Missing Links in the Proposed EU Data Protection Regulation and Cloud Computing Scenarios: A Brief Overview

by **Iheanyi Samuel Nwankwo***, LL.M, Research Assistant, Institute for Legal Informatics, Leibniz University Hannover

Abstract: Applying location-focused data protection law within the context of a location-agnostic cloud computing framework is fraught with difficulties. While the Proposed EU Data Protection Regulation has introduced a lot of changes to the current data protection framework, the complexities of data processing in the cloud involve various layers and intermediaries of actors that have not been properly addressed. This leaves some gaps in the regulation when analyzed in cloud scenarios. This paper gives a brief overview of the relevant provisions of the regulation that will have an impact on cloud transactions and addresses the missing links. It is hoped that these loopholes will be reconsidered before the final version of the law is passed in order to avoid unintended consequences.

Keywords: Cloud computing, Data Protection Regulation, Data Transfer, Controller, Processor Measures, DRM

Recommended citation: Iheanyi Samuel Nwankwo, Missing Links in the Proposed EU Data Protection Regulation and Cloud Computing Scenarios: A Brief Overview, 5 (2014) JIPITEC 32, para 1.

A. Introduction

1 Although the concept of "cloud" is metaphorical, cloud computing currently represents another big innovation in the IT industry that tends to maximize the use of the Internet. This is not only seen in its concentration of large computing power in a single space, but also in its functionality as an always available, unlimited tool to store and access data no matter the location.[1] However, like some other technical innovations before it, it has not been easy to determine how to append a precise legal definition to the concept as well as to bring its uses within a legal framework. This conundrum is easily appreciated when analyzing data protection laws within the context of cloud computing, for instance, because data represents the main raw material upon which cloud technology thrives. The fact that more data is constantly linking to individual persons, of course, plausibly triggers debates concerning data protection requirements in cloud transactions (requirements relating to privacy, security, transparency, accessibility, and rights and freedoms of data subjects). Such requirements could, for example, restrict personal data from being transferred from one country to another for jurisdictional purposes.[2] Cloud computing, on the other hand, depends on automated data movement around several data centers located in different parts of the world, and relies on the Internet for access to such data. This location-agnostic feature of cloud computing potentially has several data protection implications because of the multiple jurisdictions that may be involved.

2 European data protection law, for instance, is location-focused, assuming physical movement of data from one place to another.[3] This fact is reflected in the current Data Protection Directive 95/46/EC ("DPD") which predates the Internet boom, making it difficult to reconcile some of its provisions with the operations of Internet-enabled technologies such as cloud computing.[4] However, in a bid to reflect the traditional reasoning in a cloud framework, the Article 29 Working Party (WP29) has opined that mirroring personal data from a server in the EU to a US-located server constitutes a data transfer.[5] While this may appear convenient for the WP29, it fails to solve the complexities in applying the data export rules in cloud transactions.

3 Having recognized this state of affairs, the European Commission has published a draft proposal for a Data Protection Regulation ("draft regulation") that will replace the DPD.[6] Though the draft regulation is still undergoing parliamentary amendments, this paper seeks to examine some of its salient provisions as applicable to cloud computing models. In particular, it will focus on the controller-processor roles and data export provisions in the draft regulation that may potentially impact cloud transactions. At the end, it will show some of the missing links in the proposal that need to be addressed before the final version is passed.

B. Cloud Computing and Its Operations

4 Like most technical concepts, defining cloud computing is fraught with difficulties and controversies, especially due to the evolving nature of the technology. It is, however, not the intention of this paper to go into those controversies. For the purpose of this paper, cloud computing describes a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space.[7] A more technical and widely cited definition has been offered by the United States National Institute of Standardization and Technology (NIST).[8]

5 Cloud computing services can be offered in various forms, three of which are most prominent: SaaS, PaaS and IaaS. *Software as a Service (SaaS)* refers to providing the cloud consumer with the capability to use the cloud service provider's applications (software) running on a cloud infrastructure.[9] These applications are configured to suit the consumer's preferences and are accessible from various client devices through the Internet (e.g. web-based email or electronic health records). *Platform as a Service (PaaS)* is another service offering where the service consumer is provided with the capability to deploy onto the cloud infrastructure, applications created using programming and support tools from the cloud service provider (e.g. centralized analysis of MRI scans or X-rays built on Microsoft Azure, for example). *Infrastructure as a Service (IaaS)* refers to the capability provided to the service consumer to provision processing, storage, networks, and other fundamental computing resources on an infrastructure of the cloud service provider. One fundamental consequence of these service models is that the service consumer does not manage or control the underlying cloud infrastructure, including the network, servers, operating systems or storage,[10] but may have control over the deployed applications and possibly configuration settings for the application-hosting environment.[11]

