Queen Mary University of London, School of Law

Legal Studies Research Paper No 84/2011

Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law?

The Cloud of Unknowing, Part 3

W Kuan Hon

Julia Hörnle

Christopher Millard

~~Updated 28 October 2011: added Legal Studies Research Paper series number above, corrected typographical error on p 31 (reference should be to Regulation 2001/44/EC, not Regulation 2000/44/EC).~~

Updated 9 February 2012: updated to comment on draft Data Protection Regulation, and minor updates.

Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3[1]

W Kuan Hon,[2] Julia Hörnle[3] and Christopher Millard[4]

~~7 September 2011~~

9 February 2012

Abstract

Where data centres located in the ~~EEA~~European Economic Area ('EEA') are utilised for cloud computing services, the customers, and in some circumstances even cloud service providers, could become subject to the EU Data Protection Directive on the basis that the data centre may be an 'establishment' of theirs, or involves their 'making use' of equipment in the EEA. This may be the case whether the utilisation is direct or indirect through 'layers', for example where a non-EEA cloud user uses the services of an EEA provider, or indeed of a non-EEA provider who happens to use an EEA cloud provider or a data centre situated in the EEA. Software as a Service providers may similarly find themselves subject to the Directive if they save or retrieve cookies or the like on their end users' equipment, as EU data protection regulators have asserted, not without controversy. Even within the EEA, national implementations diverge.

[1] This article forms part of the QMUL Cloud Legal Project ('CLP') http://cloudlegalproject.org, Centre for Commercial Law Studies, Queen Mary, University of London ('CCLS'). Specifically, this paper forms part 3 of a 4-part series of related CLP papers on key foundational data protection issues relevant to cloud computing, namely: what information is regulated under the DPD; who is regulated; which country's laws apply and which authorities are competent to regulate; and how can restrictions on transferring personal data outside the EEA be addressed? The first two papers covered personal data (W K Hon, C Millard and I Walden. 'The problem of 'personal data' in cloud computing: what information is regulated?—the cloud of unknowing', International Data Privacy Law (2011) 1 (4): 211-228. doi: 10.1093/idpl/ipr018 ('CLP Personal Data Paper')) and responsibility for personal data in the cloud (W K Hon, C Millard and I Walden, 'Who is responsible for 'personal data' in cloud computing?—The cloud of unknowing, Part 2', International Data Privacy Law (2012) 2 (1): 3-18. doi: 10.1093/idpl/ipr025 ('CLP Controllers/Processors Paper')). The fourth paper covered the DPD's data export provisions (W K 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) Queen Mary School of Law Legal Studies Research Paper No 85/2011 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925066>) last accessed 9 February 2012.

The authors are grateful to Microsoft for generous financial support making this project possible. Views herein, however, are solely the authors'.

[2] ~~Research Assistant~~Consultant researcher, CLP.

[3] Senior Lecturer in Internet Law and Programme Director LLM/Diploma in Computer & Communications Law by Distance Learning, CCLS.

[4] Professor of Privacy and Information Law, CCLS; Project Leader, CLP; Research Associate, Oxford Internet Institute, University of Oxford.

The current legal uncertainties are unsatisfactory, and may discourage the use of EEA data centres or EEA providers for cloud computing. ~~We argue~~This paper argues that Data Protection Directive obligations should be applied to entities based on country of origin, within the EEA, and targeting or directing, for non-EEA entities, with clear tests for both concepts. ~~If~~While the draft Data Protection Regulation would introduce approaches based on country of origin and targeting, the concepts it uses in that regard fail to address many of the current problems. The concepts of 'establishment' ~~and 'equipment'/'means' are to be~~, 'context of activities' and 'main establishment', if retained, ~~they should~~need to be further clarified and harmonised, and the new concepts of 'occasionally offering' and 'monitoring' further explained. The status of providers of physical and software infrastructure, as well as intermediate providers, would also benefit from further clarification, in particular as regards in what circumstances EU data protection laws apply to processors, and which ~~country's security requirements and other~~ rules apply to ~~a~~ cloud ~~provider~~providers as processors.

1. Introduction

This paper focuses on the applicability of the EU Data Protection Directive[5] ('DPD') to cloud computing actors, and the jurisdiction of data protection authorities to regulate them. As will be discussed ~~in this paper~~below, the DPD may apply even to non-EEA entities, because of its potentially-broad reach. Various other key data protection law issues raised by cloud computing environments are addressed in related papers.[6]

Before a substantive discussion of applicable law and jurisdiction, it may be apt to define cloud computing. Definitions vary, but the CLP definition of cloud computing is:[7]

- Cloud computing provides flexible, location-independent access to computing resources that are quickly and seamlessly allocated or released in response to demand.
- Services (especially infrastructure) are abstracted and typically virtualised, generally being allocated from a pool shared as a fungible resource with other customers.
- Charging, where present, is commonly on an access basis, often in proportion to the resources used.

Cloud computing activities are often classified under three main service models – Infrastructure as a Service ('IaaS'), Platform as a Service ('PaaS') or Software as a Service ('SaaS').[8] These services form a spectrum, from low-level (IaaS) to high-level (SaaS)

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281/31, 23.11.1995. The DPD extends to non-EU countries within the EEA, namely Iceland, Liechstenstein or Norway, by virtue of Joint Committee Decision of the EEA Joint Committee No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication services) to the EEA Agreement OJ L 296/41, 23.11.2000. Hence, ~~we~~this paper generally ~~use~~uses the broader 'EEA' instead of 'EU' in this paper. Unless otherwise stated, references in this paper to articles and recitals will be to articles and recitals of the DPD.

[6] ~~The papers in this CLP data protection series deal with key foundational data protection issues relevant to cloud computing, namely: what information is regulated under the DPD; who is regulated; which country's laws apply and which authorities are competent to regulate; and how can restrictions on transferring personal data outside the EEA be addressed? The first two papers covered personal data (W Kuan Hon, Christopher Millard and Ian Walden, 'The Problem of 'Personal Data' in Cloud Computing – What Information is Regulated? The Cloud of Unknowing, Part 1' (2011) Queen Mary School of Law Legal Studies Research Paper No 75/2011 ('CLP Personal Data Paper') <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1783577>) and responsibility for personal data in the cloud (W Kuan Hon, Christopher Millard and Ian Walden, 'Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2' (2011) Queen Mary School of Law Legal Studies Research Paper No 77/2011 ('CLP Controllers/Processors Paper') <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1794130>. The fourth paper will cover the DPD's data export provisions. Issues surrounding compliance with data protection laws, such as security measures, will be dealt with in more detail in a separate CLP paper.~~ See n 1.

[7] S Bradshaw, C Millard and I Walden, ~~'Contracts~~'Contracts for ~~Clouds: Comparison~~clouds: comparison and ~~Analysis~~analysis of the Terms and Conditions of ~~Cloud Computing Services' (2010) Queen Mary School of~~cloud computing services', (2011) 19(3) Int J Law ~~Legal Studies Research Paper No 63/2010~~Info Tech, 187 doi:10.1093/ijlit/ear005 ('CLP Contracts Paper'~~)~~ <~~http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374~~>.).

[8] See further CLP Personal Data Paper (n ~~6)~~:1):

- IaaS - computing resources such as processing power and/or storage;
- PaaS - tools for constructing (and usually deploying) custom applications;

functionality, with PaaS in between. One cloud service may involve layers of providers, not always to the customer's knowledge, and perspective affects classification. For example, customers of storage service DropBox may consider it a SaaS; while for DropBox, which uses Amazon's IaaS infrastructure to provide its service, Amazon provides IaaS.[9] Also, PaaS may be layered on IaaS, and SaaS may be layered on PaaS or IaaS. So, for example, PaaS service Heroku is based on Amazon's EC2 IaaS.[10]

Cloud computing may also be analysed according to different deployment models:

- private cloud - where the relevant infrastructure is owned by, or operated for the benefit of, a single large customer (or group of related entities),
- public cloud – where infrastructure is shared amongst different, varying, users or 'tenants' (hence the term 'multi-tenancy'), so that different users may be serviced using the same hardware or even same application software instance, and/or have their data stored in the same database,
- community cloud - where infrastructure is owned by or operated for, and shared amongst, a specific limited set of users with common interests, eg US government users, or UK local government), and
- hybrid cloud – involving a mixture, eg a corporation with a private cloud may 'cloud burst' certain processing activities to the public cloud in times of peak demand.[11]

While cloud computing is often talked of as something taking place in the distant obscure ether, in reality, as with all other forms of computing, it must ultimately make use of physical computers, with physical storage facilities, housed in physical structures. Hence, the foundation of current cloud computing is the data centre or server farm. One major question ~~we address~~addressed in detail in this paper is the extent to which making use of a data centre located in the EEA for cloud computing services subjects the cloud user to EU data protection law. It is important to note that, even with private cloud, the cloud user does not necessarily own the infrastructure used to provide the cloud service. Ownership of the data centre building may be also divorced from ownership of the servers and other equipment located within it, ownership of the software infrastructure installed on that equipment, and ownership of the applications and other software run on top of that infrastructure. Similarly, whoever *owns* hardware or software infrastructure does not necessarily *manage or operate* the services which make use of that infrastructure in order to *provide* cloud computing services to *users*. They may well do so, as with a private self-hosted cloud where an entity acquires and operates a data centre to provide private cloud services using the data centre's infrastructure for its own benefit. But, equally, they may not. Even a private cloud, dedicated

---

- SaaS' - end-user application functionality, eg webmail services like Yahoo! Mail, social networking sites like Facebook, Salesforce's online customer relationship management service (enterprise SaaS).

[9] CLP Contracts ~~paper~~Paper (n 7), s 3, 8.

[10] Heroku, 'Can I connect to services outside of Heroku?' <http://devcenter.heroku.com/articles/external-services> last accessed ~~5 September 2011.~~9 February 2012. Heroku's acquisition by SaaS (and, increasingly, PaaS) provider Salesforce.com was completed in January 2011. Salesforce.com, 'Salesforce.com Completes Acquisition of Heroku' (2011).

[11] ~~Peter~~P Mell and ~~Timothy~~T Grance, The NIST Definition of Cloud Computing ~~(Draft),~~ Special Publication 800-145 (~~Draft) (~~US National Institute of Standards and Technology ~~January~~ 2011).

to a single entity or related group of entities, may be hosted in a data centre (or more than one) owned by another entity, and managed by a third party service provider – which may not own the data centre. As another example, an entity may have cages dedicated to it within a third party's data centre, within which cages are servers dedicated to that entity (whether rented or owned), but the entity's employees may be the only people with keys to the cages, and only they manage the servers.

~~In summary, a key point to bear~~These illustrate the importance of bearing in mind ~~is~~ that what appears, to the end user, to be a single cloud computing service, may in fact involve the combination of more than one cloud service, often using third party infrastructure. Cloud computing is effectively a form of outsourcing, at a variety of possible levels. However, beyond the cloud service provider, with whom the end user has a direct relationship, there may be one or more other providers - yet the end user may not know who they are, or how their use by the direct provider may impact on the service received. Hence, our reference to cloud computing as the 'cloud of unknowing'.

As regards the DPD, in summary it aims to encourage the free movement of personal data within the European Economic Area ('EEA') by harmonising national data protection provisions, while protecting the rights and freedoms of individuals ('data subjects') when their personal data ~~is~~are processed 'wholly or partly by automatic means'. It requires Member States to impose certain obligations on a data 'controller' (who determines purposes and means of processing personal data) provided it has the requisite EEA connection.[12] It does not apply to certain matters,[13] where Member States' national implementations may, for example, allow exemptions from certain obligations. Important national differences in data protection law exist, such as on civil liability and penalties for non-compliance.[14] ~~We address~~This paper addresses the DPD only at a European level, although illustrative national examples will be given.

~~The DPD is being reviewed and a draft reform measure is expected by the end of 2011. Cloud computing has been mentioned in many European Commission documents, so it seems likely the review will seek to address the implications of cloud computing in some fashion.~~[15]

~~In this article, we argue~~A proposed Regulation to replace the DPD and related draft measures were issued on 25 January 2012. Cloud computing was cited as one of the factors driving reform, with the aim of producing a robust and coherent EU regulatory regime that would ensure the effectiveness of data protection and engender trust for cloud services providers.[16]

---

[12] A ~~future~~separate paper ~~will discuss~~discusses transferring personal data outside the EEA – see n 6.

[13] Eg national security, defence - art 3(2).

[14] C Kuner, European Data Protection Law: Corporate Compliance and Regulation (2nd edn, OUP Oxford, 2007), ch 1 pt G.

[15] ~~European Commission, 'A comprehensive approach on personal data protection in the European Union' (Communication) COM (2010) 609 final (November 2010); Neelie Kroes, 'Cloud computing and data protection' (Les Assises du Numérique conference, Université Paris-Dauphine, 25 November 2010) SPEECH/10/686.~~

[16] European Commission, 'Data protection reform: Frequently asked questions' (25 January 20121) MEMO/12/41. The draft Regulation is 'Proposal for a Regulation of the European Parliament and of the Council

It will take time for the proposed reforms to be enacted, and another two years thereafter before they take effect, and they may well be amended in the course of the legislative process. The analyses in this paper will therefore continue to be relevant for some time. This paper refers to the proposed Regulation, in its originally-issued form, as the 'draft Regulation'.

