedicated IT solutions.[2] In the EU, SMEs most frequently use cloud email and data storage.[3] These services form the category of software-as-a-service (SaaS) and are often integrated in online office suites such as Microsoft Office 365 or Google Apps for Work. However, for SMEs it may be difficult to assess the products of these cloud providers from the data protection perspective since the legal regulations as well as the contractual frameworks of the providers are often very complex.

The aim of this article is, therefore, firstly to lists the requirements of the DPD regarding the contents of contracts between cloud provider and cloud client with consideration of the provisions of some national legislation. Secondly, based on these requirements, the contracts for provision of Google Apps for Work and Microsoft Office 365 to small and medium enterprises will be evaluated and compared from the data protection angle. Finally, the shortcomings of the current legal framework for data protection

---

1 KPMG, 2012, Exploring the Cloud: A Global Study of Government´s Adoption of Cloud, viewed 15 February 2015, <http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/cloud-computing/Documents/exploring-the-cloud-government-adoption.pdf>.

2 European Commission, 27 September 2012, *Unleashing the Potential of Cloud Computing in Europe*, viewed 15 February 2015, p.4. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF>.

3 eurostat, 16 January 2015, *Use of cloud computing services*, viewed 15 February 2015, <http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cicce_use&lang=en>.

with regard to cloud computing will be discussed, and possible improvements brought about by the General Data Protection Regulation will be analysed.

2. DATA PROTECTION IN THE CLOUD

The data protection obligations of the clients and providers in cloud computing strongly depend on the roles that they are assigned in any particular relationship under the DPD. If the data or a part of it may be considered to be personal data in the sense of the DPD and it is processed in the cloud then at least one of the persons must be a data controller. A data controller under the DPD is the individual that "defines the purpose and measures of the processing".[4] In the case of those cloud services that are not made-to-measure for an individual customer, it is always the cloud provider who determines the properties of the service, and the room for negotiation of individual parameters may be very limited. It may seem that these choices put the provider in the position of a data controller.[5] However, it is the decision of the cloud client to accept the offer of a particular cloud provider that determines the means of the processing;[6] therefore the client should be considered to be the controller of the personal data in question.

This, however, does not exclude the possibility of the provider being a controller too. If the provider decides to use the data for other purposes than chosen by the client, the provider may also become a data controller. This is possible where the cloud provider openly uses the data for marketing and advertising purposes (such as providing targeted advertisements to the service users), as well as in those cases where the provider exceeds the instructions of the client.[7]

In most other situations the provider will be a data processor – the person processing personal data on behalf of the controller.[8] This

---

4 Article 2 para. (d) of the Directive 95/46/EC on protection of individuals with regard to processing of personal data.

5 This possibility is discussed by Hon, KW, Millard, C, Walden, I 2012, 'Who is responsible for 'personal data' in cloud computing?—The cloud of unknowing, Part 2', *International Data Privacy Law*, 2011, vol. 2, no. 1, p. 6.

6 Article 29 Data Protection Working Party, 2012, Opinion 05/2012 on Cloud Computing (WP196), viewed 11 February 2015, p.8. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf> .

7 See Article 29 Data Protection Working Party, 2006, *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT)*, viewed 11 February 2015, p.26., <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf>.

8 WP196, supra note 6, p. 7.

assignment of roles is anticipated by Article 29 of the Data Protection Working Party (a body of European data protection authorities), as well as many individual data protection authorities, in their opinions and guidelines on the processing of personal data in the cloud.[9]

However, when the cloud provider only provides the customer with storage capacity for unstructured data (i.e. not, for example, content wise document storage with search options etc.) or computing power, the provider may not be (and usually is not) aware of the nature of the data the customer decides to process using the resources provided. Therefore, the position of the provider would change depending on what type of data the customer would decide to process without the provider's knowledge. Such an assignment of roles may result in unbalanced outcomes, encumbering both the cloud client and provider with a burden of obligations which are disproportionate to the potential risk brought by the contribution of the cloud provider to the operations of the cloud client.[10]

A solution to this problem may be the application of Directive 2000/31/EC on electronic commerce (ECD).[11] This directive creates a system of safe harbors shielding certain providers of information society services from liability. Among the shielded providers are also providers of hosting services,[12] who are not liable for information stored by the user of the service unless they have "actual knowledge of illegal activity or information."[13]

If the DPD is viewed as a general rule for all data processors, and the ECD as a special rule on liability issues which is also applicable to the treatment of personal data by hosting providers (i.e. if we would say that

---

[9] Czech Data Protection Office. 2013, *Communication of Czech Data Protection Office No. 65/2013/4*, viewed 11 February 2015, p.3., <https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3002> ,(Czech DPO Communication).

Information Commissioner's Office. 2012, *Guidance on the use of cloud computing (UK ICO Guidance)*, viewed 11 February 2015,p.8., <https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf>, (UK ICO Guidance).

Agencia Española de Protección de Datos, 2013, *Guía para clientes que contraten servicios de Cloud Computing*, viewed 11 February 2015, p. 13., <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf> ,(Spanish DPO Guidance).

[10] Hon, Millard, Walden, supra note 5, p. 11.

[11] Hon, Millard, Walden, supra note 5, p. 11.

[12] Hosting being "an information society service is provided that consists of the storage of information provided by a recipient of the service," Article 14 para. 1 of the Directive 2000/31/EC on electronic commerce.

[13] Article 14 para. 1(a) of the Directive 2000/31/EC on electronic commerce.

the personal scope of the ECD is narrower than that of the DPD), then the liability of hosting providers for the processing of personal data may be excluded.[14] However, it remains disputable as to whether all the obligations of the data processor may fall under the term 'liability'.