6 The above-mentioned services can be deployed in four possible ways:

- *Private cloud* where the cloud infrastructure is provisioned for exclusive use by a single organization. It may be owned, managed and operated by the organization, a third party, or some combination of them, and the data center may be hosted on or off premises of the cloud consumer.[12] This model is comparable to buying, building and managing your own infrastructure. It is more beneficial for security purposes and may not bring much in terms of cost efficiency.[13]

- *Community cloud* where the cloud infrastructure is provisioned for exclusive use by a specific community of consumers (organizations that have shared concerns due to their mission, security requirements, policy, compliance considerations, among others). It may be owned, managed and operated by one or more of the organizations in the community, a third party, or some combination of them, and the data centre may be hosted on or off premises of the cloud consumer.

- *Public cloud* where the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed and operated by a business, academic, or government organization, among others, and the data centers exist on the premises of the cloud provider.

- *Hybrid cloud* where the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community or public) that remain unique entities but are bound together by technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds).[14]

7 The cloud supply chain could be a combination of many components or services from different suppliers or providers. Multiple services are involved in the layers of the stack of the cloud ecosystem,

each of which could be managed by a different party. These could range from third parties who are involved in the provisioning of physical space for the data centers to those who maintain the data centers and even cloud brokers. A good illustration has been provided by Hon and Millard (2013),[15] and diagrammatically represented in Kate's blog.[16] It is significant to note, however, that cloud end users see the services they are using as an integrated service, and do not bother with the underlying components. Regrettably, this has the tendency of depriving the legally defined data controller the actual control of the data in factual understanding.[17] As we will see below, this state of affairs is yet to be addressed in the draft regulation.

C. Provisions of the Draft Regulation that Are Significant for Cloud Transactions

8 The draft regulation retains the core concepts and basic principles enshrined in the DPD, such as technology neutrality, controller-processor dichotomy and legal bases for data transfer to third countries, among others. This means that there are no specific provisions for cloud computing *per se*, and the data controller remains responsible for data processed on its behalf, no matter the means. At the same time, however, there are significant improvements in the draft regulation. Importantly, it will have direct application in the Member States, which will eliminate the fragmentation seen in national implementation of the DPD to a large extent.[18] Another significant change is the amendment of the extra-territorial application of Article 4(1)(c) of the DPD. In effect, this amendment will exempt the application of data export rules during a re-transfer of data that had originally been collected from a third country (involving non-EU residents) but transferred to an EU-based processor (e.g. cloud provider) for processing.[19] The French *Commission nationale de l'informatique et des libertés* (CNIL) has already initiated this exemption, thereby removing cumbersome procedures during such data re-transfer.[20] Non-EU data controllers will be regulated only where their processing activities relate to the offering of goods or services to EU subjects or monitoring their behavior.[21]

9 The draft regulation further provides additional rights to data subjects; increases the obligations of data controllers; and imposes some direct obligations on data processors (a category that most cloud service providers will possibly belong to). This will inevitably affect the relationship between cloud providers and their customers. For instance, data subjects' rights to data portability may force cloud customers to use only service providers that have portable facilities in order to comply with the law. Similarly, cloud customers will favor providers who are more proactive in their internal controls, which reflect increased accountability as envisaged in the regulation.[22]

10 A data protection certification seal has also been introduced in the draft regulation.[23] In effect, a cloud provider could voluntarily apply to the Data Protection Authorities (DPAs) to be audited and given a European Data Protection Seal as a certification mark indicating its compliant status with EU data protection law.[24] Furthermore, data controllers wishing to use cloud services for certain types of data processing such as sensitive health data will have to conduct a data protection impact assessment before sending data to the cloud. This will be the necessary implication of Article 33 of the draft regulation.[25] Mandatory notification of data breaches (by data controllers with the help of processors where necessary) will equally be given due consideration in cloud relationships when the regulation becomes effective.[26]