This paper argues that one aspect that the reform needs to address more fully is the current uncertainty concerning the boundaries between an entity falling within the jurisdiction of EU data protection law, and not being so regulated.

This paper considers the question of when non-EEA cloud users or cloud providers become subject to EU data protection law as a result of either using EEA data centres or EEA cloud providers, or saving cookies etc on the equipment of EEA residents, under art 4 DPD. This question is important as there are many consequences if a non-EEA entity becomes subject to EU data protection law. It may, for example, be required to obtain data subjects' consent or find some other justification to transfer the data 'back' outside the EEA from the EEA data centre – even if it was 'imported' to the EEA data centre from outside the EEA in the first place, and even if the data related to non-EEA persons. Of course, whether EU law can be enforced against a non-EEA entity in practice is a different issue.

For non-lawyers, there are a few preliminary points to note. An EU Directive must be implemented into a Member State's own national law, through legislation enacted locally. This means that data protection laws may be, and indeed have been, implemented inconsistently in different Member States. Art 4 is one key area where neither implementation of the DPD nor application of its requirements have led to adequate harmonisation, with some Member States extending the applicability of their law further than the DPD does, leading to practical difficulties.[17] Our analysis below is complicated by this lack of harmonisation. Space does not permit coverage of all Member States; ~~we focus~~this paper focuses on the DPD and EU regulators' collective views (in the form of the Article 29 Working Party ('A29WP')[18]), but some examples of national laws will be given. Also, it should be noted that the A29WP's views, while persuasive, are not legally binding, and indeed, as it approves decisions by simple majority, an individual Member State's regulator may well disagree with the majority view and choose not to apply the interpretations of the A29WP.

2. Jurisdiction, Applicable Law and Data Protection Law

The DPD contains provisions on applicable law and its jurisdictional reach in arts 4 and 17(3) (the latter in respect of mere processors).

---

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 2012/0011 (COD).

[17] LRDP Kantor Ltd in association with Centre for Public Reform, *New Challenges to Data Protection- Final Report* (European Commission, 2010) [36]-[44].

[18] Established under art 29 DPD, comprising national EU data protection regulators and the European Data Protection Supervisor (who supervises compliance by EU institutions with data protection requirements).

The DPD foresaw the concept of remote processing of data (see for example recital 20) where the data processor is established in a third country. The purpose of the jurisdictional provisions is to ensure the application of the data protection obligations to personal data connected with the EEA, even if the data are processed in a non-EEA country by a non-EEA established controller.[19]

As will be seen from the following discussion the meaning of these provisions is opaque, partly due to the fact that the different languages versions do not match and partly due to the fact that the Member States could not agree on a single rule of competence, such as, for example the country of origin rule in art 3 Electronic Commerce Directive ('ECD').[20]

The main obstacle however is the lack of harmonisation of the data protection rules of the Member States due to variations in the implementation of the DPD into national law.

For this reason, the provisions on applicable law and jurisdiction are subject to interpretation so that the jurisdictional scope of the DPD is in dispute. A review and simplification of the jurisdictional grounds is therefore needed, which it is hoped will be accomplished in the revision of the DPD.[21]

Before the provisions and their application to cloud computing are discussed, it should be pointed out that for the application of the EU rules the location where the personal data are physically processed is not determinative.[22] The citizenship, residence or domicile of the persons to whom the personal data relate are also not significant.[23] Even though the essence of cloud computing is the *remote* processing of data, the data controller's and data processor's respective activities are *not* removed from the scope of the DPD merely because the data ~~is~~are somewhere in the cloud, physically processed in another, non-EEA jurisdiction (or several such jurisdictions). The location of the data or of operations on the data, which may be difficult to determine in a cloud computing service, itself is not decisive. However, the means of processing (which to an extent may overlap with the location of processing) are relevant in art 4(1)(c), discussed below.

The central provisions are contained in art 4 which contains three grounds on the basis of which the European data protection regime becomes applicable to acts of data processing.

---

[19] Article 29 Data Protection Working Party, *Opinion 8/2010 on applicable law*, WP 179 (2010) ('WP179').
[20] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market OJ L 178/1, 17.7.2000.
[21] ~~A proposal for reforming the DPD is expected to be published in late 2011.~~ See n 16.
[22] See also LA Bygrave 'Determining applicable law pursuant to European data protection legislation' in J Hörnle, I Walden *Ecommerce Law and Practice in Europe* (Woodhead Publishing Cambridge 2001) 1-11, 4; however the location of equipment or means of processing is relevant, discussed at 2.3 below.
[23] WP179; U Wuermeling *Handelshemmnis Datenschutz* (Carl Heymanns Verlag 2000) 76.

2.1 The art 4 grounds

The three grounds for applying the EU rules to an act of personal data processing are (i) establishment, (ii) public international law and (iii) use of equipment within the jurisdiction, each of which will be discussed in turn.[24]

In a cloud computing context, these grounds determine the extent to which a user or provider of cloud computing services, even if not incorporated, resident or headquartered in an EEA Member State, may become subject to obligations under EU data protection law as a result of:

1. having a subsidiary, branch or agent, or even just a data centre, in the EEA; or
2. making use of a data centre located in the EEA, or other equipment located in the EEA.

2.1.1 Establishment

According to art 4(1)(a) each EEA Member State must apply the DPD as implemented in that Member State if 'the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State', ie if the controller has an establishment there and processes personal data 'in the context of the activities of that establishment'.

It is important to note that if an EEA Member State's data protection law applies to a controller on the 'establishment' basis, the controller is then subject to the requirements of the law in relation to *all* personal data processed 'in the context of the activities' of that establishment, wherever in the world the processing takes place[25] including through using a cloud computing service. If it applies on the 'equipment' basis, conceivably the controller must comply with the relevant data protection law for all processing of the personal data concerned, again even if it occurs outside the EU.

If the same controller is established in more than one EEA Member State, that controller may have to comply with the laws applicable in these different Member States: 'when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable'.[26]

This latter provision on establishments in several Member States is tautological - while attempting to determine which law is applicable, it does this by referring to the 'national law

[24] For a detailed discussion of art 4, see Lokke Moerel, 'Back to basics: when does EU data protection law apply?' [2011] 1(2) International Data Privacy Law 92.
[25] Eg in the incident relating to Belgian entity SWIFT - Article 29 Working Party, *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP 128* (2006). However, the final decision of the Belgian authority was that Belgian law did not apply on US territory – Belgian Privacy Commission, Decision of 9 December 2008, Control and recommendation procedure initiated with respect to the company SWIFT scrl, [167].
[26] Art 4(1)(a), second sentence.

applicable'. Hence the second sentence of art 4(1)(a) probably does not achieve any more than saying that for controllers with establishments in different Member States, more than one set of national data protection laws may be applicable.

In effect, art 4(1)(a) lays down a two-stage test for applicable law: (i) does the data controller have an 'establishment' on the territory of an EU Member State, and (ii) does the controller process personal data in the context of activities of that establishment? If the answer to both questions is yes, then that Member State's implementation of the DPD will apply to such personal data processing, wherever in the world it takes place – whether outside or inside the EEA. In other words, if a controller's EEA branch or office (or other 'establishment') wishes to process personal data in the cloud in the context of that branch or office's activities, it must comply with the local requirements of the EEA country in which the branch or office is established when processing personal data, wherever in the world the processing takes place. To give an example, a cloud customer based in London and using a Brazilian cloud provider with servers in Portugal to process personal data must comply with the UK Data Protection Act (not Brazilian or Portuguese laws). The UK Act would equally apply if the London office processed the personal data using a Belgian cloud provider with servers in France.

The A29WP in its opinion on applicable law ('WP179')[27] considers that the notion of 'establishment' under the DPD should be guided by the jurisprudence of the European Court of Justice ('ECJ') regarding the freedom to provide services and freedom of establishment under art 50 of the Treaty on the Functioning of the European Union. ('TFEU'). The ECJ has clarified that 'establishment' requires at a minimum a staffed office with a degree of permanence and stability: 'both human and technical resources necessary for the provision of particular services are permanently available'.[28] Recital 19 of the DPD mirrors these requirements: 'implies the effective and real exercise of activity through stable arrangements' and the 'legal form of such an establishment (...) is not the determining factor'.

While it is clear that a branch office located in the EEA is an 'establishment', it seems that technical equipment such as a server located in a Member State would not count as a 'virtual' establishment.[29] However, use of such a server may trigger that Member State's data protection law under art 4(1)(c), discussed below.

2.1.2 In the context of activities

More opaque than the notion of establishment is the phrase 'in the context of the activities of an establishment of a controller'. The English language version ('context') contrasts sharply with some of the other language versions of the DPD, for example the German version ('Rahmen'/framework) or the French version ('cadre'/framework).

[27] n 18.
[28] Case C-168/84 *Bergholz* ECR [1985] 2251 [14]; Case C-390/96 *Lease Plan Luxembourg* ECR [1998]I-2553.
[29] WP179, text to fn 19: 'A server or a computer is not likely to qualify as an establishment as it is simply a technical facility or instrument for the processing of information'.

WP179[30] has stated three factors which should be taken into account:[31] (i) the degree of involvement of the establishment(s) in the activities in the context of which personal data are processed; (ii) the nature of the activities as a secondary consideration and (iii) the goal of ensuring effective data protection. It states that a 'who is doing what' test should be applied in the sense that the test requires a determination of (i) who carries out the relevant activities and (ii) whether there is data processing in the context of these activities. The involvement of the establishment in the activities is the most important of these factors.[32]

The *Google Italy* case is a good illustration of the wide interpretation of the phrase 'in the context of the activities of an establishment' by a national court in the EU. In this case Google executives were convicted of offences for infringing Italian data protection law in connection with a video uploaded to Google Video showing abuse committed against a disabled student.[33]

The first instance court judge decided that Italian data protection law was applicable to the case, since Google had an establishment in Italy. The judge came to this conclusion despite the fact that the data in connection with its Google Video services were not processed in Italy but on servers in the US/Ireland, despite the defence's assertion that decisions about content were not made in Italy and content was not hosted in Italy, and despite the fact that AdWord links were created based on users' choices (not by Google Italy) and AdWords links went not to the videos but to advertisers' websites.[34] The judge found that:

'(a) Google Italy was the 'operative and commercial hand' of Google Inc; (b) like other Google subsidiaries, it was substantially a part of the group operating as a single unit, under the direction of Google Inc; (c) Google Italy had the possibility of linking advertising to the videos using the service Google AdWords.'[35]

It seems that the judge assumed that since Google Italy participated in the activities of Google Inc, the processing was done in the surrounding circumstances (or context) of Google Italy's activities.[36] This argument somewhat puts the cart before the horse, as in reality the relationship is the inverse: the activities of Google Italy (which apparently do not involve data processing in relation to the videos, but other ancillary activities such as marketing) are carried out in the framework of Google Inc's activities, or perhaps those of Google's European headquarters in Ireland.

[30] n 18.
[31] WP179 (ibid), 14.
[32] WP179, 30.
[33] Tribunal of Milan, Sentenza n.1972/2010.
[34] G Sartor, MV de Azevedo Cunha 'The Italian Google case: Privacy, Freedom of Speech and Responsibilities of Providers for User-Generated Contents' (2010) 18(4) *International Journal of Law and Information Technology* 356-378, 363.
[35] Ibid.
[36] The Italian version of the DPD also refers to 'context', contesto.

The judge's view mirrors the statements of the A29WP in its Opinion on search engines.[37] According to this Opinion, processing is in the context of the activities of an EEA establishment even if the establishment does not carry out or direct any processing, and its role is limited to being responsible for relations with users of the search engine or the selling of advertisements in that jurisdiction, or the establishment complies with law enforcement requests with regard to user data. Such a wide view of 'context' arguably risks rendering 'context' as a connecting factor meaningless. In our view, although this seems implicit from art 4(1)(a)'s reference to an establishment 'of the controller', the notion of 'context' needs to be linked explicitly to the processing activities of the establishment *as* a controller who determines the purposes and means of that processing. However, if, for policy reasons, lawmakers wish the net of applicability to be as wide as the judge in the Google Italy case and the A29WP in WP148 cast it, then it would be better to delete the reference to 'context' altogether, given the confusion it causes. However, the draft Regulation art 3(1) would define its territorial scope by reference to the processing of personal data 'in the context of the activities of an establishment… in the Union', so, unless this wording is changed, the problem of determining when processing is 'in the context' of an establishment's activities will remain.

The wide interpretation of 'in the context of the activities of an establishment' may also be applied to a cloud provider with one or more establishments in the EEA. It has two consequences: (1) EU data protection law may apply even if no processing of personal data is carried out at the establishment, and (2) more than one establishment in the EEA may be involved in activities such as those mentioned in WP148 or the *Google Italy* case, so that the controller is subject to two different national implementations of the DPD.