Nonetheless, even if we conclude that the exclusion of hosting providers from controllership under the DPD is possible, it will apply only to providers of content neutral resources such as storage or computing power.[15] In the case of Google Apps for Work, Microsoft Office 365 and similar SaaS solutions, the situation is quite different. It is obvious that data processed using these services will be sufficient to identify individual users, and this has to be considered as personal data under the DPD. Therefore, we may assume that the use of the services constitutes data processing under the DPD, with the cloud client being the data controller and the cloud provider being the data processor.

This assignment of roles sets many requirements regarding the legal relationship between the cloud provider and client. The first and most essential is the existence of a legal act governing the relationship between the cloud client as data controller and cloud provider as data processor.[16] While the DPD does not specify the type of the act, national legislation often requires it to take the form of a contract.[17] The contract (usually called a data processing agreement) should be in writing or in other equivalent forms.[18]

The DPD requires the contract to stipulate that "the processor shall act only on instructions from the controller."[19] Adherence to the principle of purpose limitation[20] is an essential obligation of the provider; the purpose of the processing should be outlined in the contract.[21] To ensure that only

[14] This opinion is also taken by Sator, G. 2013, 'Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?', in: International Data Privacy Law, vol. 3, no. 1, pp. 3-12.

[15] Most of the services would fall under the category of infrastructure-as-a-service (IaaS).

[16] Article 17 para. 3 of the Directive 95/46/EC on protection of individuals with regard to the processing of personal data..

[17] Schedule 1, part II, para. 12 of the Data Protection Act 1998 (UK Data Protection Act). Article 6 of Zákon č. 101/2000 Sb., o ochraně osobních údajů (Czech Data Protection Act). Article 12 para. 2 of Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Spanish Data Protection Act).

[18] Article 17 para. 4 of the Directive 95/46/EC on protection of individuals with regard to the processing of personal data.

[19] Article 17 para. 3 of the Directive 95/46/EC on protection of individuals with regard to the processing of personal data.

[20] Article 6 para. 1(b) of the Directive 95/46/EC on protection of individuals with regard to the processing of personal data.

[21] See Svantesson, DJB 2012, 'Data protection in cloud computing – The Swedish Perspective', *Computer Law & Security Review 28*, 2012, p. 478.

legally obtained data for a particular purpose are processed using a cloud service, the contract should state the types of personal data processed.[22]

Article 29 of the Data Protection Working Party`s opinion on cloud computing further recommends that the contract contain details on the client's instructions to be issued to the provider.[23] While the necessity of these requirements for detail has no explicit basis in the DPD, their absence may render a contract unenforceable, and, therefore, cause a conflict with Article 6 para. 3 of the DPD.

The second key obligation of the cloud provider, which must be included in a contract, is the obligation to comply with the agreed technical and organizational measures established to protect personal data.[24] The DPD does not specify the particular measures that must be implemented to protect personal data; however there are some national implementations that state specific requirements or measures aimed at various risk profiles (for example, in Spain or Poland[25]). A data processing agreement should also equip the cloud client with the tools that will enable them to supervise the provider's compliance with these measures, as well as with remedies for a situation in which the duty of compliance would be broken.[26]

The cloud provider should be obliged to provide the cloud client with sufficient proof of the provider's compliance, such as security certification or an audit report, for example ISO 27001, or a recent standard concerning the processing of personally identifiable information in the cloud – ISO 27018.

As to the remedies, cloud clients remain primarily liable for any security incident occurring in the course of the processing;[27] they should therefore be

---

[22] WP196, supra note 6, p. 13.

[23] WP196, supra note 6, p. 12. See also Svantesson, supra note 21, p. 479.

[24] Article 6 para 1 and 3 of the Directive 95/46/EC on protection of individuals with regard to the processing of personal data.

[25] An implementing directive for the Spanish Data Protection Act sets security measures for low, medium and high level of protection. Article 80 Real Decreto 1720/2007, Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Similar principle is applied by Article 6 para 2 Rozporządzenie Ministra spraw wewnętrznych i administracji Dz. U. z 2004 r. Nr 100, poz. 1024, w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

[26] WP196, supra note 6, p. 13.

[27] This is stressed by Svantesson, supra note 21, pp. 479. Similarly, imbalance in liability is seen as a main issue by McGillivray, K 2014. 'Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU', *Tulane Journal of Technology & Intellectual Property*, 17 (2014), p.248.

able to contractually transfer an appropriate part of the liability to the cloud provider, whose liability will not be limited to an extent that could almost completely let the liability rest with the cloud client. Furthermore, the cloud client should be able to terminate a data processing agreement, if they find material non-compliance with agreed measures that are not remedied by the provider in a reasonable time.

All the terms of the data processing agreement should be the result of consensus and should not be changed by a sole decision of one of the parties. Therefore, with regard to a data processing agreement, at least the basic terms of the contract regarding the instructions of the client and security measures should not be unilaterally changeable.[28]

Similarly, all the conditions stipulated in the data processing agreement must hold even if subcontractors are used by the provider. The terms of the subcontract should with regard to data protection follow the terms of the data processing agreement. The client should be informed as to all the subcontractors engaged in the processing of personal data and the contract should at least provide for prior notice of employment of the subcontractor with a sufficiently advanced notice period, as well as the right for the cloud client to terminate the contract in the event that they do not approve of the new subcontractor.[29]

The contract should ensure that the cloud provider is obliged to assist the cloud client in fulfilling requests of the subjects of the personal data processed using the service.[30] A procedure and time frame for the deletion of data following the termination of the contract should be clearly described.[31]

The last key requirement in a data processing agreement is related to the location of the processed data. Without information on data location, a cloud client cannot be sure that they comply with the requirement on the cross-border transfers of personal data. Personal data may only be

---

[28] See Svantesson, supra note 21, p. 477. Similarly, see Similarly, see Debussche, J, Van Asbroeck, B, Chloupek et al. 24 November 2014, '*Cloud computing and privacy series: the data protection legal framework,* part 2 of 6, viewed in 11 February 2015 <http://www.twobirds.com/en/news/articles/2014/global/cloud-computing-and-privacy-series-the-data-protection-legal-framework>.