11 While retaining the current approach for third-country data transfer, the regulation still introduces remarkable changes:

1. An adequacy assessment of a third country's level of data protection will be made by the Commission on a territorial or sector-specific basis, or for the country as a whole, as well as for international organizations.[27]

2. Where no adequacy decision has been made, appropriate safeguards by way of a legally binding instrument could be relied upon by data controllers or processors for data export through the use of any of the following:

   Binding Corporate Rules (BCRs);

   Standard data protection clauses adopted by the Commission;

   Standard data protection clauses adopted by a regulator; and

   Contractual clauses authorised by a regulator.[28]

   The compromise parliamentary text has included an additional legal basis in the form of "European Data Protection Seals", which would enable certified organizations to rely on privacy seals as an adequate basis for transfer outside the EEA.[29]

3. No further authorization will be imposed by a supervisory authority once a positive assessment has been made by the Commission, or where the standard data protection clauses adopted by the Commission or a Member State's supervisory authority are used to effect data transfer.[30]

4. The draft regulation now recognizes BCR for data processors and lays down its framework.[31]

5. The derogations in Article 26 of the DPD were maintained with some minor modifications, such as conducting an impact assessment before a transfer where the purpose is in pursuit of the legitimate interest of the controller or processor.[32]

12 Another remarkable provision in the draft regulation is the adoption of 'one-stop-shop' or general recognition of a lead authority in cases where the controller or processor is established in more than one Member State. This will be a time- and cost-saving mechanism for obtaining authorization where necessary. It is hoped that the delegated acts in the draft regulation will not create more red tape in this regard.[33] Additionally, fines of up to 500,000 EUR, or 1% of its annual worldwide turnover in the case of an enterprise, could be imposed as an administrative sanction for a violation of the regulation.[34]

13 It is believed that these provisions will make international transfer restrictions easier to navigate.[35] However, it is not certain how these reforms will look in the final version of the regulation, since recent parliamentary amendments have modified a lot of the initial provisions. The Committee on Civil Liberties and Home Affairs ("LIBE"), for instance, has rejected the adequacy finding for a processing sector, insisting that such an approval would increase legal uncertainty in international data transfers.[36] For example, this could have the effect that it would not be possible for the Commission to decide that cloud providers who are Health Insurance Portability and Accountability Act (HIPAA)-compliant in the US would provide adequate protection to host health data from the EU. The LIBE Committee also rejected the use of non-legally binding instruments for international data transfers, and additionally proposes a two-year transition period for all authorizations by DPAs on the basis of Article 26(2) or Article 26(4) of the current DPD to elapse.[37] A new provision meant to address the issue of access request by public authorities or courts from a third country has also been included in both the LIBE Committee's report and the compromise text from Parliament. This provision requires that such a transfer shall only be on the basis of a mutual assistance treaty or international agreement in force between the requesting third country and the Union or the Member State involved. A prior authorization from the supervisory authority should also be obtained before effecting the transfer, and a notification given to the data subject. A new default position has also been created by the Parliament's compromise text to the extent that where there is more than one controller or processor involved in the processing, each controller or processor will be jointly and severally liable for the damage (unless they have an appropriate written agreement establishing liability in the determination of their responsibilities), and in the case of a group of undertakings, the entire group shall be liable as a single economic entity.[38]

14 What the effect of these parliamentary amendments will be for cloud services is yet to be fully understood, except to say that obtaining new approvals after the transition period will have cost implications to data controllers and processors. Second, where no mutual assistance treaty or international agreement exists between the countries involved, there is a potential risk that this may put the cloud provider in an awkward position as to which rule to follow. In essence, because of the lack of clarity about jurisdictional boundaries, this provision would prohibit organizations from complying with governmental orders, and this makes them vulnerable to criminal penalties.