For example, a large and diverse multinational cloud provider may have offices in the EEA, say in Rome and Dublin. It provides cloud data storage facilities to businesses and consumers in the EEA, but all the data processing in respect of these facilities is managed and carried out in the US and India. Users enter into contracts for cloud services directly on the web. The provider's EEA offices are involved in software development activities and marketing. This raises the possibility that the software company has to comply with both Italian and Irish data protection laws, by analogy with the interpretation advanced in the *Google Italy* case and the A29WP's interpretation. This would be a strange result, probably not intended by the original drafters of the DPD. The applicability of two sets of law which may in some respects contradict each other is an extremely undesirable consequence of this interpretation of art 4(1)(a). In a cloud computing scenario (as in the Google search engine scenario), it is more likely that the cloud provider has establishments in a number of Member States which carry out ancillary or indeed core functions, so that multiple and conflicting data protection laws may be applicable.

The A29WP attempts to address the problem of multiple laws applicable to the same act of processing by saying that controllers may engage in several activities - so for each activity it will be necessary to decide which establishment 'owns' this activity, before a decision can be

[37] Article 29 Working Party, *Opinion 1/2008 on data protection issues related to search engines, WP 148* (2008) ('WP148'), 10.

made on applicable law: ‘their practical behaviour and interaction which should be the determining factors: what is the true role of each establishment, and which activity is taking place in the context of which establishment? Attention should be paid to the degree of involvement of each establishment, in relation to the activities in the context of which personal data are processed.’[38]

While this approach seems logical at first sight, this may be unworkable, as activities will overlap (service improvement, advertising, local and central marketing campaigns, profiling etc may all involve the same acts of data processing). This is acknowledged but not solved in the Working Paper: ‘situations where the same database can be subject to different applicable laws do increasingly happen in practice.’[39] ~~In revising the DPD it would be helpful if the European Commission were to consider this issue of national conflicts, with a possible solution being the application of a ‘country of origin’ principle across EEA Member States as in the ECD, to deal with intra-EEA conflicts.~~[40]

In revising the DPD the European Commission considered this issue of national conflicts, proposing a concept of 'main establishment' to deal with intra-EEA conflicts where there are establishments in multiple EEA states. The draft Regulation would introduce a concept of ‘main establishment’ which, for a controller, means 'the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place.' It provides for 'the supervisory authority of the main establishment' to supervise all processing activities in all Member States, where 'the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union'.

However, these provisions seem to perpetuate the concepts of 'establishment' and 'context of activities', without clarifying adequately their meaning and application. For example, could an EU data centre of the controller, whether owned by the controller or a cloud provider, be a 'main establishment'? Recital 27 does state that 'the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment'. However, their relevance still needs further explication, particularly where no 'main decisions' are taken in the EU. In particular, are EEA data centres or EEA providers 'establishments' for this purpose, and is their processing 'in the context of' their activities as 'establishments'?

Furthermore, new uncertainties are introduced. Are decisions 'main decisions' if they relate to the processing of personal data worldwide, or only in the EU? If the 'main decisions' are

[38] WP179, 15.
[39] Ibid.
[40] ~~Art 3 ECD.~~

taken outside the EU, but the controller has more than one 'establishment' in the EU, which EU establishment is the 'main establishment'? What does 'the main processing activities in the context of the activities of an establishment of a controller in the Union' mean, and how does it apply in this situation?

Within the EEA, a 'consistency mechanism' will apply where a supervisory authority intends to take measures regarding processing operations related to offering of goods or services to residents of several Member States, or to monitoring them, etc.[41] This should help promote consistency across the EEA, though the mechanism is likely to work quickly and effectively only if the relevant data protection authorities and the Commission are resourced adequately. The financial impact statement that accompanies the draft Regulation estimates that the European Commission will, without an increase in headcount, be able to implement the new consistency mechanism, carry out adequacy assessments of third countries and prepare implementing measures and delegated acts. The assumptions underlying this estimate are that the consistency mechanism will only be invoked 5 to 10 times per year, that there will be no more than 4 adequacy requests per year, and that the European Commission will handle up to 3 implementing measures per year. All three assumptions look optimistic as the draft Regulation would establish many circumstances in which the consistency mechanism may be triggered, the number of countries that are adopting data protection laws (and that may apply for an adequacy finding) is growing at an accelerating rate,[42] and no fewer than 30 of the 91 Articles of the draft Regulation would 'empower' the Commission to 'adopt delegated acts' or 'make decisions'.

2.2 International law

Art 4(1)(b) provides that a Member State's data protection law apply where the controller is not established on that Member State's territory, but its law apply by virtue of international law. This would be the case for example on a ship or aircraft flying under a particular Member State's flag.[43] This may be relevant for cloud computing if, for example, data centre facilities were to be set up on ships moored outside the territorial waters of any Member State using sea water to generate power and cool equipment. While this may sound futuristic, Google has obtained a patent in the United States for such data centres built on ships.[44] So ~~we~~in future there may well ~~see~~be data centres on ships moored outside territorial waters, with the possibility of flags of convenience being used for data protection law purposes.[45]

[41] Draft Regulation arts 3(1), 4(13) and 51(2); see also recitals 19, 27, 63-64, 97-98, art 34(5).
[42] See Graham Greenleaf, 'Global Data Privacy Laws: 89 Countries and Accelerating', Queen Mary School of Law Legal Studies Research Paper No 98/2012 (2012) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034> last accessed 9 February 2012.
[43] Ships could be moored in territorial waters, or outside territorial waters. If outside EU territorial waters, EU laws may not apply, but the laws of the flag state – which could be non-EU – could.
[44] See Larry Dignan, 'Google wins floating data center patent' (*Between the Lines*, ZDNet 2009) <http://www.zdnet.com/blog/btl/google-wins-floating-data-center-patent/17266> last accessed ~~5 September 2011.~~9 February 2012.
[45] Although other factors may influence server location, eg tax.

2.3 Equipment

The final ground on which a Member State may rely to apply its national data protection law to the provision or use of cloud computing services is contained in art 4(1)(c). Under this provision, if the data controller 'is not established on Community territory', the application of a Member State's data protection law may nevertheless be triggered if it 'makes use of equipment, automated or otherwise, situated on the territory' of that State for the purposes of processing personal data, unless the equipment is only used 'for the purpose of transit through' Community territory. Note that there is no requirement that the personal data processed has to relate to EEA individuals.

If a data controller uses equipment within art 4(1)(c) so that the relevant Member State's law applies, the data controller has to appoint a representative in the Member State concerned.[46] The role of this representative differs from Member State to Member State. In some Member States (eg Belgium, Netherlands and Greece) the representative may be subject to a fine for breaches, but in others the representative is not liable under civil or criminal provisions - hence the role of a representative is confined to communication and legal representation. The A29WP recommends harmonisation in respect of the role of the representative in the direction that data subjects should be able to exercise their rights against the representative.[47]

Prima facie there seems to be a gap in the applicability of the DPD if the controller has an establishment in a Member State, but does not engage in data processing in the context of that establishment's activities. For example a US cloud provider (providing data mining facilities for which it is the controller) operates an office in Poland for unrelated software development. This cloud provider also makes use of equipment (data centres) in several Member States for the purpose of its data mining service. It could be argued that the data processing in the context of the data mining service is not governed by art 4(1)(a) since the only activity of the Polish establishment is software development (and not data mining), hence the processing is not in the context of the activities of the Polish establishment. Secondly it could be argued that art 4(1)(c) does not apply since the cloud provider *is* established on the territory of a Member State, Poland.

The A29WP denies that there is such a gap in art 4, by interpreting the DPD to the effect that the unrelated establishment will be discounted: 'Article 4(1)(c) will apply where the controller has an 'irrelevant' establishment within the EU'.[48] In the example above, according to the A29WP the Polish establishment would not count when applying art 4(1)(c). The laws applicable would be those of the Member States in which the equipment (data centres) used are situated.

[46] Art 4(2) DPD.
[47] WP179, 23.
[48] WP179, 19- it nevertheless calls for a clarification of the issue in the ~~revised version~~revision of the DPD, ibid 30.

This raises the question of what is meant by 'equipment'. This need not necessarily be something solid, tangible or materially substantive.[49] The French[50] and German[51] versions of the DPD use the even wider expression 'means'. According to the A29WP this 'supports a broad interpretation of the notion of equipment',[52] more along the lines of 'means', to include even surveys or questionnaires.[53]

If a data controller makes use of hardware (computers, terminals, servers, storage hardware or data centres) within the territory of a Member State for the purposes of processing personal data, then that Member State's data protection law would apply.[54]

WP179 makes clear that 'it is not necessary for the controller to exercise ownership or full control over the equipment'.[55] But it is generally thought that the controller must have a degree of control over the equipment/means,[56] although WP179 seems to take a very broad view of 'making use': 'some kind of activity of the controller and the clear intention of the controller to process personal data'.[57] The question of control is relevant to the discussion of 'lights-out' data centres and the question whether they amount to equipment under art 4(1)(c) of the DPD, which is discussed further below.

An example from the UK arose in the *Douglas v Hello* litigation. In *Douglas v Hello (No 2)*[58] it was argued that using an ISDN line for transmitting photographs over the internet from New York to London was 'making use of equipment' in the UK[59] not merely for purposes of transit, with the consequence that a US photographer in New York could be a 'data controller' under the Data Protection Act 1998 through sending wedding photographs, ie personal data, digitally to London (which the recipient then sent to Spain where a magazine containing the photographs was printed). The English Court of Appeal considered that there was a 'good arguable claim' worth putting before a court regarding the interpretation of the legislation, 'which to some extent may be fact sensitive'.

The 'equipment' ground has frequently been criticised as being opaque and not workable for controllers established outside the EEA.[60] The A29WP also ~~acknowledges~~acknowledged that ~~the~~, as a result of the 'equipment' connecting factor ~~is that,~~ there may only be a limited connection with the EEA and that there is an obvious need for reform.[61] It ~~admits~~admitted that the ground has 'undesirable consequences' such as a possible universal application of EU

[49] Bygrave (n 21) 7.
[50] 'moyen'.
[51] 'Mittel'.
[52] WP179, 20.
[53] Ibid.
[54] WP148 (n 36) 10-11.
[55] WP179, 20.
[56] U Wuermeling, *Handelshemmnis Datenschutz* (Carl Heymanns Verlag 2000) 78.
[57] U Wuermeling, *Handelshemmnis Datenschutz* (Carl Heymanns Verlag 2000) 78 20.
[58] (CA) [2003] EWCA Civ 139 [45]-[47].
[59] See s 5(1)(b) Data Protection Act 1998, implementing art 4(1)(c) of the DPD.
[60] European Commission, *First Report on the Implementation of Directive 95/46/EC COM(2003)265 final* (2003), 17; Bygrave (n 21), 9.
[61] ~~WP179, 21.~~

law, but ~~recommends~~recommended the ground be retained in order to prevent the avoidance of EU data protection law where there is relevant infrastructure in the EU and only for certain data protection principles (such as legitimacy and security).[62]

For controllers not established in the EEA, the draft Regulation would apply based, not on concepts of equipment/means, but on whether they process personal data of EEA residents in relation to (1) the offering of goods or services to such data subjects (ie along the lines of a directing or targeting test), or (2) the 'monitoring' of their behaviour (a new way in which non-EEA controllers could be subject to data protection regulation).[63] This paper discusses these new tests further below.

3. Cloud computing and the long-arm reach of EU data protection law

~~We~~This paper now ~~discuss~~discusses specifically the possibility of customers and/or providers of cloud computing services becoming subject to EU data protection law under art 4, even if they are not established in the EEA, and even if they have no connection with the EEA other than one of the following situations:

(1) where a cloud provider which is a data controller saves cookies[64] or other data, or runs scripts or programs, on the computers, mobile phones or other equipment of its EEA-based users; or
(2) where a data centre located in an EEA Member State is used (perhaps along with non-EEA data centres and/or data centres located in other EEA Member States) for the provision of cloud computing services.

[62] ~~Ibid~~WP179, 21, 32.
[63] Draft Regulation arts 3(2), 25(2)(d), 25(3); see also recitals 20-21, 63-64, 105. Recital 21 expands on what is considered 'monitoring' - 'whether individuals are tracked on the internet with data processing techniques which consist of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes'. Such a controller must also appoint an EEA representative - in only one of the Member States concerned, rather than all of them - who interacts with EEA supervisory authorities (and is liable in the EEA for penalties - art 78(2)) - unless the controller is established in a third country ensuring an adequate level of protection, is a small or medium sized enterprise or public authority or body, or is 'only occasionally' offering goods or services to EEA residents - art 25, recitals 63-64. Such a controller (and indeed, processors) must also appoint an independent data protection officer to assist it internally on compliance, if it is in the public sector, is a large enterprise, or (whatever its size) if its 'core activities' 'involve' processing operations which 'require' 'regular and systematic monitoring' - art 35(1), recital 75. A large enterprise is one that has at least 250 employees.
[64] Cookies are text files which are 'set', ie saved onto a user's computing equipment by the user's web browser, when the user visits a webpage with the browser and the browser automatically follows instructions sent by the web server to save the cookie. Cookies may be retrieved from the user's equipment and 'read' by the website on subsequent browser visits to the site. Cookies may also be set by Javascript or other scripts run by the browser, eg after automatically downloading the script from a visited webpage. Information saved in a cookie may be used for authentication, identifying a user session, saving user's preferences or shopping cart contents, or other purposes – A Barth, Internet Engineering Task Force (IETF), 'Request for Comments 6265 HTTP State Management Mechanism' (2011) ISSN: 2070-1721..