[29] WP196, supra note 6, p. 11. Similarly, see Svantesson, supra note 21, p. 477, Debussche, Van Asbroeck, Chloupek et al., supra note 28, or McGillivray, supra note 27, p.246.

[30] WP196, supra note 6, p. 13. See also Svantesson, supra note 21, p. 478. Rights of data subjects are stated, namely in Articles 12, 14 and 15 of the Directive 95/46/EC on protection of individuals with regard to the processing of personal data.

[31] WP 169, supra note 6, p. 13. Article 6 para 1(e) of the Directive 95/46/EC on protection of individuals with regard to the processing of personal data.

transferred outside the EU to countries with an adequate level of protection as determined by decisions of the European Commission.[32] Data may be freely transferred to the US if the cloud provider, as a recipient of the data, is certified in a Safe Harbor program organised by the Department of Commerce, and remains certified throughout the course of the processing. To so-called third countries lacking an adequate level of protection personal data may be transferred on the condition that the parties adhere to specific Binding Corporate Rules, but the process of approval for such rules is complicated and usually too costly for SMEs.[33]

The second possible way in order to enable personal data transfer to a third country lacking an adequate level of protection is incorporation of the Standard Contractual Clauses from Commission Decision 2010/87/EU into the data processing agreement.[34] The aim of Commission Decision 2010/87/EU is to overcome the absence of adequate protection in a destination country by means of contractual safeguards. These Standard Contractual Clauses are not required to be the only clauses of the data processing agreement, but no other business related clauses included in the contract shall contradict them,[35] otherwise the established protection would not be sufficient.

There are of course many other matters that should be address in the contracts as contributing to best practice in data protection, such as notification of law enforcement access to the data or interoperability,[36] but none of these are strictly required under the DPD.

3. ANALYSIS OF CONTRACTS

3.1 GOOGLE APPS FOR WORK

The provision of Google Apps for Work to its users is governed by the Google Apps Enterprise (Online) Agreement[37] (GA Agreement) which is concluded upon registration for the services. This agreement may be further amended by accepting a Data Processing Amendment to a Google Apps

[32] Article 25 of the Directive 95/46/EC on protection of individuals with regard to the processing of personal data.

[33] McGillivray, supra note 27, p. 243.

[34] Articles 27 and 26 para 4 of the Directive 95/46/EC on protection of individuals with regard to the processing of personal data.

[35] Recital 4 of the Commission Decision 2010/87/EU.

[36] WP196, supra note 6, p. 13.

[37] Google February 2014, Google Apps Enterprise (Online) Agreement, viewed 11 February 2015, <https://www.google.com/intx/cs/work/apps/terms/2014/2/premier_terms_ie.html>.

Agreement[38] (DP Amendment) or Model contract clauses for Google Apps[39] (MCCs). However, acceptance of such additional contractual documents is voluntary and requires a specific procedure to be performed by the client at the administration console.[40] For customers located in the EU, the contract is concluded with Google Commerce Limited (Google).

On its own, the GA Agreement does not satisfy the basic requirements of a data processing agreement, since the security measures established to protect the personal data of the client are not sufficiently addressed.

Section 2.2 of the GA Agreement states for which purposes Google may process client data. Instructions of the client are sufficiently addressed in the contract.[41] However the contract does not describe what kind of data will be processed under the agreement as is recommended by Article 29 of the Working Party`s opinion on cloud computing.[42] Other details with regard to client instructions, such as the Service Level Agreement, are treated with acceptable detail in the contract.

A shortcoming of the GA Agreement is the treatment of security measures. The agreement only states that "Google will take and implement appropriate technical and organisational measures to protect Customer Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access," without any further detail. Such a general description does not satisfy the requirements of the DPD.

Google addresses this defect of the GA Agreement by offering its EU based clients the option of concluding a DP Amendment, but this option is not automatically suggested to the clients.[43] The DP Amendment overcomes some of the issues of the GA Agreement. The types of data processed are described in Appendix 1 to the GA Amendment. However, the most important improvement is the description of the implanted security

[38] Google 2015, *Data Processing Amendment to Google Apps Agreement*, viewed 11 February 2015, <https://www.google.com/intx/en/work/apps/terms/dpa_terms.html>.

[39] Google 2015, *Standard Contractual Clauses (processors)for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection*, viewed 11 February 2015, <https://www.google.com/intx/en/work/apps/terms/mcc_terms.html>.

[40] Google 2015, *Model contract clauses for Google Apps*, viewed 11 February 2015, <https://support.google.com/a/answer/2888485?hl=en>.

[41] Section 15 of the Google February 2014, Google Apps Enterprise (Online) Agreement, viewed 11 February 2015, <https://www.google.com/intx/cs/work/apps/terms/2014/2/premier_terms_ie.html>.

[42] WP196, supra note 6, p. 13. The definition of the term Customer Data is too broad in Section 15 to satisfy this requirement.

[43] For example as a part of the "Getting Started" guide displayed upon the first sign-in to the services.

measures in Appendix 2 to the DP Amendment. This description is detailed and enables the client to evaluate whether these measures are adequate for their risk profile.

With regard to the proof of actual implementation of the measures, Google pledges it will maintain ISO/IEC 27001:2005 certification or a comparable certification for the services during the term of the GA Agreement[44] and SSAE No. 16 Type II / ISAE No. 3402 report or a comparable report on logical security controls, physical security controls and system availability of the systems used for provision of the services.[45] These contractual obligations should suffice to ensure Google's compliance with security measures.

Concerning the remedies for a case of non-compliance with the security measures, the contract enables the client to terminate it on a breach.[46] In addition, a client may claim damages against Google, but Google's liability is considerably limited under the GA Agreement.[47] The limitation is not applicable to liability for "misuse of confidential information."[48] It is not clear how to interpret this exemption; however the word "misuse" rather suggests that only intentional, not negligent, conduct would be covered. The client may, therefore, bear a disproportionate portion of the liability for a breach that they are unable to prevent.

