http://dx.doi.org/10.12697/JI.2016.24.03

Liliia Oprysk
Doctoral student
University of Tartu

The Forthcoming General Data Protection Regulation in the EU

Higher Compliance Costs Might Slow Down Small and Medium-sized Enterprises' Adoption of Infrastructure as a Service[*1]

1. Introduction

Infrastructure as a Service (IaaS) accounts for a significant proportion of cloud computing services overall, and, according to Gartner, in 2014 'the absolute growth of public cloud IaaS workloads surpassed the growth of on-premises workloads for the first time'[*2]. A recent report from RightScale[*3] showed that 95% of the organisations surveyed were already using or experimenting with IaaS[*4], with 89% of respondents using public cloud services[*5]. Moreover, 32% of small and medium-sized businesses (enterprises with fewer than 1,000 employees for the purpose of the report) were already using cloud infrastructure heavily at that time, as compared to 25% of enterprises in general[*6].

The widespread adoption of cloud-based technologies among these companies does not come as a surprise: small and medium-sized enterprises are more likely to seek a less expensive option for maintaining their IT infrastructure and to have a smaller budget at their disposal. Neither is their interest in IaaS, which is usually the first step in adoption of cloud-based solutions, as it requires less preparation and integration than do Platform as a Service (PaaS) and Software as a Service (SaaS) options. Indeed, IaaS provides several benefits when compared to traditional computing infrastructure provision[*7]. Nevertheless, it has to be noted that the resources a client acquires under IaaS are pretty much the same ones it can obtain from a traditional IT outsourcing (ITO) provider. Aspects that differ are the process of obtaining and expanding the resources; the nature of business relations between the parties; and, finally, the contractual arrangements.

1 The author would like to thank Dr Idir Laurent Khiar, Dr Elia Ambrosio, Prof. Karin Sein, Prof. Aleksei Kelli, and Prof. Katrin Nyman-Metcalf for their feedback that contributed to improving the text of the article.

2 Gartner says worldwide cloud infrastructure-as-a-service spending to grow 32.8% in 2015. 18.5.2015. Available at http://www.gartner.com/newsroom/id/3055225 (most recently accessed on 4.7.2016).

3 RightScale is one of the leading providers of cloud management solutions, conducting an annual survey of technical professionals to assess the state of the cloud computing market.

4 RightScale State of the Cloud Report 2016. Available at https://www.rightscale.com/lp/state-of-the-cloud (most recently accessed on 4.7.2016), p. 2.

5 *Ibid*., p. 9.

6 *Ibid*., p. 7.

7 S. Leimeister, M. Böhm, C. Riedl, H. Krcmar. The business perspective of cloud computing: Actors, roles, and value networks. ECIS 2010 Proceedings. Available at http://home.in.tum.de/~riedlc/res/LeimeisterEtAl2010-preprint.pdf (most recently accessed on 4.7.2016), p. 7.

A few years ago, the European Commission (EC) recognised the potential of cloud computing and certain advantages of promoting its adoption within the EU. Small and medium-sized enterprises[*8] (SMEs) have often been given the focus in the EC's efforts to promote competitiveness of European businesses. The aim with the first comprehensive cloud computing strategy[*9], calling for unleashing the potential of cloud computing in Europe, was to address the factors hindering businesses, especially SMEs, from adopting cloud services. In its turn, the Horizon 2020 programme[*10] includes cloud computing on its list of priority areas each year. The Work Programme for 2016–2017[*11], for example, is intended to foster competitive, innovative, and reliable cloud computing for small and medium-sized enterprises and for public institutions.

These extensive efforts on the part of the EC notwithstanding, adoption of cloud-based solutions is not a clear-cut choice for a business. Compliance is listed among the top three challenges for clients adopting cloud-based solutions[*12] and is unlikely to disappear from the list. Aside from there being the issues of compliance related to operation in a heavily regulated industry (alongside finance, health care, etc.), there is the matter of data protection compliance, which is becoming highly topical in light of the recent adoption of the General Data Protection Regulation[*13] (GDPR). As a fair percentage of businesses process personal data of their customers in one or another way and offer their services in the EU, it is highly likely that numerous individual SMEs are going to have to comply with the data protection legislation in the EU.