3.1 Cookies etc

This first scenario is not uncommon with SaaS. ~~Let us say~~Suppose that a non-EEA established cloud provider is the data controller[65] in respect of personal data processed in providing a particular cloud application, such as an online calendar service or social networking service. Would it have to comply with the implementation of the DPD in a Member State on the basis that it processes personal data by saving a cookie (or similar) or running a script on EEA-based users' computers? The A29WP has stated in several of its Opinions[66] that the 'installation'[67] of a cookie by a remote, non-EEA established service provider would amount to 'making use of equipment' in a Member State, hence triggering the application of that Member State's data protection law. In fact, in WP179, the A29WP refers expressly to a cloud computing scenario as an example of the application of art 4(1)(c). The example used is an online diary management system: 'if the service uses calculating facilities, runs java scripts or installs cookies' for the purpose of storing and retrieving and aggregating personal data then the cloud provider would have to comply with the data protection laws of the Member States where the users are located when the facilities etc are installed and used.[68] Therefore, if a cloud service requires the storage of a cookie or running of a script on the computer of an EEA based user for the purpose of processing personal data, this would be sufficient in the A29WP's opinion to trigger the application of EU data protection law.

In such a situation, the 'equipment' ground may lead to the application of 27 Member States' data protection law if the cloud service provider is the controller and provides services to users across the EU. This is obviously a practical problem for the controller, such as the requirement to appoint a representative in all those Member States. It affects all online services with EEA users which require the user to log in with a user name and password, if the login is handled by storing cookies on the user's computer (which most such services do). It also affects some services that do not require a login but still use cookies, such as many websites.

It is important to distinguish between cloud customers and cloud providers. The cloud customer may well be the controller of personal data (eg its clients' personal details) which it uploads to a cloud provider's service, but not all cloud services providers are controllers. Often a provider may not be a controller but merely a processor on behalf of its business customers, and indeed, in some cases, such as where its services are used only for raw processing power and not for persistent data storage, arguably it may be neither controller nor processor.[69]

Against this, it may be argued that the very act of storing a cookie or running a script on the user's equipment to process personal data is sufficient to make the provider a controller.

---

[65] See the discussion above.
[66] WP148 (n 36), 10-11; Article 29 Working Party, *Opinion 5/2009 on online social networking WP 163* (2009), 5, and WP179, 21.
[67] Ie setting.
[68] WP179, 22.
[69] CLP Controllers/Processors Paper (n ~~6).~~1).

However, much depends on the particular circumstances, which need to be analysed individually. A SaaS provider may offer a cloud application to end users which involves the storage of cookies or running of scripts, and the provider may therefore be the controller in relation to any personal data processed. However, in a multi-layered situation where the SaaS provider uses PaaS or IaaS to provide its service to end users, it would seem that only the SaaS provider should be considered the controller in relation to any personal data processed using the service – neither the PaaS nor the IaaS provider, which are mere infrastructure providers, should be considered controllers of that personal data, even if their services include tools which facilitate the creation and access of cookies etc.[70]

Furthermore, if a cloud customer who is an individual uses a PaaS or IaaS service which stores cookies on the individual user's computer in connection with their login to the service, the platform or infrastructure provider may be the controller of the individual user's account/login details. But if the user then processes personal data (eg of third party clients) using the PaaS or IaaS service, the provider should not necessarily be considered a controller of the personal data processed by the individual using this service.[71]

3.2 Data centres

The two questions to be answered in this section are (i) whether a data centre or server farm located in an EEA Member State (perhaps along with non-EEA data centres and/or data centres located in other EEA Member States) and used for the provision of cloud computing services may constitute an 'establishment' in the EEA and (ii) whether the use of an EEA data centre for providing or consuming cloud computing services constitutes 'making use' of equipment in the EEA. ~~We assume below~~This paper assumes that providers are at most mere processors; should a provider cross the line into 'controller', which would depend on the circumstances, then much of the discussion below regarding cloud customers who are controllers may apply to it also.

3.2.1 Data centre or third party data centre operator as 'establishment'?

Key to abbreviations:

Customer customer or user of cloud computing services, being an entity incorporated in a non-EEA country; Customer will usually be a controller of personal data.

Provider provider of cloud computing or related services.

DataCentreState data centre country, being here an EEA Member State in which a data centre used in cloud computing is located.

[70] Unless and until they access the data – ibid.
[71] Although in some circumstances the PaaS or IaaS provider might become a controller – ibid.

If Customer, an entity incorporated in a non-EEA country, runs a data centre in EEA State DataCentreState (but has no EEA offices, branches or subsidiaries etc), and uses the data centre to process personal data for Customer's private cloud, this raises the question of whether the data centre is an 'establishment' and whether the processing within the data centre is 'carried out in the context of the activities' of that establishment, so that State DataCentreState's data protection law applies to the processing.

As discussed above, the meanings of 'establishment' and 'established' in art 4 are not sufficiently clear, nor are they implemented consistently across Member States.[72] A server is unlikely to be considered an 'establishment' as 'it is simply a technical facility or instrument for the processing of information'.[73] However, a data centre comprises a building, normally with employees to maintain the servers, power, cooling, physical security etc. If Customer owns the building and employs those employees, it seems more likely that the data centre would be considered an 'establishment' of Customer.

Next, recall that an entity which operates equipment within a data centre, in order to provide cloud computing services, does not necessarily have to own the building and/or the equipment. If Customer rents space in the data centre of a third party provider, Provider, which runs a data centre in the EEA, eg a room, cage, rack space, the question arises whether this would amount to an establishment of Customer. How much space – a building, five racks - would amount to an establishment? If a single server is not an establishment, but a data centre may be, where should the line be drawn? What if Customer rents use of servers in Provider's data centre, but Customer does not own the servers? And does it matter whose employees maintain Customer's servers – Provider's, or Customer's own? What if third parties own and operate the data centre, but for the sole benefit of Customer, ie as a dedicated private cloud managed by a third party? Does that make the data centre an 'establishment' of Customer?[74] Many of these issues are relevant to data centres generally such as used in traditional outsourcing, not just cloud computing, and again clarity on these issues would be helpful.

---

[72] For example, the Dutch data protection authority seems to interpret 'established' in art 4(1)(a) to require incorporation under Netherlands law, thus applying Dutch data protection laws on the 'establishment' ground only to Dutch corporations, see Moerel (n 23). For an outline of several different national implementations of 'establishment', see Douwe Korff, *New Challenges to Data Protection Working Paper No 2 - Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments* (European Commission, 2010) 27-29.

[73] WP179, 12.

[74] In one case on freedom of establishment, an English bookmaker Stanley had commercial agreements with Italian operators or intermediaries relating to the creation of data transmission centres to make electronic means of communication available to Italian users, collect and register users' intentions to bet, and forward them to Stanley in the UK. The ECJ considered that these arrangements involved Stanley having a presence, indeed 'agencies', in Italy, and that: 'Where a company established in a Member State (such as Stanley) pursues the activity of collecting bets through the intermediary of an organisation of agencies established in another Member State (such as the defendants in the main proceedings), any restrictions on the activities of those agencies constitute obstacles to the freedom of establishment'. Case C-243/01 *Gambelli e.a.* [2003] ECR I-13031 [14], [46].

But even if a data centre can be considered to be an 'establishment' of Customer, the question arises whether the processing performed within its servers and other equipment is carried out 'in the context of' Customer's activities. Again, this concept is not harmonised across the EU and some Member States have failed to implement this criterion.[75]

On the one hand, if a data centre is 'an establishment', then in a sense *all* personal data processing conducted using its equipment could be said to be 'in the context of' its activities, because the very function of a data centre is to provide facilities to process data. On the other hand it could be argued that a data centre has no independent activities of its own, hence it never processes data 'in the context of' *its* activities. Arguably the processing within a data centre should be considered as a purely 'passive' technical activity, carried out in the context of *other*, 'real', activities of the controller *as such*. It could be said that the processing is carried out *as* the activity of the data centre as processor, not *in the context of* its activities as controller, and therefore that the technical processing within the data centre is not a 'real' exercise of activity within recital 19.

This view seems to be supported by two hypothetical examples given in WP179. The first involves a controller established in Austria which outsources processing to a processor in Germany: 'The processing in Germany is in the context of the activities of the controller in Austria. That is to say, the processing is carried out for the business purposes of, and on instructions from the Austrian establishment. Austrian law will be applicable to the processing carried out by the processor in Germany.' This example suggests that the 'context' considered is *not* that of the mere processor in Germany.[76]

The second example involves a Japanese-headquartered entity with an Irish office which deals with issues connected with the processing of personal data of its users, and a Hungarian data centre which processes and stores that personal data but is only involved in 'technical maintenance'. Here, WP179 states that the data centre should apply Irish law to the processing in the data centre, but Hungarian law to any processing of the personal data of the data centre's employees.[77] This example is relevant to the situation where a non-EEA entity uses its own data centre located in the EEA to process personal data, ie self-hosted private cloud. It is also relevant to where a non-EEA entity has a sales office, for instance, established in the EEA, in the context of whose activities no personal data ~~is~~are processed, but it also has a data centre in the EEA processing personal data in the context of its non-EEA activities.

[75] There is no requirement for 'context' in the laws of Finland, Greece and Sweden, while Austria's law applies simply to 'processing of personal data in Austria' - European Commission, *Analysis and impact study on the implementation of Directive EC 95/46 in Member States* (2003) 6 and Lilian Mitrou, *New Challenges to Data Protection Country Study A.5 – Greece* (European Commission, 2010) 6-7. Italy's law applies to 'processing of personal data, by anyone, carried out on the territory of [Italy]', Denmark's law to activities by a Denmark-based controller, but only if those activities 'are carried out within the territory of the European Community'. Korff (n 68) 28.

[76] If Austrian and German laws conflict, however, German law would apply as regards the security requirements – see section 4 below.

[77] 16-17.

The second example implies that processing of personal data within a data centre should not be treated as being in the context of its own activities as data processor, but only in the context of other, 'real', establishments' activities; and, taking the example to its logical conclusion, if the data centre owner has no other 'establishment' in the EEA which carries on 'real' activities, the 'establishment' ground should not apply at all.

The data centre, in other words, is an 'irrelevant' establishment, even if it is an 'establishment'.[78] The point here is that, for the purposes of applying the equipment ground under art 4(1)(c), the A29WP attempted to introduce the concept of a 'relevant' establishment in order to address the possible lacuna in art 4(1)(c) previously discussed. Art 4(1)(c) only applies if the controller is not 'established on' Community territory. WP179 interpreted art 4(1)(c) as referring only to a 'relevant' establishment.[79] Thus, even if a controller has an EEA establishment, that establishment would be discounted, and art 4(1)(c) would be applied, unless it is a 'relevant' establishment. In considering 'relevance', the A29WP effectively used the 'context of activities' test from art 4(1)(a). In other words, if an EEA establishment does not process personal data 'in the context' of its activities, it is not considered a 'relevant' establishment.

~~We argue~~This paper argues that if an EEA establishment is considered not to be processing personal data in the context of its activities, and therefore is an 'irrelevant' establishment for the purposes of art 4(1)(c), it should equally be considered not to be processing personal data in the context of its activities for the purposes of art 4(1)(a). 'Context of activities' should be approached consistently under both sub-paragraphs. Say that certain processing is *not* considered to be 'in the context' of an establishment's activities for the purposes of art 4(1)(c), which means it is not a 'relevant' establishment for that purpose, therefore the equipment ground is not disapplied. In that situation, if in fact no 'equipment' is used, it should not be arguable that the same processing by the same establishment *is* nevertheless 'in the context' of its activities so as to apply data protection jurisdiction under the art 4(1)(a) establishment ground.

The same reasoning, in relation to the processing in a data centre not being in the context of the data centre owner/operator's activities, holds true if the non-EEA entity does not have any office or other establishment in the EEA, but only a data centre in the EEA (eg for a self-hosted private cloud). In relation to a 1-person office, WP179 considers[80] that it should be 'actively involved in the activities in the context of which the processing of personal data takes place' in order to be an establishment. This approach supports the argument that a data centre is not an 'establishment' of the data centre owner in relation to the processing occurring within the data centre, as the owner (and even the cloud service provider) is not actively involved in the processing activities, which are controlled by the cloud user.

[78] See 3.2.3 below on 'relevant' establishment.
[79] Ibid.
[80] WP179, 12. Korff (n 68) 25 considers 'An agent used on an ad hoc basis is not an establishment of the controller but merely a "processor" (although if the arrangements between the controller and the agent become quasi-permanent, this could change)'.