Google is entitled to unilaterally change the services, and the client is provided with no remedy for the instance that such a change negatively influences their compliance with data protection law.[49] Furthermore, Google

[44] Section 2.8 of the Google February 2014, *Google Apps Enterprise (Online) Agreement*, viewed 11 February 2015, <https://www.google.com/intx/cs/work/apps/terms/2014/2/premier_terms_ie.html>. and 6.4 of the Google 2015, *Data Processing Amendment to Google Apps Agreement*, viewed 11 February 2015, <https://www.google.com/intx/en/work/apps/terms/dpa_terms.html>.

[45] Section 2.9 of the Google February 2014, *Google Apps Enterprise (Online) Agreement*, viewed 11 February 2015, <https://www.google.com/intx/cs/work/apps/terms/2014/2/premier_terms_ie.html>. and 6.5 of the Google 2015, *Data Processing Amendment to Google Apps Agreement*, viewed 11 February 2015, <https://www.google.com/intx/en/work/apps/terms/dpa_terms.html>.

[46] Section 11.1 of the Google February 2014, *Google Apps Enterprise (Online) Agreement*, viewed 11 February 2015, <https://www.google.com/intx/cs/work/apps/terms/2014/2/premier_terms_ie.html>.

[47] Sections 13.1 and 13.2 of the Google February 2014, *Google Apps Enterprise (Online) Agreement*, viewed 11 February 2015, <https://www.google.com/intx/cs/work/apps/terms/2014/2/premier_terms_ie.html>.

[48] Section 13.1 of the Google February 2014, *Google Apps Enterprise (Online) Agreement*, viewed 11 February 2015, <https://www.google.com/intx/cs/work/apps/terms/2014/2/premier_terms_ie.html>..

[49] Section 1.2 of the Google February 2014, *Google Apps Enterprise (Online) Agreement*, viewed 11 February 2015, <https://www.google.com/intx/cs/work/apps/terms/2014/2/premier_terms_ie.html>.

may change the security measures guaranteed by Appendix 2 to the DP Amendment. Although "any such change shall not cause a material degradation in the security of the Services,"[50] there is no guarantee that the modified measures will indeed match the risk profile of the client.

As to subcontracting, the GA Agreement entitles Google to use subcontractors on the condition that such subcontracts will respect the terms of the GA agreement with regard to access to and use of a client's data. The client is entitled to request information regarding the subcontractors and their location.[51] The client may not refuse any subcontractor that is not considered to be acceptable by them from the data protection perspective.

When the service provision is terminated, Google is obliged to delete the client's data within a maximum period of 180 days.[52] Similarly, the access to, correction and deletion of the data are sufficiently addressed in the DP Amendment to enable the client to comply with any requests of data subjects.[53]

The location of the processing may vary, since Google may transfer a client's data to "the United States or any other country in which Google and its Subprocessors maintain facilities,"[54] which may potentially be any country. Hence, it must be counted on that data will be transferred to countries even without an adequate level of personal data protection. For this eventuality Google offers the client an option of entering into the MCCs containing the Standard contractual clauses issued by the European Commission; however not exercising this option does not influence the functioning of the services. Clients who do not opt for the MCCs, therefore, potentially allow illegal cross-border transfer of the personal data they control.

---

[50] Appendix 2 to the Google 2015, *Data Processing Amendment to Google Apps Agreement*, viewed 11 February 2015, <https://www.google.com/intx/en/work/apps/terms/dpa_terms.html>.

[51] Section 2.15 of the Google February 2014, *Google Apps Enterprise (Online) Agreement*, viewed 11 February 2015, <https://www.google.com/intx/cs/work/apps/terms/2014/2/premier_terms_ie.html>.

[52] Section 7.2 of the Google 2015, *Data Processing Amendment to Google Apps Agreement*, viewed 11 February 2015, <https://www.google.com/intx/en/work/apps/terms/dpa_terms.html>.t.

[53] Sections 7.1 and 8 of the Google 2015, *Data Processing Amendment to Google Apps Agreement*, viewed 11 February 2015, <https://www.google.com/intx/en/work/apps/terms/dpa_terms.html>.

[54] Section 10.1 of the Google 2015, *Data Processing Amendment to Google Apps Agreement*, viewed 11 February 2015, <https://www.google.com/intx/en/work/apps/terms/dpa_terms.html>.

The wording of the MCCs used by Google differs from that wording issued by the European Commission by the addition of an extra paragraph concerning liability to Clause 6. This paragraph no. 4 states that each party's aggregate liability under or in connection with the MCCs is limited to the amount paid to Google for the services in the previous 12 months. From the wording "without prejudice to paragraphs 1, 2 and 3 of Clause 6," it is not clear whether paragraph 4 does not limit the liability under paragraphs 1, 2 and 3, or simply does not exclude its existence while capping its height. The second interpretation would seem to be intended by Google as it follows the limitation of liability introduced into the GA Agreement.[55] However, it may be found by the data protection authorities that this limitation contradicts the previous paragraphs of the liability clause.

Another issue that may constitute a contradiction to MCCs was already discussed. The difficulty is the choice of the auditor, which is fully left to Google under the DP Amendment, while the MCCs require the auditor to be chosen "by the Data Exporter, where applicable, in agreement with the supervisory authority."[56]

3.2 MICROSOFT OFFICE 365

The basic provisions regulating the relationship are given by the Microsoft Online Subscription Agreement[57] (MOS Agreement) and Privacy Notice[58] which are agreed upon by the client when purchasing the paid version of the services. The most important document referenced by the MOS Agreement are the Online Services Terms[59] (OS Terms) which detail the terms for the provision of online services including Office 365. The MOS Agreement is concluded with Microsoft Ireland Operations Limited (Microsoft).