This article provides an overview of the changes wrought in the data protection legislation by the GDPR and discusses how the reform might reshape the data protection compliance requirements for SMEs using IaaS to process personal data. In particular, the article addresses the questions of whether SMEs will still opt for IaaS under the new regulation and whether the GDPR interferes with one of the other EC goals – wider adoption of cloud computing by SMEs. The author uses qualitative methods to analyse the provisions of the GDPR, identify which of them are going to influence the data protection compliance of SMEs using IaaS, and establish whether the reform will impede achievement of wider cloud adoption.

2. Infrastructure as a Service as a cloud service model

Infrastructure as a Service is one of several cloud service models. In this approach, the cloud provider supplies basic computer resources (processing power, storage, routers, etc.) on which clients can run software. The cloud provider owns the infrastructure (or hires it from a third party) and maintains it, while the customer pays for it on a pay-as-you-go basis. It is worth noting at this juncture that, while some scholars use alternative terms for this particular cloud service model[*14], 'IaaS' is a widely used term throughout the IT industry[*15].

8 SMEs are enterprises that 'employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million', according to Article 2 of the Annex to the Commission Recommendation on the definition of micro, small, and medium-sized enterprises, 6.5.2003, C(2003) 1422.

9 Unleashing the potential of cloud computing in Europe. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 27.9.2012, COM(2012) 529. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF (most recently accessed on 4.7.2016).

10 The EU Framework Programme for Research and Innovation, a financial instrument to drive economic growth and create jobs. For more information, see https://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020 (most recently accessed on 4.7.2016).

11 Horizon 2020 Work Programme 2016–2017, 5i. Information and communication technologies, 2015. Available at http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-leit-ict_en.pdf (most recently accessed on 4.7.2016).

12 RightScale State of the Cloud Report 2016 (see Note 4), p. 20.

13 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.

14 See M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia. Above the clouds: A Berkeley view of cloud computing. Technical report, EECS Department, University of California at Berkeley, 2009, p 3; L. Wang, J. Tao, M. Kunze, A. C. Castellanos, D. Kramer, W. Karl. Scientific cloud computing: Early definition and experience. 10th IEEE International Conference on HPCC, 2008, p. 3; L. Youseff, M. Butrico, D. Da Silva. Toward a unified ontology of cloud computing. Grid Computing Environments Workshop, 2008, p. 3.

15 The most widely used definition is the one by the National Institute of Standards and Technology (NIST). See P. Mell, T. Grance. The NIST definition of cloud computing. National Institute of Standards and Technology, Information Technology Laboratory, 2011. Available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (most recently accessed on 4.7.2016), p. 3.

Some examples of IaaS are Amazon's Simple Storage Service (S3)[*16] and Elastic Compute Cloud (EC2)[*17], which was a pioneer in the field and leads the way in IaaS public-cloud operations[*18], with a share of about half of the market[*19].

Since, after all, cloud computing is a result of IT outsourcing's evolution,[*20] IaaS is just an alternative way to obtain infrastructure resources by outsourcing its provision to an external provider. There are a few clear benefits to cloud services, with the most significant of these for a business being the absence of substantial up-front investments. With IaaS, clients get infrastructure resources without negotiating complex outsourcing agreements or engaging in time-consuming negotiations every time they find themselves in need of additional resources. Consequently, what constitutes the difference between IaaS and the traditional outsourcing option is not the resource itself but the way of delivering it, along with the cost and effort necessary to obtain and maintain it.

Companies using traditional ITO services happily adopt IaaS in accordance with their needs. A PwC survey showed that 22% of ITO customers used a public cloud in 2011.[*21] However, the percentage using an external or internal private[*22] cloud was substantially higher.[*23] Despite the many benefits of IaaS, companies using traditional ITO services will not automatically want to switch to IaaS. There are a few reasons for which a company may want to stick with ITO, but this article goes into only one of these – compliance with the EU data protection rules.