Notwithstanding the implications of the Japanese/Hungarian example, WP179 generally takes a very broad view of 'context', as did the Italian court in the Google Italy case, and WP148.[81]On that wide view, Customer would have to comply with DataCentreState's data protection law in relation to personal data processing within the data centre in DataCentreState, even if the data were collected in Customer's own non-EEA country for its business in that country and related only to residents of that country. This uncertainty may discourage non-EEA persons from building EEA data centres, eg, to host their own private clouds. It is important to resolve these inconsistencies, and to clarify whether 'in the context of the activities of an establishment of the controller' includes a data centre's technical processing activities (when it performs no other economic activity), or whether the processing must be considered in the context of *other* distinct 'activities' of the controller.

Consider now another scenario where it is assumed that Customer uses a second data centre in another EEA State, and that personal data can flow back and forth between the data centres in DataCentreState and the other State, as may occur in cloud computing. If a data centre is an 'establishment' and the processing of personal data within it is considered to be 'in the context of' the data centre's activities, Customer may have to comply with the data protection laws of both DataCentreState and the other State in relation to the same personal data,[82] which may be difficult or impossible given that national laws differ and may even be in conflict. This might discourage the building or use of data centres in multiple EEA states.

Another scenario is where Customer engages the services of a third party provider, Provider. ~~We assume~~This paper assumes Provider is established in an EEA Member State, DataCentreState, and owns and manages a data centre in DataCentreState which is dedicated to Customer's use for Customer's private cloud.[83] In this scenario, it must be examined whether this third party data centre amounts to an establishment of Customer.

There is much ECJ jurisprudence on the meaning of 'establishment' in relation to freedom to provide services and freedom of establishment under art 50~~, Treaty on the Functioning of the European Union ('TFEU'),~~ TFEU, and the A29WP in WP179 considers that this jurisprudence provides useful guidance when interpreting 'establishment' under art 4.[84] Under that jurisprudence, an entity may in certain circumstances be considered to have an 'establishment' through having a third party agent in the territory concerned, and WP179 states that even a 'simple agent' may constitute an establishment 'if his presence in the Member State presents sufficient stability'.[85]

[81] n 36.
[82] See recital 19, text after n 27, above.
[83] Ie a dedicated managed private cloud, but this analysis could apply equally to a traditional IT outsourcing involving dedicated managed hosting using an EEA data centre.
[84] While acknowledging that 'it is not clear whether this and subsequent interpretations by the ECJ as regards the freedom of establishment under art 50 TFEU could be fully applied to the situations covered by art 4 of the Data Protection Directive' – WP179, 11. Moerel (n 23) suggests that it would be more appropriate to consider the jurisprudence on 'establishment' under the EU legislation on e-commerce and broadcasting.
[85] WP179, 12.

Furthermore, some Member States explicitly include agencies as 'establishments'. For example, the Irish Data Protection Act 1988 section 1(3B)(a) has as the jurisdictional ground '…the data controller is established in the State and the data are processed in the context of that establishment', and then defines 'established in the State in section 1(3B)(b) to include:

> '…(d) a person who does not fall within subparagraphs (i),(ii) or (iii) of this paragraph but maintains in the State -
>
> (I) an office, branch or *agency* through which he or she carries on any activity, or
>
> (II) a regular practice'.

Maintaining 'a regular practice' seems an even wider concept than agency. The UK data protection legislation is similarly broad,[86] while the French legislation seems broader still.[87]

There is therefore a risk for Customer that the dedicated third party data centre could be considered an 'establishment' of Customer. Based on the art 50 TFEU cases, the extent of Provider's independence may be a factor, so that the more tightly the cloud provider tries to control the third party data centre's activities (as seems more probable with private cloud), the more likely perhaps that it will be considered an establishment of the cloud provider.

~~We~~This paper now ~~consider~~considers the scenario where the cloud provider Provider is using someone else's infrastructure to provide cloud services for Customer – renting space in someone else's building, renting someone else's servers. If Provider rents a whole data centre, or simply space or server space within another's data centre, again similar questions arise as before as to whether the arrangement constitutes an 'establishment' of Customer, and there is again a need for clarity. Does the stability of the arrangement matter more than how it is provided? Is the arrangement considered more 'stable' if the whole data centre is dedicated to Customer, than if only part of it is?

Consider further the scenario where Provider is a subsidiary of Customer, incorporated under the law of DataCentreState. Assume Provider owns and runs the data centre in DataCentreState but does nothing else. Assume that, for Customer's business in its non-EEA country of incorporation, it is the controller of personal data, which are processed in Provider's data centre in DataCentreState. Does this involve processing 'in the context of the activities of an establishment of the controller on the territory of the Member State', so as to subject Customer to DataCentreState's data protection law for all personal data processing within the data centre?

Recital 19 explicitly states that a subsidiary with separate legal personality may be an 'establishment'. So again the meaning of 'context of the activities' is critical here. If the

[86] Section 5 UK Data Protection Act 1998 is in almost identical terms.
[87] Art 5(1) Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés: 'a controller is deemed to be established [in France] if he carries out an activity on French territory in the context of an establishment [*installation*], whatever the legal form [of that establishment]'. Translation from Douwe Korff, *New Challenges to Data Protection Country Study A.3 – Greece* (European Commission, 2010).

processing in the data centre in DataCentreState is considered to be 'in the context of' Customer's activities *in DataCentreState*, ie if Provider's activities in DataCentreState are attributed to Customer, then Customer as controller is subject to DataCentreState's law for the processing. However, if the processing is in the context only of Customer's activities *in its non-EEA country*, then arguably DataCentreState's law does not apply. In other words, treating a subsidiary of Customer as an 'establishment' of Customer seems to look through the corporate veil, equating the position to the one above where Customer directly owns a data centre in DataCentreState and uses it process personal data. But should not Provider's separate legal personality be recognised?[88] Should not the position be similar to that where Provider is an independent third party?

Again, as before, the laws of multiple Member States may be applicable if Provider has data centres in several states. Also, if Provider is incorporated in or has headquarters in yet other Member States, the (possibly conflicting) laws of those states may be applicable too. This position is not satisfactory.

~~We~~This paper now ~~consider~~considers the scenario where Provider has several unrelated customers, including Customer, all of whom Provider services using Provider's data centre in EEA Member State DataCentreState. Public cloud services providers typically have multiple customers.

It is possible that Customer may have less control over Provider here than when it is the only customer, although much will depend on the facts. With more independence for Provider, it is less likely that Provider would be considered an agency of Customer so as to cause Customer to have an establishment in DataCentreState. In other words, individual users may have less control, and the provider may be more independent of users, with public cloud, as compared to private cloud. Also, processing could occur in different servers at different times, not just servers dedicated to one user. Could this mean there is less stability for the user, making it less likely that the user (if non-EEA) has an EEA 'establishment'?

If Customer is nevertheless considered to have an 'establishment' through the 'agency' of Provider, does it matter if Provider is 'agent' solely for Customer, or if Provider is 'agent' for other customers too? Given that stability of the arrangements is the key issue, not exclusivity, it cannot be ruled out that Provider or its data centre might constitute an 'establishment' of *each* of its customers. Multi-tenancy should not affect the stability of each tenant's arrangements.

If so, then the same issue arises as above as to whether the personal data processing in Provider's data centre is considered to be in the context of 'an establishment' of a customer as controller, or whether it is only the activities of customers, *other than* the technical processing activities of the data centre, which should count when considering 'context'.

[88] C Kuner, European Data Protection Law: Corporate Compliance and Regulation (2nd edn, OUP Oxford, 2007)122 (d) – the DPD contains no concept of piercing the corporate veil.

The question also arises whether it makes it more likely that Customer has an establishment in the EEA if Provider offers a choice of geographical regions where its customers' data or applications are hosted, and Customer deliberately selects the EEA region for its services, so that Provider's data centres in the EEA (ie in DataCentreState) will be used to provide cloud computing services to Customer. The question here is essentially whether the ability for Customer to choose a region makes it more likely that Customer is deemed to have control, and therefore deemed to have an establishment in DataCentreState. What if Customer is not offered a choice of regions by Provider, but consciously decides to use Provider's services in the knowledge that Provider's data centres are located only in the EEA? To what extent, if at all, should that knowledge (or lack of it) affect the position?

Considering further another common public cloud scenario, what if Customer uses SaaS provided by a third party, which (through layers of other providers) is ultimately hosted on a data centre in DataCentreState? In this scenario, Customer would have much less fine-grained control of the computing service, as it will merely be using an application, and Customer may have no control at all over which data centres the third party provider chooses to use. Here, arguably it is least likely that Customer would be considered to have an establishment in DataCentreState. But to what extent, if at all, should the position be affected by Customer's knowledge (or lack of it) as to Provider's arrangements behind the scenes with other providers and/or their arrangements with the ultimate infrastructure provider? Finally, ~~we consider~~this paper considers the position of a so-called 'lights-out' data centre. This is a data centre that has eliminated the need for direct access by personnel under normal circumstances and is operated in an automated fashion, accessed and managed by remote systems. Would such a data centre trigger the application of the DPD under art 4(1)(a)? Does it matter who employs the security guards who may still patrol a lights out data centre? If the data centre is owned by the non-EEA entity Customer, and it employs the security guards and controls the processing that takes place within that data centre, it is possible that the data centre may be considered an 'establishment' of Customer. Should it make a difference whether such a data centre is dedicated to one entity, or is multi-tenancy? It seems stability and control are the key issues, and the discussions above would apply here. Whether or not such a data centre is an 'establishment, it may well amount to 'equipment' or 'means', which ~~we discuss~~is discussed next.

3.2.2 Data centre or data centre operator as equipment or means

~~We assume~~This paper assumes for now that Customer has no 'establishment' in the EEA.[89] While it is unclear to what extent a non-EEA user may be said to have an EEA 'establishment' through using an EEA provider or EEA data centre, it seems much clearer that a server is 'equipment' or means, and so is a data centre.[90] The key question then is,

[89] ~~We consider~~ This paper considers further below the 'transit through' exception and the condition that the 'controller is not established on Community territory'.
[90] WP148 (n 36) 11.

when will a non-EEA user be considered to 'make use of' an EEA server or data centre, so as to be within this ground?

As previously mentioned, WP179 considers that 'making use' involves two elements: (i) some kind of activity of the controller, and (ii) the clear intention of the controller to process personal data. These two elements are not helpful regarding the use of EEA data centres for processing personal data, as there the controller clearly intends to process personal data and will be carrying out activity, technical processing, within the data centre. Unfortunately, WP179 does not refer to an intention of the controller to process personal data *using EEA equipment or means* – although elsewhere in WP179, that is implied.[91] ~~We argue~~This paper argues that intention to process personal data using EEA equipment or means should be explicitly addressed. WP179 also states that while not every use of equipment within the EU/EEA will lead to the DPD being applicable, the controller need not exercise ownership or full control over the equipment for the processing to fall within the DPD's scope. The equipment should simply be 'at the disposal of the controller for the processing of personal data'. [92]

Should this ground apply, another uncertainty arises regarding the extent of its application, which WP179 acknowledges: 'It could be questioned whether the principles will only be applicable to the part of the processing taking place in the EU, or to the controller as such, for all the stages of the processing, even those taking place in a third country. These questions have particular significance in network environments such as cloud computing, or in the context of multinational companies.'[93] WP179 then concludes that, if this ground applies, the full DPD should become 'applicable to the controller as such, for all the stages of the processing, even those taking place in a third country'. This includes the data export restrictions, even though WP179 notes the implications are problematic.[94]

If Customer owns or rents a data centre in Member State DataCentreState for its self-hosted private cloud, it is clear that Customer makes use of equipment in the EEA for processing personal data, and that therefore the personal data processing taking place within that data centre is subject to DataCentreState's law, including data export restrictions – even if the data does not relate to EEA residents, and originated outside the EEA. There is no 'context' requirement here, unlike with the 'establishment' ground.

Non-EEA entities therefore risk becoming subject to EEA data protection law in relation to personal data they process using EEA data centres, even if collected outside the EEA.

---

[91] See text to n 105.
[92] Article 29 Working Party, *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites*, WP 56 (2001) ('WP56') 9.
[93] 24.
[94] 25. Kuner (n 84) 4.33 discusses a view that if an EEA Member State's law applies to a non-EEA person by virtue of art 4, the data export restriction should not apply, as the purpose of the restriction is to ensure that substantive data protection law requirements apply to the data, and that person will be bound by those substantive laws under art 4 so transfer of the data to it should not be restricted.

If Customer has data centres in multiple EEA Member States, and personal data flows between them, it would seem that the laws of each of those states will apply to the processing of that data.

Whether Customer owns or rents a data centre, rack space or servers in a data centre is immaterial for the purposes of this ground – it is clear from WP179, above, that EEA data protection law would apply irrespective of ownership status, if Customer directly uses equipment in the EEA.

Next, ~~we consider~~this paper considers the scenario where Customer has no EEA presence, but uses the services of a third party provider Provider, an EEA entity which hosts and manages Customer's private cloud on Provider's data centre located in EEA Member State DataCentreState.[95] Again, ~~we assume~~this paper assumes that the data centre is dedicated to Customer and its data, and does not host the data of any of Provider's other customers.