---

[55] Sections 13 of the Google February 2014, *Google Apps Enterprise (Online) Agreement*, viewed 11 February 2015, <https://www.google.com/intx/cs/work/apps/terms/2014/2/premier_terms_ie.html>.

[56] Clause 5(f) of the Google 2015, *Standard Contractual Clauses (processors)for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection*, viewed 11 February 2015, <https://www.google.com/intx/en/work/apps/terms/mcc_terms.html>.

[57] Microsoft 2015, *Microsoft Online Subscription Agreement*, viewed 13 February 2015 , <portal.office.com/Commerce/Mosa.aspx?cl=en&cc=en-UK> (available only upon registration for the services, no up to date and publicly available wording was found).

[58] Microsoft 2015, *Privacy Notice*, viewed 13 February 2015, <http://www.microsoft.com/online/legal/v2/?docid=18&langid=en-UK>.

[59] Microsoft 2015, *Online Services Terms January 1, 2015*, viewed 13 February 2015, <http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8248>.

The basics of the data processing agreement are regulated by the Additional European Terms Subsection of the OS Terms, which state that Microsoft is a data processor acting on their client's behalf and that it will act only upon instructions of the client. With regard to the purpose of the processing the OS Terms state that "Customer Data will be used only to provide Customer the Online Services including purposes compatible with providing those services."[60] Categories of the processed data are specified as "e-mail, documents and other data in an electronic form in the context of the Online Services."[61] The scope of the client's instructions is only given by the MOS Agreement and the OS Terms.[62]

The OS Terms describe the security measures implemented by Microsoft. The description is general but addresses a large number of areas.[63] With regard to proof of implementation, Microsoft will make available to the client its security policy compliant with ISO 27001 and 27002 standards, and have such security audited by an independent third party professional. A summary of the report resulting from the audit shall be made available to the client at their request.[64]

The MOS Agreement does not entitle the client to terminate the contract specifically for breach of Microsoft's obligation. However, even with a long term subscription, the client may terminate the services for cause with a one month termination period with the right to a refund for the remainder of the subscription.[65] Besides that, the right to terminate the contract for non-compliance with instructions of the client or Standard contractual clauses issued by the European Commission is granted by Clause 5(b) of the clauses included in Attachment 3 to the OS Terms.

---

[60] General Privacy and Security Terms Section, para. Use of Customer Data of the Microsoft 2015, *Online Services Terms January 1, 2015*, viewed 13 February 2015, <http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8248>.

[61] Appendix 1 to the Standard Contractual Clauses in Attachement 3 to the Microsoft 2015, *Online Services Terms January 1, 2015*, viewed 13 February 2015, <http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8248>.

[62] Data Processing Terms Section, Additional European Terms Subsection, para. Intent of the Parties of the Microsoft 2015, *Online Services Terms January 1, 2015*, viewed 13 February 2015, <http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8248>.

[63] Data Processing Terms Section, Security Subsection of the Microsoft 2015, *Online Services Terms January 1, 2015*, viewed 13 February 2015, <http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8248>.

[64] Data Processing Terms Section, Certifications and Audits Subsection of the Microsoft 2015, *Online Services Terms January 1, 2015*, viewed 13 February 2015, <http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8248>.

[65] Section 3 para. b(ii) of the Microsoft 2015, *Microsoft Online Subscription Agreement*, viewed 13 February 2015 , <portal.office.com/Commerce/Mosa.aspx?cl=en&cc=en-UK> (available only upon registration for the services, no up to date and publicly available wording was found).

The liability of Microsoft for damages caused by a breach of its obligations under the MOS Agreement is strictly limited[66] and liability for certain damages is excluded.[67] This limitation leaves the client a significant portion of the burden of liability with regard to the data subject.

Neither the MOS Agreement nor the OS Terms allow unilateral changes. The contract may only be changed upon expiration of its term through the due renewal procedure.[68]

By agreeing to the MOS Agreement, the client also agrees to Microsoft's use of subcontractors.[69] Each subcontract shall contain no less protective terms than the Data Processing Terms Section of the OS Terms, and Microsoft will notify the client of any new subcontractor participating in the provision of the services with at least 14 days' advance notice. The clients may terminate the services within this notice period if they do not approve the new subcontractor.[70]

Microsoft pledges to delete the client's data within 90 days from the termination of the services.[71] Microsoft is also obliged to provide the client with the ability to correct, delete or block the processed data, or make such corrections, deletions or blockages on their behalf.[72]

With regard to location of the data processing, Microsoft warrants that it will store the most sensitive part of the data of clients from the EU in that region.[73] With regard to other data Microsoft is and will remain certified for

---

[66] Sections 6 para. a and 9 of the Microsoft 2015, *Microsoft Online Subscription Agreement*, viewed 13 February 2015 , <portal.office.com/Commerce/Mosa.aspx?cl=en&cc=en-UK> (available only upon registration for the services, no up to date and publicly available wording was found).

[67] Section 6 para. b of the Microsoft 2015, *Microsoft Online Subscription Agreement*, viewed 13 February 2015 , <portal.office.com/Commerce/Mosa.aspx?cl=en&cc=en-UK> (available only upon registration for the services, no up to date and publicly available wording was found).

[68] Section 2 para. d of the Microsoft 2015, *Microsoft Online Subscription Agreement*, viewed 13 February 2015 , <portal.office.com/Commerce/Mosa.aspx?cl=en&cc=en-UK> (available only upon registration for the services, no up to date and publicly available wording was found).

[69] General Privacy and Security Terms Section, Use of Subcontractors Subsection of the Microsoft 2015, *Online Services Terms January 1, 2015*, viewed 13 February 2015, <http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8248>.

[70] Data Processing Terms Section, Privacy Subsection para. Subcontractor Transfer of the Microsoft 2015, *Online Services Terms January 1, 2015*, viewed 13 February 2015, <http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8248>.

[71] Data Retention Section of the Microsoft 2015, *Online Services Terms January 1, 2015*, viewed 13 February 2015, <http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8248>.