Increasing adoption of cloud computing encourages traditional ITO providers to enter the cloud computing market. The competitiveness of a particular provider in the market is influenced not only by specific characteristics of its service but also by that provider's ability to meet clients' expectations and flexibility in satisfying clients' compliance needs. Consequently, changes that complicate specific vendors' ability to meet data protection compliance requirements may reshape the market as a whole.

3. SMEs and external service providers under the legislation currently in force

The data protection legislation currently in force, the Data Protection Directive[*24], protects the rights of persons whose personal data are being processed. It does so by defining roles and obligations of the parties involved in the processing. The specific roles involved are data controller and data processor, where the former is defined as determining the purposes and means of the processing[*25] and the latter as processing personal data on behalf of the controller[*26]. The data controller has a variety of obligations with regard to personal data and ability to allocate responsibilities to third parties[*27]. The data processor, on the other hand, does not have specific obligations except to act only upon instructions from the controller;[*28] to ensure fair

16 Amazon Webservices launches. Amazon, 14.3.2006. Available at http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=830816 (most recently accessed on 4.7.2016).

17 J. Barr. Amazon EC2 Beta. Amazon, 25.8.2006. Available at https://aws.amazon.com/blogs/aws/amazon_ec2_beta/ (most recently accessed on 4.7.2016).

18 The term 'public cloud' is used to refer to a model wherein resources can be purchased by any potential client; i.e., the service is publicly available.

19 RightScale State of the Cloud Report 2016 (see Note 4), p. 31.

20 O. Yigitbasioglu, K. Mackenzie, R. Low. Cloud computing: How does it differ from IT outsourcing and what are the implications for practice and research? – *The International Journal of Digital Accounting Research* 2013 (13), p. 102.

21 The future of IT outsourcing and cloud computing: A PwC study. 2011. Available at https://www.pwcaccelerator.com//pwcsaccelerator/docs/future-it-outsourcing-cloud-computing.pdf (most recently accessed on 4.7.2016), p. 29.

22 A private cloud is built for use by a single client. It may be managed by an external service provider (as an 'external cloud') or operate on the premises of a client (in what is called an internal cloud).

23 Roughly 41% of respondents used an external private cloud, and 31% of them used an internal private cloud. See Note 21.

24 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 1995, No. 281, 23.11.1995.

25 *Ibid*., Article 2 (d).

26 *Ibid*., Article 2 (e).

27 Opinion 1/2010 on the concepts of 'controller' and 'processor'. Article 29 Working Party, WP 169, 00264/10/EN, Brussels, 16 February 2010, p. 4.

28 Directive 95/46/EC (see Note 24), Article 17 (2).

and lawful processing of data, compatible with specific purposes[*29]; and to implement appropriate technical and organisational measures to protect personal data against threats[*30].

SMEs collecting personal data of their customers and processing said data for a specific purpose in the course of their business are data controllers within the meaning of the Directive and will have to comply with the relevant provisions. As long as SMEs process the data themselves without involving third parties, they will retain sole responsibility for the compliance with the EU data protection rules. However, if SMEs delegate the processing to an external party or use third-party infrastructure to process the data, the external provider becomes a data processor and, in turn, influences the controller's data protection compliance. Consequently, SMEs' data protection compliance is affected by whether they process data themselves via the infrastructure they own or rent or instead outsource the whole process or particular stages of it to an external party.

While there is no doubt that SMEs in those circumstances are data controllers, the question of whether an external provider automatically becomes a data processor is problematic. External providers can be involved in the processing in a number of ways, but should every provider of infrastructure resources be deemed a data processor? In essence, should an IaaS provider supplying merely means of processing and without actual knowledge of the data be considered equal to an ITO provider carrying out certain stages of processing in full awareness of the nature of the data?