Through engaging Provider, is Customer using 'equipment' or 'means' in the EEA? Of interest here is the March 2011 decision by the French data protection authority, Commission nationale de l'informatique et des libertés (CNIL), in relation to use of French *processors* by non-EEA persons. In CNIL's view, non-EU entities who use the services of providers located in France to process personal data are thereby using 'means'[96] situated in France, and therefore are subject to the French Data Protection Act.

However, the CNIL wanted: 'to be realistic and pragmatic in applying the French law to such situations. The aim is to ensure a high level of protection of personal data while, at the same time, generating practical solutions in order not to hamper the development of service provisions propositions by French companies'.[97] Therefore, the CNIL decided to exempt from certain obligations the processing of certain types of personal data for limited purposes, when it is performed by French service providers on behalf of controllers established outside the EU, and to allow transborder data flows "back" to these non-European companies.[98]

The risks to data subjects' privacy resulting from these transfers were considered to be limited as those non-European companies collected the personal data in their own country, ie outside the EU. However, the non-EU controller remains liable for any breaches of French data protection law, and must appoint a representative in France. Also, the contract between the non-EU controller and French data processor must stipulate the processor's security and

[95] Again this discussion could apply equally to a traditional IT outsourcing.
[96] Indeed, the CNIL considers that if a controller established outside the EU sends a paper form to a data subject in France, the form constitutes a "means" used to process data. Korff (n 68), 30.
[97] CNIL,'CNIL facilitates the use of outsourcing services performed in France on behalf of non-European companies' (CNIL, 2011).
[98] Délibération n° 2011-023 du 20 janvier 2011 dispensant des traitements automatisés effectués sur le territoire français par des prestataires agissant pour le compte de responsables de traitement établis hors de l'Union européenne et concernant des données personnelles collectées hors de l'Union européenne (dispense n° 15) (2011) – ie the processing of personal data relating to employees, clients and prospects, for the purposes of managing payroll, employees, clients and prospects. is exempt from obligations of: notification, authorisation by the CNIL of data transfer back outside the EU, and (if it would involve disproportionate effort) informing the data subjects about that processing.

confidentiality obligations and require the processor to act only on the controller's instructions (ie the art 17 requirements), and in particular a policy to secure and control access to the data must be implemented.

The CNIL decision seems applicable to French data centres as well as French providers, whether for private or indeed public clouds, as it refers to 'means' situated on French territory, ie if Provider is not itself a French entity but uses a data centre located in France, it seems that the exemptions under the decision may also apply.[99] However, the decision refers explicitly to the use of a provider, so it does not seem to apply to the previous scenario where a non-EEA entity directly uses a French data centre or servers in a French data centre rather than going through a provider, although logically the same policy reasons apply there.

The CNIL decision is limited to French data protection law, and as stated may be understandable for pragmatic reasons, although it could be queried whether the DPD in fact permits Member States to allow such exemptions.

What about the position in other EEA Member States? WP56 considers that the controller 'makes use of' equipment 'if the controller, by determining the way how *[sic]* "the equipment works, is making the relevant decisions concerning the substance of the data and the procedure of their processing: "In other words, the controller determines, which data are collected, stored, transferred, altered etc., in which way and for which purpose"'.[100] That last sentence in particular does not seem to add anything as a controller, by definition, determines what data to collect and store, what analyses to perform on the data, etc. Also, the sentence 'by determining the way how the equipment works, is making the relevant decisions' is unclear and does not assist, because the controller does not necessarily determine how the equipment works, even if it is using a local computer to process personal data. There are issues regarding whether Provider is a controller (rather than processor) because Provider, although engaged by Customer, determines 'means' used (ie its data centre in France).[101] But ~~if we assume~~assuming that only Customer is the controller, it still seems likely that Customer would be considered to be using 'equipment' in the EEA.[102]

Directly relevant is WP179's statement that 'outsourcing activities, notably by processors, carried out in the EU/EEA territory on behalf of controllers established outside EEA may be considered as "equipment"'.[103] On this basis, Customer would be using equipment in the EEA. Nevertheless, WP179 suggests that 'account should be taken of the sometimes

[99] Whether, if Provider is incorporated in another EEA Member State, that State's laws also apply (on the 'establishment' or 'equipment' ground), is another matter, depending on that State's national implementation of the DPD.
[100] WP56 (n 88), 9.
[101] See the CLP Controllers/Processors Paper (n ~~6).~~1).
[102] Even if Provider were considered a controller, that would not exclude the possibility of Customer (who remains a controller) still being considered to use equipment in the EEA through Provider.
[103] Assuming that Customer has no establishment in the EEA in the context of which such personal data processing is taking place. Or in the words of WP179, 20, 'provided they are not acting in the context of the activities of an establishment of the controller in the EEA - in which case art 4(1)(a) would apply.'

undesirable consequences *[such as a possible universal application of EU law[104]]* of such an interpretation, as developed below in III.4: if controllers established in different countries over the world have their data processed in a Member State of the EU, where the database and the processor are located, those controllers will have to comply with the data protection law of that Member State'. It goes on to state that 'A case-by-case assessment is needed whereby the way in which the equipment is actually used to collect and process personal data is assessed.'[105]

Given these statements and the A29WP's consistently-held view that saving cookies on EEA residents' computers 'makes use' of equipment in the EEA,[106] it seems probable that use of an EEA data centre in cloud computing will bring the user within the scope of the DPD. If the data centre's computers are used to analyse or data mine, rather than passively store, personal data, that might perhaps make EU regulators even more inclined to consider the controller within scope even if the data are collected elsewhere. More clarity on the significance of 'the way in which the equipment is actually used' would be helpful. Similarly, with a 'lights out' data centre, it is the location of the data centre used which determines the position, rather than the location of the place from which the controller controlled the processing occurring within the data centre.

There is also a possible issue if Provider is a subsidiary of Customer, incorporated in another Member State. It appears that in the Netherlands, a subsidiary incorporated in the State is itself considered to be 'means' in that Member State under art 4(1)(c), so that the Dutch data protection authority would apply Dutch law to, say, a US corporation processing data in the US, if it has a Dutch subsidiary.[107] If the State in which Provider is incorporated is a Member State which takes this view, Customer could be considered to be using means in both DataCentreState and the other State, and thus be subject to the laws of all those States in relation to the same processing.

~~We~~This paper now ~~consider~~considers the scenario where Provider has a data centre in another EEA Member State, and personal data can flow back and forth between the data centres in DataCentreState and the other State.

Here, if Customer can be considered to be using equipment in the EEA (as discussed above), it seems that it would be using equipment in both DataCentreState and the other State, with the result that both states' laws apply to the processing.

One further question that might arise is whether Customer can be said to be making the 'relevant decisions' to use the data centres in both DataCentreState and the other State – or is that decision only Provider's, regarding automated load balancing between its data centres? On the basis of current law and practice it seems likely that regulators would still simply attribute the use of data centres in both Member States to Customer.

---

[104] WP179, 31.
[105] Ibid 20.
[106] WP56 (n 88), WP148 (n 36) 10-11, WP179.
[107] Moerel (n 23), paragraph containing fn 78.

What if more layers are involved in this scenario? What if Provider is not incorporated in the EEA (or even if it is), and Customer does not know that Provider intends to use an EEA data centre to process personal data for Customer? Would Customer be considered to make use of EEA equipment then? This example typifies the 'cloud of unknowing'.

WP179 expressed the view that 'The application of the DPD to a controller for the whole processing should be supported as long as the link with the EU is effective and not tenuous (such as by almost inadvertent, rather than intentional, use of equipment in a Member State).'[108] Would multiple layers of providers mean the link is 'inadvertent'? What if the controller contractually restricts its provider from using any EEA data centre or provider, but the provider still does so in breach of contract - would that make the link tenuous enough?

The CNIL decision seems to be an example of a regulator taking account of 'sometimes undesirable consequences', by applying French data protection law to non-EEA controllers in a more limited fashion when the risks are judged to be lower, in an 'equipment' situation. It may signal the way towards a possible future EEA-wide approach to cloud computing, whereby fewer data protection obligations are applied to non-EEA controllers who process, in EEA data centres or through EEA cloud providers, personal data collected outside the EEA and returned to outside the EEA. Such an approach would, as the CNIL noted, help foster, or at least not impede, the development of services by EEA providers.[109]

More generally, WP179 suggests that a more specific connecting factor, taking relevant 'targeting' of individuals into account, could usefully complement the 'equipment/means' criteria for legal certainty, and could be considered in relation to the current revision of the data protection framework. ~~We discuss targeting~~Targeting and other possible solutions are discussed later.

Similar issues apply with public cloud.

If Provider provides a cloud service which uses physical infrastructure in the EEA, will Customer have the necessary intention to 'make use of' EEA equipment? This seems probable if Customer has the ability to choose the EEA region for its processing, and does so. It seems less likely if Customer does not make a selection, unless it can be said that, by not selecting, it knows and accepts that its data could be processed in an EEA data centre, depending on how the service has been structured.

As with the 'establishment' ground, more control may be possible with IaaS/PaaS than most types of SaaS. With most SaaS services, Customer cannot control which data centres Provider chooses to use to provide Provider's SaaS service, and Customer may not even know which data centres are used to provide services to it or to store its data. However, Customer may have more precise control with IaaS or PaaS, for example a choice of geographical regions, and generally cloud customers have more control over processing using IaaS/PaaS than with SaaS (although some SaaS services may also offer a choice of regions).

[108] 24.
[109] WP179, 32.

If a public cloud provider has multiple users, as is common, that should not of itself affect each user's 'making use' of equipment, unless perhaps it reduces each user's control. For EU data protection law to be applicable based on use of means or equipment, there is no requirement for the use to be exclusive. Each customer may be making use of means or equipment through Provider or its data centre.

The main relevance of Provider having one or more customers is that if Customer is Provider's only customer (or one of only a few), then perhaps, depending on the facts, Customer might be more likely to have effective control, and therefore be more likely to be considered to intend to 'make use of' Provider or Provider's equipment. The situation will depend on the particular facts, and a clearer test of 'make use of' is much needed.

If the infrastructure is shared, and the same physical server could be processing Customer's data one minute, and someone else's data the next, is the server sufficiently at Customer's 'disposal'? Or is it enough that potentially it could be used for Customer's processing? Again, clarity is needed regarding shared infrastructure and possibly transient use.

What if Provider is a non-EEA entity which uses another cloud provider Provider2 to provide its services to Customer (eg Provider is a SaaS provider using an IaaS provider Provider2), and it is Provider2 which chooses to use an EEA data centre for the processing? To what extent should Customer be taken to know that EEA equipment is being used, and to what extent should such imputed knowledge mean that Customer should be considered to be making use of EEA equipment? To what extent should Customer be required to investigate sub-providers? The more layers that are involved, the further removed this may be from Customer, but the position is far from clear.

It is unclear what significance, if any, should be attributed to Customer's knowledge of the data centre location(s), or to Customer's control over the locations used, and whether it chooses to select a location. For example, should Customer be deemed to know that its data will be processed in the EEA, even with SaaS, if Provider only has EEA data centres? Should Customer be required to investigate all the underlying layers?

Transit through

The 'equipment/means' ground does not apply if 'such equipment is used only for purposes of transit through the territory of the Community'.

The question then arises, could the processing of personal data in EEA servers or data centres be considered to be only for transit? In cloud computing the data may be moving from data centre to data centre, eg in a 'follow the sun' type of arrangement, [110] so that the personal data may not be permanently in EEA data centres. Can this be considered 'transit through'?

[110] Moving data processing to data centres which have the most available energy (eg solar power when the sun is shining, or a wind powered data centre when it is windy there), or to certain regions during working hours for those regions when employees are most likely to need to use the data –<http://en.wikipedia.org/wiki/Follow-the-sun> last accessed ~~5 September 2011.~~9 February 2012.

Much will depend on the facts, eg if the personal data are used for local customer support in the region, then it may not be likely to be considered in 'transit' through the region. Again, this issue needs to be considered carefully during the review of the DPD. In particular, perhaps data protection law requirements may be relaxed if the data relate only to non-EEA persons and the controller has no other EEA connection except that it (or its provider) uses an EEA data centre in cloud computing.

Another complication is that, as in other areas, this aspect has also been implemented inconsistently into national laws. Denmark, France, Italy, Luxembourg, Portugal and Sweden exempt transit through the European Community or EU, correctly; whereas each of Belgium, Finland, Ireland and the UK only exempt transit through its own national territory; and the laws of Greece, the Netherlands and Spain refer simply to "transit".[111] French law does not implement this exception at all.[112] Obviously, this issue ~~needs to be~~is not currently harmonised ~~too~~.

3.2.3 EEA establishment + use of equipment – the possible lacuna

As previously mentioned, there seems to be a gap in art 4. Art 4(1)(c) on equipment use only applies if the controller 'is not established on Community territory'. If the controller is so established but does not process personal data in the context of that establishment's activities, then the 'establishment' ground cannot be used to apply EU law to it; but neither can the EEA equipment/means ground, because it is established on Community territory. This might mean that a controller can avoid the application of EU data protection law.