[72] Data Processing Terms Section, Additional European Terms Subsection, para. Customer Data Access of the Microsoft 2015, *Online Services Terms January 1, 2015*, viewed 13 February 2015, <http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8248>.

[73] Data Processing Terms Section, Location of Customer Data at Rest Subsection para. Office 365 Services of the Microsoft 2015, *Online Services Terms January 1, 2015*, viewed 13 February 2015, <http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8248>.

the Safe Harbor program, and the OS Terms include the Standard Contractual Clauses issued by the European Commission in its Attachment no. 3. The clauses are not modified in any way. As to possible contradictions with the clauses in the MOS Agreement or the OS Terms, the issue is auditing of services. The OS Terms state that the client agrees to exercise its auditing rights under the Standard Contractual Clauses by instructing Microsoft to execute the audit via a third party security professional as was described above. However, the client has the right to change this instruction.[74]

4.DISCUSSION

4.1 CONTRACTS

Altogether, Google's contractual framework for the provision of Google Apps for Work suffers from several deficiencies that may cause conflict with the DPD and corresponding national legislations. The most obvious deficiency is that a legally compliant data processing agreement is not automatically concluded with clients from the EU. Instead a specific action is required from the client, and its performance is not even actively recommended by Google.

Furthermore, the wording of the GA Agreement concerning liability is ambiguous, and the client must take into account the possibility that Google's liability under the agreement is strictly limited. Google is entitled to unilaterally change the services and the security measures established to protect personal data. The client has no right to object to Google's choice of subcontractors participating in the data processing. An ambiguous clause limiting liability is added to the MCCs and a client's right to audit under the MCCs is limited by the DP Amendment. Both of these provisions may be contradictory to the Standard Contractual Clause. Such a contradiction is not compliant with the Commission Decision 2010/87/EU.

The contract for Microsoft Office 365 also suffers from certain deficiencies, namely the strict limitation of liability that applies even to damages caused by a breach of data protection law. The period of Microsoft's notice for a new subcontractor is rather short. Also the

[74] Data Processing Terms Section, Certifications and Audits Subsection of the Microsoft 2015, *Online Services Terms January 1, 2015*, viewed 13 February 2015, <http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8248>.

regulation of audit rights in the OS Terms may potentially contradict Standard Contractual Clauses.

If the contracts for both of the services are compared from the data protection perspective, then Microsoft Office 365 performs substantially better. The most significant issue of liability limitation is not in direct breach of the data protection law, rather it only creates a misbalance in the contractual framework. On the other hand, deficiencies of the GA Agreement are considerable. They are partly remedied by the DP Amendment and the MCCs, but some of them remain unresolved. EU-based clients using Google Apps for Work are, therefore, facing a risk of breach of data protection law and subsequent sanctions from their national data protection authorities, especially if they have not opted for the DP Amendment and the MCCs.

4.2 LEGAL FRAMEWORK

From a legal perspective, cloud providers and cloud clients and especially SMEs may face several issues related to the most frequent cloud services.[75] Firstly, the differences between the national implementation of the DPD complicate the situation for the providers who may struggle to provide a unified service with terms that would be found compliant with data protection law in all EU member states.

Secondly, not all the requirements are expressly stated in the legislation and clients must therefore study the guidance issued by various authorities to ensure they meet all of them. Subsequently, a client may face difficulty when trying to identify their own obligations and subsequently assess the product of the provider.

Thirdly, in many cases, the data processed using the services will contain only a limited portion of personal data and this data will not be considered as sensitive by their subjects. In these cases, the obligations laid on the client as a data controller may be disproportionate. On the other hand, in cases where large amounts of data are processed using a cloud service, the data protection framework may lack sufficient detail to effectively regulate the relationship.[76]

Lastly, the core issue that arose from the discussion above regarding contracts is the imbalance in liability between the controller and processor.

[75] Eurostat, supra note 3.

[76] For example, with regard to the security measures that should be implemented in such case.

The current legal framework makes the cloud client, as a controller, almost solely liable for the processing, allowing the cloud provider to contractually limit their liability to a minimum.[77]

The current legal framework is, therefore, lacking with regard to unification, clarity and scalability. The General Data Protection Regulation proposed by the European Commission[78] as amended by the European Parliament[79] (GDPR) aims to address some of these challenges. One of the main ambitions of the regulation is to unify the legal framework for data protection in the EU.[80] As a regulation with direct applicability the GDPR has good chances of meeting this expectation. Furthermore, it contains provisions addressing co-operation and consistency among the independent national data protection authorities.[81] However, there are still questions that remain unresolved with regard to unification, for example the co-existence of the GDPR with national and EU-wide rules on the processing of personal data in specific sectors such as telecommunications, healthcare or financial services.[82]

On top of that, not all the duties of the data controller are stated more clearly in the GDPR in comparison to the DPD. The wording proposed by the European Commission contained an obligation of the controller to audit the effectiveness of the security measures,[83] but this obligation was removed and replaced by a more general obligation. Furthermore, the GDPR

---

[77] McGillivray comes to a similar conclusion, see McGillivray, supra note 27, p. 250.

[78] European Commission 2012, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data nd on the free movement of such data (General Data Protection Regulation)*, COM/2012/011 final, viewed 15 February 2015 , <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012PC0011&from=EN>.

[79] European Parliament 12 March 2014, *Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)'*, viewed 15 February 2015, <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN>.

[80] This is also anticipated by the European Commission. European Commission 27 September 2012, *Unleashing the Potential of Cloud Computing in Europe*, viewed 15 February 2015, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF>.

[81] Chapter VII of the European Parliament 12 March 2014, *Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)'*, viewed 15 February 2015, <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN>.