Assigning the data processor role to a cloud service provider has, accordingly, been questioned and debated. Nonetheless, the Article 29 Working Party[*31] declared that a cloud computing provider becomes a data processor by providing the data controller with the means and the platform for the processing of personal data.[*32] Hence, whether SMEs obtain infrastructure resources from an ITO provider or instead use IaaS, the external provider will be regarded as a data processor. It is of great relevance that entrusting a third party with provision of underlying infrastructure influences SMEs' compliance, specifically the obligations of a controller related to the performance of the data processor.

Firstly, the controller has to choose a processor that provides sufficient guarantees in respect of the technical security and organisational measures governing the processing of data and must ensure that processor's compliance.[*33] Whilst in the process of choosing between IaaS and a traditional outsourcing service or even between individual IaaS vendors SMEs certainly take into account the technical specifications and security features of each service, closer analysis or inspection may not be possible in the case of IaaS. The nature of public IaaS and cloud-based services in general does not afford or entail much integration or co-operation between the parties; rather, it takes a form in which a service provider supplies ready tools available for use by the client for whatever purposes. Reaching the legally prescribed goal is problematic unless the IaaS provider makes the service available for examination.

Secondly, there must be a legally binding contract between controller and processor, under which the obligation to ensure appropriate technical and organisational measures to protect the data must be binding for the processor too.[*34] The obligation to conclude a binding agreement serves the purpose of providing the data controller with complete control over the processing of personal data and eases ensuring of data protection compliance. While ITO agreements serve this purpose – to define the relationship between the parties and meet their expectation[*35] – IaaS is different in this respect. Cloud service providers supply cloud services on the basis of terms of service[*36] specified on a Web page, which in most cases are decided upon unilaterally (especially with public IaaS) and do not provide assurance that the service to be delivered suits the client's purposes. While large enterprises might have the bargaining power to negotiate a tailored contract as IaaS clients, the same certainly is not true for SMEs.

29 *Ibid*., Article 6 (1b).

30 *Ibid*., Article 17.

31 The Article 29 Working Party was set up in accordance with Article 29 of the Data Protection Directive to provide, *inter alia*, advice on uniform application of the Data Protection Directive.

32 Opinion 05/2012 on Cloud Computing. Article 29 Working Party, WP 196, 01037/12/EN, Brussels, 1 July 2012, p. 4.

33 Directive 95/46/EC (see Note 24), Article 17 (2).

34 *Ibid*., Article 17 (3).

35 A. Kavaleff. Successful outsourcing through proactive contracting – strategy, risk assessment and implementation. – *Scandinavian Studies in Law* 2006/49, p. 222.

36 'Terms of service', 'terms and conditions', and also 'terms of use' are common names that providers of online services use to refer to an agreement governing usage of their service. The author uses 'terms of service' to refer to agreements of this type.

Therefore, even with the legislation currently in place, opting for a traditional ITO service (provision of the infrastructure, owned and managed by the provider on the SME's premises or in a remote location) will be beneficial in terms of SMEs' compliance with the data protection rules. The outsourcing provider still becomes a processor of personal data; however, SMEs will have a lot more control over the process, by negotiating an agreement and meeting their compliance needs. On the other hand, this will require more effort in the stage of entering into a contract and maintaining it, so the agreement will come at a higher transaction cost.

4. Forthcoming changes and challenges for data protection compliance

The forthcoming changes to the data protection framework, in the form of the recently adopted General Data Protection Regulation[*37], do not provide a completely new system to protect the interests of data subjects whose personal data are being processed. These changes are, however, going to influence the cloud computing industry in general and SMEs obtaining cloud services in particular. Although the roles associated with the processing of personal data remain the same, obligations will be substantially widened, especially those of a data processor.