D. The Draft Regulation and Cloud Realities: Missing Links

15 While the draft regulation and various amendments to it are being debated, it is important to point out some other issues that have not yet been addressed in the proposal, especially in relation to cloud computing. First, as pointed out earlier, cloud computing involves various layers and intermediaries of actors for which a strict application of the data controller-processor dichotomy may be ambiguous and misleading.[39] This can be seen in the use of intermediaries such as cloud brokers and integrators who act as a conduit between the cloud customer and the provider but in fact have no infrastructure to process data. Some other actors in the cloud stack, such as those who provide the physical infrastructure, may be so remote from the actual data processing that regarding them as either a joint controller or a processor may make no sense. So far, the draft regulation has not taken proper cognizance of these sets of actors. The closest attempt at recognizing this gap is in a new provision in the LIBE Committee's report that introduced a new party defined as "producers".[40] Though by a stretch of argument the definition of "data producer" may include some cloud intermediaries, this may be an ambiguous way of describing all of them, since some of the intermediaries do not have any infrastructure for producing or processing data but only provide monitoring services. Of course, making every party in the chain of transaction joint controllers will not solve the problem as purported in Article 24 of the draft regulation. Hert and Papakonstantinou (2012) have opined as follows:

> *... the distinction between data controllers and data processors, that was perhaps clear at the time the Directive was introduced, is increasingly disputed in the contemporary complex business environment. [...] The distinction between the two data processing actors is becoming increasingly blurred in an interconnected world of ubiquitous computing. In view of the above, perhaps the preferable way forward would be*

for the Commission to boldly abolish the notion of "data processors" from its Regulation altogether, and vest the data controller title, rights and obligations upon anyone processing personal information, regardless of its means, conditions or purposes.[41]

16 While this stand may appear extreme, it goes to show the frustration at reconciling the inadequate nature of the binary division of actors in the data processing chain, where collaborating but autonomous entities are involved, and whose mutual relationships can no longer be characterized as a simple 'relationship of command' or 'principal-delegate' relationship.[42] Not clarifying these relationships in the draft regulation may have unintended consequences, such as creating legal uncertainty as to the status of actors and the allocation of responsibility in the data processing chain.[43] A number of opinions have called for a rethinking in the classification of actors in view of modern data processing possibilities, of which cloud computing is a ready example.[44] The draft regulation, as well as the various parliamentary amendments, has not devoted significant attention to this issue.

17 Second, the regulation has retained the use of the model contractual clauses. However, in their present form these clauses do not adequately cover all the constellations of cloud transactions. For instance, there are no model contractual clauses for an EU processor to transfer data to a controller in a third country, or for an EU processor to transfer data to a sub-processor in a third country.[45] These cases are possible as more data processors in the EU are transacting with many data controllers and sub-processors who are outside the EU.[46] Furthermore, certain clauses in the model do not reflect and may not fit into the technical and organizational frameworks of cloud services. For instance, the assumption that the data controller is the strong, controlling party that has the actual ability to instruct and control the processor (cloud providers, for example) may be illusory.[47] Provisions requiring the processor to submit its facilities for audit by the controller and supervisory authorities are less feasible in the cloud, in view of the millions of customers a cloud provider may have.[48] It is also less likely that a cloud service provider will first obtain prior written consent from all of its customers before engaging in every support service, where those are regarded as sub-processing.[49] As Svantesson (2012) rightly observes, "the power-balance in cloud computing agreements is typically different to the power-balance between data controllers and data processors anticipated in the data protection regulation."[50] This calls for an amendment of these clauses in view of emerging structures in modern data processing realities.

18 Third, some of the provisions of the draft regulation on international data transfer raise fresh questions.[51] In spite of the controversies surrounding the use of "onward transfer" in the EU-US Safe Harbor framework, it has been recognized in the regulation without any definition or mechanism for its application.[52] The concept entails that after EU personal data is transferred to a Safe Harbor-certified US entity, further transfers from the importer to a third party (onward transfers) are possible, subject to restrictions under the Safe Harbor.[53] It is not clear how this concept will apply to other entities that are not subject to the Safe Harbor framework, since the original concept has been limited to the US. There is a need for more clarity in the application of the concept if it is intended to have a general application, so that it does not serve as a tool to circumvent data protection requirements.[54]

19 Fourth, although the draft regulation has recognized the use of BCRs, its application only within the same group of companies or organization will still limit its potential impact. The inability to transfer data between two different processors or controllers, who both have duly approved BCRs but not belonging to the same group, is not logical. This appears to be contrary to the case where two third countries that have adequacy status are allowed to transfer EU data between them on that basis. A similar facility should be accorded to BCR-approved entities since it represents a binding obligation.