[82] See Kotschy, W 2014, ‚The proposal for a new General Data Protection Regulation—problems solved?', *International Data Privacy Law*, 2014, vol. 4, no. 4, pp. 276 or Blume, P 2014, 'The myths pertaining to the proposed General Data Protection Regulation', *International Data Privacy Law*, 2014, vol. 4, no. 4, pp. 269-273.

mandates the European Commission to issue numerous by-laws and implementing acts creating potentially unclear borders between binding and non-binding rules. Whether the GDPR will clarify the obligations of clients and providers in cloud computing is therefore at least questionable.

As a positive aspect it must be highlighted that the GDPR clearly states that it does not limit the application of the ECD and, therefore, exempts providers of IaaS cloud services from the scope of certain data protection obligations.[84] Also the extended obligations of the processor with regard to documentation, co-operation with data protection authorities, security measures, impact assessment and compliance reviews may be perceived as an improvement.[85] Additionally, the concept of processing sectors that may be declared as areas with an adequate level of protection may facilitate international data transfers in cloud computing.[86] The GDPR also tackles the issue of subcontracting, but the currently proposed wording is very general.[87] Despite these improvements in flexibility and assignment of liability, much more could be done. Instead of merging the roles of processor and controller in one responsible subject with scaled obligations and liability, the GDPR follows the original dichotomy introduced by the DPD. Furthermore, the GDPR does not contain a true de minimis clause that would exempt small scale, low-risk processing from its scope. The size of the processing simply influences the less important obligations of the controller[88] and additional obligations of the controller are added.[89] With

---

[83] Article 22 para 3 of the European Parliament 12 March 2014, *Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)'*, viewed 15 February 2015, <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN>.

[84] Article 3 para 3 of the Article 22 para 3 of the European Parliament 12 March 2014, *Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)'*, viewed 15 February 2015, <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN>. See Sartor, supra note 14.

[85] Articles 28, 29, 30, 33 and 33a of the GDPR, supra note 78, as amended by the European Parliament. See also Blume, P 2015, 'It Is Time for Tomorrow: EU Data Protection Reform and the Internet', *Journal Of Internet Law*, vol. 18, no. 8, p. 7.

[86] Article 41 of the GDPR, supra note 78. See also Blume, P. 2015, supra note 88, p. 9.

[87] Article 26 para. 2(d) of the GDPR, supra note 78, as amended by the European Parliament. The original wording proposed by the Commission was more strict and less ambiguous. See also McGillivray, supra note 27, p. 248.

[88] Such as the appointment of a data protection officer. Article 35 para 1(b) of the GDPR, supra note 78.

[89] Reding, V 2012, 'The European data protection framework for the twenty-first century', *International Data Privacy Law*, vol. 2, no. 3, pp. 119-129.

regard to liability, the processor still does not share primary liability for security and compliance with the controller regarding the processing in its entirety.[90]

In short, with regard to the improvements in cloud computing expected from the GDPR, these will probably not be brought about by adoption of the currently proposed text. Its future reviews should therefore focus on clarification, simplification, scaling and balancing liability.

Nevertheless, whether the GDPR should be beneficial to cloud clients and providers or not, it will not come into force in the close future, nor for that matter will any other amendment to the DPD. Therefore, cloud clients have to find solutions as to how to effectively assess the offers of cloud providers and ensure compliance of the offered processing with the DPD. With regard to this challenge, the European Commission established the Cloud Select Industry Group and its subgroup aimed at service level agreement standardisation. This subgroup issued Cloud Service Level Agreement Standardisation Guidelines.[91]

The guidelines are built around the concept of service level objectives which also cover data protection issues. The coverage is detailed and reflects the recommendations of Article 29 of the Data Protection Working Party. The relevant service level objectives include certification, purpose specification, data minimization, retention and disclosure limitation, transparency and notice, accountability, data location and handling of data subjects' requests. Besides this, specific service level objectives for security are also included, such as authentication and authorization, cryptography, security incident management, logging and monitoring, auditing and security verification. The guidelines also address performance and data management. For each service level objective the guidelines provide its context, the explanation why it is needed and a description of how it should be addressed in an agreement. According to the experience of the author, the guidelines are very useful in both assessing and drafting data processing agreements for cloud computing.

---

[90] The processor is not included in Article 22 para. 1 of the GDPR, supra note 78. See also Blume, P 2015, supra note 88, p. 7. However, McGillivray argues that not all liability should be transferred to the processor, see McGillivray, supra note 27, p. 248.

[91] Cloud Select Industry Group – Subgroup on Service Level Agreement 24 June 2014, *Cloud Service Level Agreement Standardisation Guidelines*, viewed 15 February 2015, <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6138>.

5. CONCLUSION

Provision of cloud services to clients based in the EU may often fall under the scope of European data protection law represented by the DPD. Cloud clients and providers may be assigned different roles under the DPD according to the nature of the processing. The client is in most cases a data controller. The provider may be also a data controller if they process the personal data for their own purposes, such as advertising, or a data processor if they only act on the instructions of the client. They may also not fall under the scope of the DPD if they qualify as a hosting provider under the ECD, by not being aware of the nature of the data processed using their service.

In cases where the cloud provider is a data processor, such as with the SaaS solutions where it is obvious from the design of the service that personal data will be processed, the relationship between the cloud provider and the cloud client must be governed by a contract. This contract must state that the provider is bound by the instructions of the client, must describe the scope of the client's instructions and the purpose of the processing and types of data processed. Furthermore the contract must describe security measures, the methods of proving provider's compliance with these measures and remedies for a case of their non-compliance. The contract must not allow for unilateral changes to material provisions and must regulate the use of subcontractors by the provider. If the data is to be processed outside the EU and countries with adequate level of protection, the provider must be Safe Harbor certified for the USA, and for other countries the contract must contain the Standard Contractual Clauses issued by the European Commission.

The contractual framework for the provision of Microsoft Office 365 seems to be compliant with the above listed requirements except for minor deficiencies and an imbalance in liability. The contractual structure for the provision of Google Apps for Work suffers from more severe deficiencies that may render it non-compliant with the national data protection laws of EU member states. To ensure at least a minimal level of compliance, additional operations of the client are required. Google also strongly limits the right of the client to audit, as well as its own liability towards the client. The contract also enables unilateral changes of its essential provisions by Google.