The data processor will now be obliged not to engage other processors in the processing of data without prior specific or written consent from the data controller.[*38] On the data controller's side, it will be difficult to ensure meeting of this requirement in the context of IaaS, as the nature of cloud computing services is geared fundamentally toward service composed of elements delivered by various vendors. In the likely event of planning to switch vendor or approach new vendors, cloud service providers are unlikely to inform their clients in advance or, even more improbable, to obtain consent for doing so. In addition, another obligation of the data processor – to maintain a record of all the data processing activities[*39] – might be difficult to fulfil in the context of cloud agreements. It requires adoption of additional organisational and technical measures. These measures have to be negotiated in each and every case or, alternatively, be part of functionality built into the service itself. Once again, the cost of entering into agreement is going to increase.

The obligation to notify the controller of any personal-data breach without undue delay[*40] will result in additional substantial changes. Unlike with ITO services wherein the provider actively reports to the clients, the burden of detecting and communicating violations of the service level agreement[*41] (SLA) in IaaS usually rests with the client[*42] and not the provider. Currently, SMEs not only have to monitor availability of the cloud service but also must report any violations of the SLA in time if they are to receive compensation.[*43] Therefore, this obligation requires considerable changes in the respective SLAs.

Perhaps the most problematic aspect of the GDPR for SMEs using IaaS is that a contract between controller and processor will have to stipulate the nature and the purpose of the processing of personal data, categories of data subjects, etc.[*44] This is customary in outsourcing agreements, wherein the provider and client typically seek long and lasting partnership and share more information on the nature of the activities to be performed, so as to meet the objectives of the outsourcing better. However, in the absence of a specific connection between a public IaaS provider and its client, it is unlikely that the client will be willing to share such information; that the provider will be interested in it; and, finally, that doing so is absolutely necessary. Hence, standard IaaS contracts will have to be modified, just as SLAs will. At present, the practice is

37 The GDPR (see Note 13).

38 *Ibid*., Article 28 (2).

39 *Ibid*., Article 30.

40 *Ibid*., Article 33 (2).

41 A service level agreement is an agreement between a service provider and a client stipulating concrete metrics according to which service has to be delivered and evaluated. These agreements are widely used within the IT industry.

42 S. Baset. Cloud SLAs: Present and future. – *CM SIGOPS Operating Systems Review* 2012 (46) / 2, p. 63. – DOI: http://dx.doi.org/10.1145/2331576.2331586

43 For example, Amazon's EC2 SLA states that any claim has to be submitted in accordance with a sample form and include logs supporting the claimed outage before the end of the second billing cycle from when the incident occurred. Amazon EC2 Service Level Agreement, 2013. Available at http://aws.amazon.com/ec2/sla (most recently accessed on 4.7.2016).

44 The GDPR (see Note 13, Article 28 (3).

slightly different, to put it mildly. In 2010, 31 cloud services, offered by 27 cloud providers, were subjects in a study of terms of service[*45]. The results, while somehow expected, were still surprising: 18 agreements had been modified during the previous half-year period and the change was reported (the last revision date was available), 28 agreements remained unchanged and there was notification of this fact, a further 19 were unchanged without that being reported (no revision date was available), and four agreements had been changed without notification.[*46]

In light of what is stated above, it becomes apparent that, to comply with the GDPR, SMEs will need to invest more in IaaS in the stage of negotiations and entering into an agreement than before. The business model behind IaaS provides a cost-saving approach by eliminating costs associated with infrastructure maintenance and entering into a contract, thereby enabling clients to access and expand the resources without undue delay. In consequence, the current advantages of IaaS over traditional ITO will be diminished by the upcoming changes.

Setting aside the fact that, because of differences in bargaining power, it could well be problematic to force an IaaS provider to negotiate all the terms, we can see that compliance will also substantially increase transaction costs[*47]. Various hidden costs have been attributed to IT outsourcing in the past[*48]; however, these will become a reality for cloud computing services too. Companies consider cloud computing to be a way to reduce transaction costs[*49]; therefore, increases in these costs will also influence SMEs' intention to adopt cloud computing[*50].