To give a concrete example, ~~let us say~~suppose that Customer is 'established on Community territory' because it has a branch in an EEA Member State or a subsidiary incorporated there. The branch or subsidiary runs a data centre in the EEA, and Customer processes personal data for its business *in its non-EEA country of incorporation* using that data centre. If the data are not processed 'in the context of' the activities of the EEA establishment, ie the branch or subsidiary (as ~~we have~~ argued earlier), then the establishment ground does not apply. But, as Customer 'is established' on Community territory, the equipment ground does not apply either. So no EU data protection law would apply to the processing within that data centre. This is similarly the case if Customer directly owns a data centre in the EEA (without having any branches or subsidiaries there), and through that data centre is considered to be 'established on Community territory' but is not processing personal data 'in the context of' the establishment's activities. This possible lacuna may be due partly to inconsistent drafting: art 4(1)(c) refers to to 'established on', art 4(1)(a) to 'establishment of', and art 4(1)(c) makes no reference to context of activities of the establishment. If, instead of 'the controller is not established on Community territory', ~~art 4~~art 4(1)(c) had read, 'the controller does not have any establishment on the territory of a Member State in the context of whose activities it processes personal data', there would be no gap. The A29WP has, as mentioned above,

[111] Korff (n 68) 30.
[112] European Commission, *Analysis and impact study on the implementation of Directive EC 95/46 in Member States* (2003), 7.

effectively interpreted that provision in that way: if the controller does have an EEA establishment, but does not process personal data in the context of that establishment's activities, then it is an 'irrelevant establishment', to be ignored when considering art 4(1)(c).[113]

3.2.4 Establishment and equipment/means - summary

In summary, when a non-EEA entity, perhaps through several 'layers' of providers, ultimately processes personal data within an EEA data centre or through an EEA-incorporated provider, it is not clear when it should be considered, through the EEA data centre or EEA provider, to have an 'establishment' in the EEA. It may be more likely to make use of equipment in the EEA than to have an 'establishment'.

The risk for the non-EEA entity, whether on establishment or equipment grounds, seems greatest with private cloud where the non-EEA entity owns the data centre, or perhaps has a dedicated private cloud managed by a third party. However, it still exists even with public cloud, and seems greatest with IaaS, particularly if the entity chooses the EEA region, though it may decrease with PaaS and even more with SaaS, depending on the situation.

It may perhaps be that, with more layers of providers, the risk becomes remoter, but the role of the entity's knowledge (or not) of the ultimate use of EEA data centres or EEA providers, or its ability to opt for such use, is not sufficiently clear – in either 'establishment' or 'equipment' contexts.

The tables in the Appendix summarise some of the possible permutations, illustrating the complexity in practice of common real-life cloud computing situations.

4. Cloud service provider as data processor - local obligations

The final jurisdictional provision discussed in this paper is that contained in art 17(3~~)~~), which provides that a data processor established in a Member State must also comply with technical and organizational security measures mandated by the law in that Member State. Hence a data processor must comply with the security measures imposed by the law of the Member State where the controller is established and the security measures of the Member State where the data processor is established. So if a cloud customer who is a data controller is established in Member State A, but the data ~~is~~are stored by cloud providers as processors at various points in time in data centres (whether of the same provider or different providers) in five separate Member States, the security requirements of all five Member States would have to be complied with by the provider; and similarly if the customer is not an EEA entity but uses cloud services which employ data centres in more than one EEA Member State.

[113] Even so, ~~we are~~there still ~~left with~~remains the ~~difficulty~~difficult issue of what 'context' means and whether, if a data centre is an establishment, personal data processing taking place within its servers should be considered 'in the context' of its activities.

This is problematic since the security requirements vary considerably between Member States.[114] For example, in the UK the requirement is simply to take 'appropriate technical and organisational measures', whereas Italy has set out in detail what those security measures should be, eg for reuse of storage media, access to sensitive passwords, etc; Denmark requires internet transmissions of personal data to be encrypted, and Austria, as well as defining detailed minimum security measures, requires documentary records of those measures.[115] Where detailed security requirements conflict, the A29WP considers that the law of the processor's Member State should prevail, and be considered sufficient even if law of the controller's Member State imposes greater obligations. The A29WP has called for harmonisation of security requirements.[116]

The draft Regulation art 3 would expressly apply it to 'the processing of personal data in the context of the activities of an establishment of' a processor in the EEA. Therefore, cloud providers may become directly subject to EU data protection law obligations under the draft Regulation, unlike the current position. Although art 1(13) would clarify that a processor's 'main establishment' is its place of central administration in the EEA, which is clearer than the position with controllers, the current problems with interpreting 'context of' activities in relation to controllers' 'establishments' would now be extended to cloud providers as well as cloud users. This may deter non-EEA providers from building or using EEA data centres or EEA sub-providers. Indeed, conceivably, cloud providers with an EEA 'administration' may be subject to the draft Regulation's requirements if the processing is 'in the context' of its EEA establishment's activities, wherever in the world the processing activities take place, and even if they process personal data of only non-EEA residents. Thus, the draft Regulation may have the effect of deterring non-EEA cloud providers from setting up or retaining any 'establishments' in the EEA which may be said to be places of 'administration', such as EEA offices.

The draft Regulation in art 30 and recital 66 would also impose direct security obligations on processors, including making risk assessments. However, as argued in the CLP Controllers/Processors Paper, some cloud providers may not know whether data stored on their equipment by EEA users are 'personal data' or not. It does not seem appropriate to subject them to similar liabilities as providers who do know. Furthermore, art 26(4) would explicitly make a 'processor' liable as controller if it processes personal data 'otherwise than as instructed' by the controller. While this simply reflects the current position, the requirement for processors to 'act only on instructions' from the controller does not accommodate how cloud computing operates. Generally it is the controller itself who processes data using the provider's resources, rather than the provider actively processing data for the controller, so it makes little sense to refer to the controller 'instructing' the processor in relation to the processing.

[114] WP179, 25.
[115] Kuner (n 84), 5.137.
[116] WP179, 25.

Finally, the draft Regulation still would not fully address the position of processors. For example, its recital 39 acknowledges that processing 'to the extent strictly necessary for the purposes of ensuring network and information security' is a legitimate interest of controllers. However, it does not mention processors, or specify (as would be desirable) that such processing for security purposes would not render a processor a 'controller'.

5. An alternative approach: targeting/directing

The complexity and ambiguity of the provisions on applicable law has led to divergent and deficient implementation of these provisions in national law.[117] For this reason a study commissioned by the European Commission states: 'better, clearer and unambiguous rules are desperately needed on applicable law'.[118] The main recommendation of the Study is that both EEA and non-EEA controllers should have to comply with the data protection law of one Member State *only*.[119] This clearly would take away one layer of complexity (but only on the regional EEA level - it would not solve the wider international issues).

This recommendation ~~has been~~was taken up by the A29WP. In respect of the current reform of data protection law at European level ~~in the shape of a revision of the DPD~~, the A29WP cautiously ~~recommends~~recommended a shift to country of origin regulation, which the draft Regulation has taken up.[120] This would mean that all establishments of a data controller within the EEA would apply the same law, namely that of the controller's main establishment, regardless of where the establishments are situated. However the Opinion also ~~states~~stated that a pre-requisite to country-of-origin regulation is comprehensive harmonisation of data protection legislation, including the security obligations, and the draft Regulation aims to achieve such harmonisation.[121]

Furthermore the A29WP ~~accepts~~accepted that the 'equipment/means' connecting factor may be tenuous and hence ~~recommends~~recommended that the 'equipment/means' test be replaced by a directing/targeting test similar to the test in respect of jurisdiction in consumer contracts[122] contained in Regulation 2001/44/EC art 15 as interpreted by the ECJ in the *Pammer/Alpenhof* case.[123]

This issue is relevant to cloud services providers (typically SaaS providers) which are said to be brought within the scope of EU data protection law because they save cookies or run scripts etc on EEA residents' equipment.

---

[117] European Commission ~~(n *),~~'A comprehensive approach on personal data protection in the European Union' (Communication) COM (2010) 609 final (November 2010), 17.
[118] LRDP Kantor Ltd (n 16), [44].
[119] Ibid.
[120] WP179, 31. See also LRDP Kantor Ltd (n 16), 26. On the draft Regulation see n 16.
[121] Ibid.
[122] Ibid,
[123] Joined Cases C-585/08 and C-144/09, *Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG (C-585/08) and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09)*, judgment 7 December 2010 (not yet reported in ECR).

In *Pammer/Alpenhof* the ECJ had to decide whether a website operator directs its activities to a particular Member State. For this to be the case, the trader 'must have manifested its intention to establish commercial relations with consumers from one or more other Member States including that of the consumer's domicile'.[124] However the ECJ also pointed out that this does not mean that a consumer has to provide 'proof of an intention on the part of the trader to develop activity of a certain scale with those other Member States'.[125] The ECJ established a test of taking into account all circumstantial evidence surrounding the website and the trader's commercial activities in order to assess whether, objectively speaking the trader was targeting the consumer's domicile. The ECJ listed, by way of non-exhaustive examples and in the context of the two cases for preliminary references before it, the following factors[126]:

(i) the international nature of the activity

(ii) mention of itineraries to reach the place of the trader's establishment or a place where the service is provided

(iii) use of a language or a currency other than those used in the trader's place of establishment

(iv) mention of telephone numbers with an international dialling code

(v) marketing focused on the consumer's domicile, including keyword advertising or paying for other country specific referencing services

(vi) use of a top-level domain other than that of the Member State in which the trader is established

(vii) reference to an international customer base, for example through reviews, testimony and other circumstantial evidence.

One obvious missing connecting factor is the nature of the activities of the trader.

The A29WP ~~adds~~added to these factors: the delivery of goods or services in a Member State, and the accessibility of the service depending on the use of an EU credit card.[127]

A targeting/directing test to decide which Member State's data protection law is applicable may indeed be preferable to the establishment/equipment grounds set out in the current art 4. It would provide that a Member State's data protection law applies in respect of a particular processing of personal data if a controller directs its activities to that Member State and the processing occurs in the framework of these activities. In other words, this test would connect the processing to the activities of a data controller and connect the activities to the territory of a Member State or several Member States.

[124] [75].
[125] [82].
[126] [93].
[127] WP179, 31.

WP179 explicitly ~~proposes~~proposed the condition: '…that the activity involving the processing of personal data is targeted at individuals in the EU'.[128] It also makes the valid point that the law applicable to consumer contracts is determined by a similar targeting test, so it makes sense to apply a similar test to the law applicable to data protection, since consumer protection law and data protection law overlap to an extent[129] (for example in the area of unfair commercial practices).

To what extent would the draft Regulation improve the position in relation to cloud computing? The draft Regulation's proposed replacement of equipment/means with tests based on offering goods or services to EEA residents or monitoring their behaviour, as mentioned in the text to n 63 above, should result in clearer, less artificial tests. However, the challenge may transform into one of determining when a controller 'only occasionally' offers goods or services to EEA residents and the scope of 'monitoring' behaviour (for example, it seems to catch profiling, but not collection of personal data for the purposes of profiling).

The problems with any targeting/directing test are twofold: (i) that targeting is always a question of degree - how much targeting is required before the controller would be subject to a Member State's law (in the case of the draft Regulation, how much would be required to go beyond 'only occasionally'?) and (ii) burden of proof - who would have to show that a controller targeted a particular Member State?

As to (i), some cloud services may not be on their face be 'linked' to any territory at all - the services are provided online without reference to any particular territory, and the marketing strategy of the cloud provider may also be territory-neutral. Some cloud users may not consider territory relevant when choosing to use certain online services. This raises the question whether mere knowledge of the cloud provider (or any other online service provider) that its user base includes users domiciled in the EEA or is likely to include users domiciled in the EEA (because of the nature of the service, its attractiveness to EEA users and the volume of the activities) should be sufficient. Such an argument would be similar to the 'stream of commerce' cases in the US approaches to jurisdiction where a large manufacturer has constructive knowledge that its products may end up in a particular country through the chain of distributors.[130] ~~Similar~~Similarly, with online services which are ubiquitous and accessible from everywhere, it could be argued that the question of whether a particular service provider should be subject to the law of a particular country should depend on whether that service provider knows that it is providing services to users in that country.[131] How much knowledge is required before a provider crosses the line of 'only occasionally' offering cloud services to EEA residents? Is it significant that the draft Regulation refers to 'offering' rather than 'supplying', ie targeting or marketing rather than actual 'sales'?

[128] Ibid.
[129] Ibid, see also Bygrave (n21) 10-11.
[130] *Asahi Metal Industry Co v Superior Court* 480 US 102 (1987) - this case turned on whether there were sufficient minimum contacts, rather than knowledge as such and it concerned goods rather than services, but the rationale can be applied by analogy.
[131] For a similar argument see A MacDonald 'Youtubing Down the Stream of Commerce' (2009) 19 *Albany Law Journal of Science and Technology* 519-556, 552-556.

As to (ii), the cloud provider is in the best position to know about its marketing strategy and the operation of its service and its website, but it may be difficult to prove a negative (ie that it did not market its services in the EEA). The draft Regulation does not address the burden of proof, and would benefit from an explicit statement on the subject.