The current legal framework for data protection in the provision of cloud services lacks unification, clarity and scalability. With exception to unification, the GDPR is not expected to bring about a substantial improvement if it is adopted with the current wording.

To cope with the problems arising from the interaction of cloud contracts with current European data protection law as represented by the DPD, cloud clients and providers may use Cloud Service Level Agreement Standardisation Guidelines to draft and assess data processing agreements.

LIST OF REFERENCES

Directive 2000/31/EC on electronic commerce.

Directive 95/46/EC on protection of individuals with regard to processing of personal data.

Commission Decision 2010/87/EU.

Data Protection Act 1998 (UK Data Protections Act).

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Spanish Data Protection Act).

Real Decreto 1720/2007, Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (Implementing directive for the Spanish Data Protection Act).

Rozporządzenie Ministra spraw wewnętrznych i administracji Dz. U. z 2004 r. Nr 100, poz. 1024, w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Implementing directive for the Polish Data Protection Act).

Zákon č. 101/2000 Sb., o ochraně osobních údajů (Czech Data Protection Act).

Agencia Española de Protección de Datos, 2013 [accessed 2015-02-11], 'Guía para clientes que contraten servicios de Cloud Computing', retrieved

from http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf (Spanish DPO Guidance), p. 13.

Article 29 Data Protection Working Party, 2012, Opinion 05/2012 on Cloud Computing (WP196), viewed 11 February 2015, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion- ecommendation/files/2012/wp196_en.pdf>

Article 29 Data Protection Working Party, 2006, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT), viewed 11 February 2015 p.26., <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf>.

Blume, P 2015, 'It Is Time for Tomorrow: EU Data Protection Reform and the Internet', *Journal Of Internet Law*, vol. 18, no. 8, pp. 3-13.

Blume, P. 2014, 'The myths pertaining to the proposed General Data Protection Regulation', *International Data Privacy Law*, 2014, vol. 4, no. 4, pp. 269-273.

Cloud Select Industry Group – Subgroup on Service Level Agreement 24 June 2014, Cloud Service Level Agreement Standardisation Guidelines, viewed 15 February 2015, <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6138>.

Czech Data Protection Office. 2013, Communication of Czech Data Protection Office No. 65/2013/4, viewed 11 February 2015, <https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3002, (Czech DPO Communication)>.

Debussche, J, Van Asbroeck, B, Chloupek et al. 24 November 2014, 'Cloud computing and privacy series: the data protection legal framework, part 2 of 6, viewed in 11 February 2015 <http://www.twobirds.com/en/news/articles/2014/global/cloud-computing-and-privacy-series-the-data-protection-legal-framework>.

European Commission 2012, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data nd on the free movement of such data (General Data Protection Regulation), COM/2012/011 final, viewed 15 February 2015 , <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012PC0011&from=EN>.

European Commission 27 September 2012, Unleashing the Potential of Cloud Computing in Europe, viewed 15 February 2015, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF>.

European Parliament 12 March 2014, Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)', viewed 15 February 2015, <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN>.

Eurostat, 16 January 2015, Use of cloud computing services, viewed 15 February 2015, <http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cicce_use&lang=en>.

Google 2015, Data Processing Amendment to Google Apps Agreement, viewed 11 February 2015, <https://www.google.com/intx/en/work/apps/terms/dpa_terms.html>.

Google 2015, Model contract clauses for Google Apps, viewed 11 February 2015, <https://support.google.com/a/answer/2888485?hl=en>.

Google 2015, Standard Contractual Clauses (processors)for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, viewed 11 February 2015, <https://www.google.com/intx/en/work/apps/terms/mcc_terms.html>.

Google February 2014, Google Apps Enterprise (Online) Agreement, viewed 11 February 2015, <https://www.google.com/intx/cs/work/apps/terms/2014/2/premier_terms_ie.html>.

Hon, KW, Millard, C, Walden, I 2012, 'Who is responsible for 'personal data' in cloud computing?—The cloud of unknowing, Part 2', *International Data Privacy Law*, 2011, vol. 2, no. 1, pp. 3-18.

Information Commissioner's Office. 2012, Guidance on the use of cloud computing (UK ICO Guidance), viewed 11 February 2015,p.8., <https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf> (UK ICO Guidance)

Kotschy, W 2014, ,The proposal for a new General Data Protection Regulation—problems solved?', *International Data Privacy Law*, 2014, vol. 4, no. 4, pp. 274-281.

KPMG, 2012, Exploring the Cloud: A Global Study of Government´s Adoption of Cloud, viewed 15 February 2015,

<http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/cloud-computing/Documents/exploring-the-cloud-government-adoption.pdf>.

McGillivray, K 2014. 'Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU', *Tulane Journal of Technology & Intellectual Property*, 17 (2014), pp.217–253.

Microsoft 2015, Microsoft Online Subscription Agreement, viewed 13 February 2015 , <portal.office.com/Commerce/Mosa.aspx?cl=en&cc=en-UK> (available only upon registration for the services, no up to date and publicly available wording was found).

Microsoft 2015, Online Services Terms January 1, 2015, viewed 13 February 2015, <http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8248>.

Microsoft 2015, Privacy Notice, viewed 13 February 2015, <http://www.microsoft.com/online/legal/v2/?docid=18&langid=en-UK>.

Reding, V 2012, 'The European data protection framework for the twenty-first century', *International Data Privacy Law*, vol. 2, no. 3, pp. 119-129.

Sator, G 2013, 'Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?', *International Data Privacy Law*, vol. 3, no. 1, pp. 3-12.

Svantesson, DJB 2012, 'Data protection in cloud computing – The Swedish Perspective',in: Computer Law & Security Review 28, 2012, pp. 476-480.