Ironically, the GDPR excludes SMEs from the application of the data portability right, as it serves solely the data subjects[*51]. The wording of the relevant clause allows only the data subject to receive the data in a widely used format and does not grant the SME (as a data controller and not the subject) the right to request the same from the data processor. In the case of SMEs using IaaS, the SME would be obliged to provide the data to its clients (data subjects) in a widely used format while the IaaS provider would have no obligations whatsoever to the SME in this regard.

This is by no means an exhaustive list of the changes that will directly influence relations between SMEs and IaaS providers. The upcoming reform threatens cloud service as such or, more precisely, its provision by cloud providers established in the EU or offering services to European customers[*52]. Even if cloud providers proactively adapt to the forthcoming changes, opting for a cloud service will not be as beneficial as it was before, so whether SMEs would still consider IaaS an option at the end of the day is questionable. In the absence of clear indications of readiness to adapt, the scale of the impact remains to be seen.

45 S. Bradshaw, C. Millard, I. Walden. Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services. – *International Journal of Law and Information Technology* 2011 (19) / 3, pp. 187–223.

46 *Ibid*., pp. 215–216.

47 The cost associated with exchange of the goods or services between the parties. For more on the transaction-cost approach, see O. Williamson. The economics of organization: The transaction cost approach. – *The American Journal of Sociology* 1981 (87) / 3, pp. 548–577. – DOI: http://dx.doi.org/10.1086/227496.

48 For discussion of vendor search, contract, transition, and management costs, see J. Barthélemy. The hidden costs of IT outsourcing. – *MIT Sloan Management Review* 2001 (42) / 3, p. 61.

49 G. Garrison, S. Kim, R. Wakefield. Success factors for deploying cloud computing. – *Communications of the ACM* 2012 (55) / 9, pp. 62–68. – DOI: http://dx.doi.org/10.1145/2330667.2330685.

50 H. Hamilton. An examination of service level agreement attributes that influence cloud computing adoption. Doctoral dissertation for Nova Southeastern University, 2015. Available at http://nsuworks.nova.edu/gscis_etd/53 (most recently accessed on 4.7.2016), p. 90.

51 The GDPR (see Note 13, Article 20).

52 Processing of personal data is subject to the GDPR if the controller or processor is established in the EU or offers services to data subjects in the EU or monitors their behaviour. See Article 3 of the GDPR.

5. European Commission initiatives aimed at fostering cloud computing

On the other hand, wider adoption of cloud computing by SMEs is an objective set by the European Commission in the context of its Digital Single Market Strategy*[53]. A number of European Commission initiatives have looked specifically at the contractual aspect of relations between clients and cloud providers. Three of them are of particular relevance for SMEs' compliance with data protection legislation: The Data Protection Code of Conduct for Cloud Computing, the Cloud Service Level Agreement Standardisation Guidelines, and the Report on Standards Terms and Performance Criteria in Service Level Agreements for Cloud Computing Services.

In early 2015, the Cloud Select Industry Group (C-SIG) presented the first draft of the Data Protection Code of Conduct*[54], which is a voluntary instrument for cloud service providers' use in proactively demonstrating their compliance with the data protection principles, via adherence to the code by either self-evaluation or a third-party audit. Notwithstanding its potential, it faced criticism from the Article 29 Working Party*[55] for failure to acknowledge the forthcoming changes, to clarify the notion of personal data, and to prevent terms of service that favour the service provider. When updated in response to the concerns raised, the code can become an instrument that cloud providers would rely on to attract SMEs as IaaS clients. However, the balance has to be maintained in order for the code to remain appealing for adherence, since indicating support for it does not automatically mean compliance. Rather, it indicates recognition of clients' demands.

C-SIG also presented the Cloud Service Level Agreement Standardisation Guidelines*[56], which cover B2B relations (relations between service providers and clients who are not consumers). The aim with these guidelines was to contribute to the development of relevant ISO standards and to list basic principles to be borne in mind in drafting of SLAs for cloud services. Among other things, they address data protection compliance and provide a tool for a controller's use to evaluate a particular service. Nonetheless, they do not take into account the forthcoming changes. If updated accordingly, however, the guidelines can be useful for both SMEs and IaaS providers who are willing to enter into an agreement compliant with data protection rules.