E. Conclusion

20 It is encouraging that the draft regulation will bring a level of harmonization in the data protection regime within the EU. However, cloud realities show that much still needs to be done in order to reap the full potential of cloud computing in Europe. There is a need for legislators to understand cloud architecture, features and business models. Hon, *et al* (2012) argue that some of the current difficulties in the legal aspects of the cloud arise not necessarily because contract terms are poor, but because data protection laws assume certain things which are not true in the cloud.[55] If the present reform is not holistic, it may lead to unintended consequences. Reflecting privacy in a pragmatic way without disproportionately interfering with technological advancements is essential in this e-age.[56] It is hoped that the outlined missing links in the draft regulation will be addressed while the proposal is still debated.

* The original version of this paper was submitted to the Taylor Wessing 2013 Essay Competition, and the author is grateful to Prof. Dr. Nikolaus Forgó for his guidance in the course of writing the paper. The author also appreciates the support of Julia Pfeiffenbring and Marcelo Corrales.

1 E. Ustaran, *The Future of Privacy*, (DataGuidance, UK, 2013) p.10.

2 E. Yoran, "Cloud Computing and Data Residency Laws", *Sys-con Media*, (available at: http://www.sys-con.com/node/2660874).

3 D. Svantesson, "Data Protection in Cloud Computing – The Swedish Perspective", *Computer Law & Security Review*, Vol. 28, Issue 4, 2012, pp. 476-480.

4 P. De Hert and V. Papakonstantinou, "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals", *Computer Law & Security Review,* Vol. 28, Issue 4, 2012, pp. 130 -142.

5 See Article 29 Working Party Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP128 (2006).

6 European Commission, A proposal on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final. This paper will take into account some of the amendments to the original draft such as the EU Parliament's Committee on Civil Liberties, Justice and Home Affairs ("LIBE") report of January 2013 (available at: https://www.huntonprivacyblog.com/wp-content/files/2013/01/Albrecht-Report-LIBE.pdf), and European Parliament Compromise Text published on October 21, 2013: (available at: https://www.huntonprivacyblog.com/files/2013/12/EUCompromise-Text.pdf).

7 Article 29 Working Party, Opinion 05/2012 on Cloud Computing, p. 4.

8 NIST defines it thus: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, 2011 (available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf).

9 *Ibid.*

10 This is the case in public clouds but may vary in other deployment models.

11 Mell and Grance, *op. cit.,* note 8.

12 *Ibid.*

13 N. Metha, "The 4 Primary Cloud Deployment Models", 2012 (available at: http://www.cloudtweaks.com/2012/07/the-4-primary-cloud-deployment-models/).

14 Mell and Grance, *op. cit*, note 8.

15 W. Hon and C. Millard, "Cloud Technologies and Services" in C. Millard (ed), *Cloud Computing Law,* (Oxford University Press, United Kingdom, 2013) pp. 13-16.

16 (Available at: http://www.katescomment.com/iaas-paas-saas-definition/)

17 See the Article 29 Working Party, Opinion 05/2012, op cit, note 7.

18 For instance, a Regulation will also abolish certain flexible approaches by DPAs such as the ability of a data controller to make a self-assessment of the adequacy level for data export in the UK. See "The New EU Data Protection Regulation - Revolution or Evolution?", (available at: http://www.slaughterandmay.com/media/1844766/the-new-eu-data-protection-regulation-revolution-or-evolution.pdf) p. 6.

19 See Art. 3 of the Proposed Regulation. See also W. Hon and C. Millard, "How Do Restrictions on International Data Transfer Work in Clouds?" in C. Millard (ed), *Cloud Computing Law,* (Oxford University Press, United Kingdom, 2013) p. 255.

20 See L. de Souza, "CNIL Simplifies Formalities for Non-EU Companies Using Data Processors in France", (available at: http://www.hldataprotection.com/2011/03/articles/international-eu-privacy/cnil-simplifies-formalities-for-noneu-companies-using-data-processors-in-france/).

21 Art. 3(2) of the Draft Regulation.

22 "How Proposed EU-Wide Data Protection Regulation Will Affect U.S. Based Businesses", (available at: http://www.cooley.com/showalert.aspx?Show=66023).