The objective for the final report 'Standards Terms and Performance Criteria in Service Level Agreements for Cloud Computing Services'*[57] was to summarise existing rules with respect to SLAs in the Member States and to create a model SLA that could be used by cloud service providers. The study for that report showed that it is uncommon to have cloud- and SLA-specific legislation in place and that global providers offer standard, non-negotiable SLAs, whereas small national providers may allow clients to negotiate the terms. The model SLA developed in the report is not a standalone contract but a cloud-oriented set of elements to be addressed in SLAs, comprising only measurable and technology-neutral metrics. It targets B2B contracts and is not comprehensive, but it could complement existing guidelines if the results of the separate initiatives for these were to be revised, codified, and developed further.

One of the most recent proposals made by the European Commission in the context of the Digital Single Market Strategy is the Digital Content Directive*[58], designed to harmonise some facets of contracts for

53 A Digital Single Market Strategy for Europe. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 6.5.2015, COM(2015) 192. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192 (most recently accessed on 4.7.2016).

54 Data protection code of conduct for cloud service providers. Available at http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=11194 (most recently accessed on 4.7.2016).

55 Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, Article 29. Working Party, 2588/15/EN WP 232, 2015. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf (most recently accessed on 4.7.2016).

56 Cloud service level agreement standardisation guidelines, 2014. Available at http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6138 (most recently accessed on 4.7.2016).

57 Standards terms and performance criteria in service level agreements for cloud computing services. Final Report, time.lex and Spark Ltd, 2015. Available at http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=10860 (most recently accessed on 4.7.2016).

58 Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, COM(2015) 634 final. Available at http://ec.europa.eu/justice/contract/files/digital_contracts/dsm_digital_content_en.pdf (most recently accessed on 4.7.2016).

supply of digital content[*59]. Cloud services are within the scope of the proposed Directive because the notion of digital content (the subject of the Directive) encompasses services that allow creation of the data at issue[*60]. However, it excludes SMEs from the scope of application by defining a consumer as a natural person acting outside the connection of said person's trade or business[*61]. Hence, SMEs will not be eligible to enjoy certain rights in respect of contracts for the supply of cloud services, in contrast to private consumers.

In summary, it can be stated that the European Commission sees SMEs' adoption of cloud computing as beneficial for the Digital Single Market and has initiated various studies in this context. Still, most of the reports addressing data protection compliance are no longer accurate, because of the forthcoming changes. Furthermore, some of the related legislative initiatives fail to acknowledge B2B relations, by being consumer-centric – namely, the Digital Content Directive.

6. Conclusions on how the new regulation is likely to affect SMEs' use of IaaS

When we return to the initial questions – that is, whether SMEs will be equally interested in adopting IaaS when the GDPR comes into force and whether the GDPR interferes with the objective of wider adoption of cloud computing by SMEs – it is apparent that the former is to be answered in the negative and the latter in the affirmative. The coming changes will diminish the main benefits that IaaS offers today, which are low transaction cost and rapid access to easily scalable resources. To remain compliant with the data protection rules, SMEs will have to invest heavily in negotiations with the providers (if providers will actually be willing to negotiate) or consider alternative options – namely, traditional outsourcing services.

Data controllers' and data processors' compliance under the forthcoming data protection regime can be effectively secured through an appropriate agreement and co-operation when SMEs obtain traditional outsourcing services. However, cloud computing does not anticipate the same level of co-operation between the parties; the services are offered on a take-it-or-leave-it basis. A sensible choice for SMEs seeking to obtain infrastructure resources would be to co-operate with a traditional IT outsourcing provider (possibly previously known) rather than approach an external cloud provider and use a public IaaS solution. Consequently, the GDPR interferes with another EC objective, wider adoption of cloud computing by SMEs.