23 Art. 39 of the Draft Regulation.

24 The compromise parliamentary text has provided more detail on the mechanism for certification.

25 See also the new Art. 32a of the compromise parliamentary text.

26 Art. 31 of the Draft Regulation.

27 Art. 41 of the Draft Regulation.

28 Art. 42 of the Draft Regulation.

29 Art. 42(2)(aa) of the Draft Regulation as amended in the compromise parliamentary text. See also N. McBride, L. Sotto and B. Treacy, "Privacy and Data Security: The Future of the US-EU Safe Harbor", *Practical Law*, (available at: https://www.huntonprivacyblog.com/files/2013/12/Privacy-Data-Security-The-Future-of-the-US-EU-Safe-Harbor.pdf).

30 Art. 42 (3) of the Draft Regulation.

31 See Arts. 42 and 43 of the Draft Regulation.

32 See Art. 44 of the Draft Regulation.

33 "Impact of the draft EC data protection Regulation on data transfers," (available at: http://www.taylorwessing.com/globaldatahub/article_impact_draft_regulation_data_transfers.html).

34 See Art. 79 of the Draft Regulation. Note however that the compromise parliamentary text has increased the figure to 5% of annual worldwide turnover of an enterprise or €100 m.

35 *Op. cit,* note 33.

36 European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 2012/2011 (COD).

37 Note that the compromise parliamentary text extended the transition period to five years. See Art. 41(8) of the Draft Regulation as amended in the compromise parliamentary text.

38 See the amendment of Art. 77 in the compromise parliamentary text. See also Hunton & William Executive briefing paper update 3 on the proposed General Data Protection Regulation, December 2013.

39 P. Blume, "Controller and Processor: Is There a Risk of Confusion?", *International Data Privacy Law,* Vol. 3, No 2, 2013, pp.140-145. See also B. Alsenoy, "Allocating Responsibility Among Controllers, Processor, and 'Everything in Between': The Definition of Actors and Roles in Directive 95/46/EC", *Computer Law and Security Review,* Vol. 28, Issue 1, 2012, pp. 25-43.

40 'Producer' means a natural or legal person, public authority, agency or any other body which creates automated data processing or filing systems designed for the processing of personal data by data controllers and data processors. See Art. 4 – (point 6 a (new)) of the LIBE Report. Similarly, the compromise parliamentary text has included a definition for "third parties", but this appears not to cover cloud intermediaries. See Art. 4(7a) of the compromise parliamentary text.

41 Hert and Papakonstantinou, op cit, note 4, p. 134.

42 B. Alsenoy, op. cit, p. 39.

43 P. Blume, op. cit, note 39.

44 See P. Blume, op. cit, B. Alsenoy, op. cit, W. Hon and C. Millard, op cit, Hert and Papakonstantinou op. cit.

45 See J. Hartung, "Germany's New Rules on Processor Agreement," (available at. http://wn.com/Germany%27s_new_rules_on_international_processor_agreements).

46 W. Hon and C. Millard, "Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4", 2011, (available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2034286).

47 W. Hon, C. Millard and I. Walden, "Who is Responsible for Personal Data in the Clouds?" in C. Millard (ed), *Cloud Computing Law,* (Oxford University Press, United Kingdom, 2013) pp. 193 -219.

48 See clauses 5(f), 8(2), 12(2) of the controller to processor standard clauses 2010.

49 See clauses 5(h) and 11, *ibid.*

50 D. Svantesson, *op. cit.*, note 3.

51 See, for instance, C. Kuner, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", *Bloomberg BNA Privacy and Security Law Report*, 2012, p. 9.

52 Art. 40 of the Draft Regulation.

53 N. McBride, *op. cit,* note 29.

54 See C. Kuner, "Onward Transfer of Personal Data under the U.S. Safe Harbor Framework", *Privacy and Security Law Report,* 2009, pp.1-2.

55 W. Hon, C. Millard and I. Walden, "Negotiating Cloud Contracts - Looking at Clouds from Both Sides Now," 2012, (available at: http://ssrn.com/abstract=2055199), p. 40.

56 E. Pyykko, "Data Protection at the Cost of Economic Growth?" *ECRI Commentary*, No. 11, November 2012, p. 2.