While interest in cloud services is currently growing, the proposed data protection regime will either slow it down or considerably change the state of the market. As data protection rules better suit outsourcing relations, long-established ITO providers with a large customer base will certainly benefit. By catching up with recent technological developments, they will be able to offer more flexible solutions and provide comprehensive guarantees as to data protection compliance. Obtaining outsourcing services does still have its dangers;[*62] nevertheless, some of them may soon be addressed by the European Commission proposals.[*63]

Despite a considerable number of initiatives to promote cloud adoption by SMEs, the results of most of them are going to become obsolete – firstly, because they do not refer to the GDPR; secondly, because they assume the parties to have equal bargaining power; and, finally, because they lack provision for incentives for the service providers. The cloud computing market is largely self-regulated right now, and, although there are competition concerns at the moment, they will be overshadowed by compliance concerns and increases in transaction cost.

While large enterprises may be able to address these compliance concerns effectively by allocating the necessary resources, SMEs will not be able to do the same and will need to reconsider their options. Those SMEs that are planning to adopt IaaS may want to think twice about whether to entrust the provision of resources to an external cloud provider and opt for a public cloud option or instead turn to an outsourcing

59 *Ibid*., Recital 2.

60 *Ibid*., Article 2 (1a).

61 *Ibid*., Article 2 (4).

62 Such as 'data hostage' terms – clauses allowing the service provider to retain the data until certain conditions are met (the provider being paid for the service, a termination fee being paid, etc.). See R.H. Carpenter. Walking from cloud to cloud: The portability issues in cloud computing. – *Washington Journal of Law, Technology and Arts* 2010 (6) / 1, p. 4.

63 The data hostage issue could be addressed by a proposal on data ownership and the free flow of data. See Note 53 (A Digital Single Market Strategy for Europe), p. 20.

provider and purchase a private-cloud or even non-cloud solution. Those SMEs already taking advantage of public-cloud IaaS will have to either negotiate new terms with the provider (which might prove difficult) or turn to an outsourcing provider.

One could avoid such consequences by developing a data protection framework that is more suitable for today's realities. Rather than assume that similar business relations exist between each company processing personal data and the respective subcontractor(s), the data protection scheme should acknowledge diversity of business models and consider whether it is necessary to make the same demands of each and every actor. Secondly, the EC may want to consider making data protection rules less data-subject-oriented. As was shown above, the EC, in an attempt to serve data subjects, misses an opportunity to address B2B relations too and provide further benefit to data subjects. Thirdly, it could be advantageous to look for an alternative notion of personal data. There have been discussions about what that could be, with proposals ranging from abolishing the controller–processor concept and vesting data controller obligations in anyone processing the data[*64] to not treating encrypted data as personal data in the absence of an encryption key[*65].

Although the Commission 'does not tend to be overly intrusive, in order to avoid hampering the technological development of the ICT sector in the EU, which is perceived to be a key sector of the EU economy'[*66], it remains to be seen how the forthcoming changes are going to affect competition in the market for computer infrastructure resources. A transaction cost that has become so high that it exceeds the perceived benefit could hinder the intended impact of the legislation.[*67] Forcing an ill-suited framework into place may harm competition without achieving substantial results in protecting data subjects' rights and could hamper further development of technology, not to mention interfering with the efforts to promote cloud computing's adoption.

64 P. Hert, V. Papakonstantinou, D. Wright. The proposed data protection regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. – *Computer Law & Security Review* 2012 (28) / 2, pp. 133–134.

65 W. Hon, C. Millard, I. Walden. Who is responsible for 'personal data' in cloud computing? – The cloud of unknowing, Part 2. – *International Data Privacy Law* 2012 (2) / 1, p. 14.

66 L. Luciano, I. Walden. Ensuring competition in the Clouds: The role of competition law? – *ERA Forum* 2011 (12) / 2, p. 271. – DOI: http://dx.doi.org/10.2139/ssrn.1840547.

67 S. Romanosky, A. Acquisti. Privacy costs and personal data protection: Economic and legal perspectives. –*Berkeley Technology Law Journal* 2009 (24) / 3, p. 1096.