As regards the lacuna analysed above, the draft Regulation does not 'close the loophole' for controllers. Under art 3(1), the draft Regulation would apply 'to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.' Art 3(2) would then apply the targeting test 'to the processing of personal data of data subjects residing in the Union by a controller not established in the Union'. Therefore, if a controller is 'established in' the EEA, but is not processing personal data 'in the context' of the activities of any of its EEA establishments, the draft Regulation would not apply to it at all. It would be desirable if the draft Regulation could explicitly address this issue and clarify that 'established in' means the same as 'has an establishment in', as discussed above.

Interestingly, there is no similar loophole for processors. If a provider processes personal data 'in the context of the activities of an establishment' of the provider in the EEA, it seems it would be subject to the draft Regulation in relation to its worldwide processing.

6. Conclusion and recommendations

From the above discussions, it is clear that the DPD applies in two situations to a cloud customer who is a controller with its main headquarters outside the EEA, even if it processes the data outside the EEA: (i) where carried out in the context of activities of an establishment of the controller in the EEA, or (ii) if the controller has no establishment whatsoever in the EEA, if it uses equipment or means in the EEA for the processing of personal data. Hence, the territorial link is (i) an establishment, or (ii) equipment or means of processing. However, art 4 would benefit from clarification, especially as it applies to the use of EEA data centres or EEA providers, particularly where layers of providers are involved.

The current legal uncertainties need to be addressed if non-EEA entities are not to be discouraged from using EEA data centres, EEA providers, or indeed non-EEA providers which ultimately use EEA data centres. Policymakers need to consider, decide and set out clearly:

- in exactly what circumstances should a non-EEA entity be regulated because it uses an EEA data centre (or space/servers in a data centre) or an EEA provider, including the relevance of:
    - layers of providers,
    - the entity's actual or deemed knowledge (or not) about EEA infrastructure (or infrastructure in a specific Member State) being ultimately used, and
    - the entity's ability to choose (or not) whether EEA infrastructure should be used, and
- what regulations should be applied to such a non-EEA entity (if at all), such as when the personal data processed do not relate to EEA residents and do not originate from the EEA.

For understandable policy reasons, EU lawmakers consider that, in some circumstances, EU data protection jurisdiction should extend extra-territorially to non-EU service providers who process the personal data of EU consumers.[132] EU policymakers have signalled their intention to improve harmonisation across the EU, particularly as regards applicable law.[133]

The challenge is to define the boundaries involved, with sufficient clarity for practical application, and in a way that adequately balances the interests in protecting privacy and in fostering the EU-wide, and indeed global, development and use of cloud computing services by EU providers and users, and it seems apparent that the draft Regulation, while attempting to address some of the key issues, does not do so adequately.

~~There are significant precedents within the EU for an approach which focuses~~Notably, clearer rules are needed on the ~~location~~determination of ~~economic activities rather than the location of technological equipment, such as in relation to the ECD, insurance services and online gambling.[134] While these mainly focus on internet web servers rather than cloud computing servers, the principle should be the same in relation to data centres.~~

[132] Viviane Reding, 'Your data, your rights: Safeguarding your privacy in a connected world' (Privacy Platform 'The Review of the EU Data Protection Framework' Brussels, 16 March 2011) SPEECH/11/183.
[133] For example, Vivane Reding, 'The reform of the EU Data Protection Directive: the impact on businesses' (European Business Summit Brussels, 18 May 2011) SPEECH/11/349.
~~[134] ECD recital 19 provides:~~

> ~~The place at which a service provider is established should be determined in conformity with the case-law of the Court of Justice according to which the concept of establishment involves the actual pursuit of an economic activity through a fixed establishment for an indefinite period; this requirement is also fulfilled where a company is constituted for a given period; the place of establishment of a company providing services via an Internet website is not the place at which the technology supporting its website is located or the place at which its website is accessible but the place where it pursues its economic activity; in cases where a provider has several places of establishment it is important to determine from which place of establishment the service concerned is provided; in cases where it is difficult to determine from which of several places of establishment a given service is provided, this is the place where the provider has the centre of his activities relating to this particular service.~~

~~Similarly, see European Commission, *Interpretative Communication – Freedom to provide services and the general good in the insurance sector (2000/C 43/03)*, OJ C 43/5, 16.2.2000:~~

> ~~The Member State of establishment of the insurance undertaking with which a policy is concluded in this way is the Member State of establishment of the insurer that effectively comes on the insurance activity (head office or branch) and not the place where the technological means used for providing the service are located (e.g. the place where the Internet server is installed).~~

~~European Commission, *Green Paper on on-line gambling in the internal market* COM/2011/0128 final (2011) states:~~

> ~~According to the e-commerce directive[54], a company offering information society services is established where it pursues its economic activity. It is therefore neither the place where the technology supporting its website is located nor the place where the website is accessible. In cases where it is difficult to determine from which of several places of establishment a given service is provided, the place where the company has the centre of its activities relating to the particular service should be the deciding factor. Since a company can use one or multiple servers or a "cloud based"[55] infrastructure and since it can switch and relocate them within a very short period of time, a server cannot be considered a secure link to determine the company's place of establishment relating to a particular on-line service.~~

~~While a data centre is more than just a server, a company may equally be able to move its cloud services to use a different data centre just as easily.~~

~~It is hoped that,~~'main establishment' for ~~EEA~~ controllers~~, the data protection law reforms will provide for the applicable law to be that of a single country of origin, with clear rules as to how to that country of origin is to be determined. Substantive harmonisation of data protection laws would be a pre-requisite.~~

~~For non-EEA controllers, data protection law jurisdiction should be applied based on targeting by the controller of EU residents, along the lines of *Pammer/Alpenhof*, rather than over-stretching the meaning of 'equipment/means'. There is support for this approach as shown by WP179 and the above speech of Commissioner Reding.~~

. If the concepts of ~~establishment/equipment~~'establishment'/'context of activities' are to be retained, the meanings of 'establishment' and 'context' need to be ~~clarified.~~explained in much greater detail. In particular, ~~arts 4(1)(a) and 4(1)(c)~~art 3 of the draft Regulation should be amended to eliminate the inconsistent usages of 'establishment of' and 'established ~~on~~'in' and make it clear that both refer to the same concept~~;~~, to close the possible gap ~~in art 4(1)(c); and spell~~. It should be spelled out that a subsidiary is not ~~'means'~~ an 'establishment' of its parent, but (if applicable) a controller or ~~'equipment'.~~processor in its own right. It is important that the implications of using EEA cloud service providers or EEA data centres are made very clear. ~~National law conflicts should also be eliminated, particularly in relation to security requirements~~In relation to the targeting concept, more guidance is needed on when offering of services will exceed 'only occasionally', and the meaning and scope of 'monitoring'. It should be made explicit who bears the burden of proof on 'offering' and 'monitoring'.

Finally, the status of providers of the physical and software infrastructure, as well as intermediate providers, ~~would also benefit from clarification. Consideration should be given to whether specific provisions relating to processors are desirable~~require further clarification in order to reduce uncertainties for cloud service providers, for example when they are processing data for non-EEA controllers~~, or are themselves non-EEA entities which have no 'establishment' in the EEA other than data centres.~~. To what extent should they be subject to EU data protection law in relation to that processing~~, and how can they determine which Member State~~'s? The draft Regulation aims to eliminate national law ~~apply? Clear rules are~~conflicts and stipulate a 'main establishment' concept as the basis for regulating processors. This is laudable, much needed ~~for determining which State's~~, and particularly important in relation to security requirements ~~apply to processors, ie an equivalent~~. However, it is vital that the draft Regulation further clarifies the exact scope of ~~'establishment' for~~its applicability to processors~~.~~, and the same issues regarding 'context of activities' arise equally here. The 'instructions' requirement, and similar requirements relating to use of processors, do not take proper account of how cloud computing operates. If the intention is to impose EU data protection security requirements on processors having any EEA 'administration', regardless of the position or country of their controllers, this should be made explicit, and inappropriate provisions expressly disapplied.

Appendix - Practical application – use of EEA data centres

The tables below summarise the position of a non-EEA entity Customer, which for cloud computing services directly or indirectly uses data centres in the EEA (in Member State DataCentreState, or in some scenarios both Member States DataCentreState and another Member State). ~~We assume~~This paper assumes the 'transit through' exemption does not apply.

Key to abbreviations:

Customer customer or user of cloud computing services, being an entity incorporated in a non-EEA country; Customer will usually be a controller of personal data. ~~We assume~~This paper assumes Customer is incorporated and based in a non-EEA country, and collects personal data in that country for its business there, where the data relate only to residents of that country. ~~We~~This paper also ~~assume~~assumes Customer has no other presence in the EEA, unless otherwise stated.

Provider provider of cloud computing or related services.

DataCentreState data centre country, being here an EEA Member State in which a data centre used in cloud computing is located.

Multiple means several data centres in different EEA Member States are used, between which personal data may flow automatically.

~~We summarise~~This paper summarises in each alternative scenario whether EU data protection law could be applied to Customer, based on either the:

- establishment/context ground ('effective and real exercise of activity through stable arrangements'), or
- the equipment ground ('if the controller, by determining the way how the equipment works, is making the relevant decisions concerning the substance of the data and the procedure of their processing', and (i) some kind of activity of the controller, and (ii) the clear intention of the controller to process personal data).

If Provider is considered to determine 'purposes and means' of the processing so as to be considered a controller (for example through its choice of data centre(s) or any sub-provider used), then the analyses regarding Customer would apply to Provider.

Private cloud

	Type	Variations	Establishment and context?	Equipment?
1	Private cloud – self-hosted	A. If Customer owns the data centre/servers	Uncertain. There may be enough stability for an 'establishment', especially if Customer's employees maintain the servers. However, arguably the personal data processing within the data centre is not 'in the context' of the data centre's activities. The position is unclear.	Yes
		B. If Customer rents space/servers	As in 1A. Possibly, stability increases if Customer uses more space/servers, particularly if its employees maintain the servers. Conversely, arguably the number of servers/employees dedicated to Customer should not matter – nothing turns on the 'size' of an establishment, only whether there *is* an establishment. As above, the 'context' question is unclear.	Yes
		C. If Customer has an establishment O in the EEA, eg marketing office for hardware sales or software licensing	Arguably, same as above. However, the wide view of 'context' taken by the A29WP raises the risk that the processing in DataCentreState could be deemed to be in the context of ***O's*** activities.	This is the apparent lacuna in art 4(1)(c). WP179 would consider O to be an 'irrelevant' establishment, so that Customer is still considered to be making use of equipment in DataCentreState.
		D. Multiple	Uncertain. Either there is insufficient 'stability' in both DataCentreState and the other State, as data are not definitively in one centre or the other, or Customer has establishments in ***both*** states, subjecting the same processing to the laws of both DataCentreState and the other State. Whether the second data centre is used for full replication/backup or just for 'overflow' may be relevant. The context issue again arises here.	Yes, Customer would be subject to the (possibly conflicting) laws of both DataCentreState and the other State for the same processing, if the distributed processing employs equipment in both those states.
		E. Lights out data centre	Uncertain. Customer may still control processing operations in the centre, albeit remotely.	Yes

	Type	Variations	Establishment and context?	Equipment?
2	Private cloud – data centre dedicated to Customer, owned and managed by Provider	A. If Provider is incorporated/ established in DataCentreState	It is uncertain to what extent Customer may be considered 'established' in DataCentreState through a third party, eg Provider or Provider's data centre. Relevant factors may include the extent to which the data centre is dedicated to Customer, and the extent of Customer's control over activities therein through its contract with Provider (possibly Customer may be afforded greater control if it is Provider's only customer using that data centre). Again, the context question remains relevant.	Probably, although in a sense Provider also determines 'how the equipment works'. It seems that a case by case assessment should be undertaken to avoid 'undesirable consequences'.
		B. If Provider is incorporated/ established in the other State	Uncertain. Customer risks being considered to have an establishment in DataCentreState, through the dedicated data centre in DataCentreState; and possibly also in the other State, through using Provider's services, as Provider is incorporated in the other State. This depends on the national laws of DataCentreState and the other State. Again, the context question is relevant.	Very probably, in DataCentreState – see 2A. the other State's law determine whether Customer is using 'means' in the other State through its use of Provider, although the data centre is in DataCentreState.
		C. If Provider (non-EEA) has no other EEA presence	Uncertain. See 2A: could the data centre be attributed to Customer nevertheless, because it is dedicated to Customer? Again, the context question arises.	Very probably, in DataCentreState – see 2A. The processing is still conducted on EEA territory, ie DataCentreState.
		D. If Provider rents the data centre/ servers	Ownership should not matter, but it is unclear to what extent the number or proportion of servers/employees dedicated to Customer affects whether it has an establishment, see 1B.	See 2A. Ownership/full control is unnecessary. 'Intention' is, but activity in the EEA plus intention to process personal data suffices.
		E. Multiple	If Customer is considered to have an 'establishment' through Provider or the data centre, see 1D.	Yes, in both DataCentreState and the other State – hence, both their laws would apply to the same processing.
		F. If Provider is a subsidiary of Customer	Customer may be more likely to be considered to have an establishment through Provider if Provider is its subsidiary, in some states.	Customer would be using equipment in DataCentreState; but, if Provider is incorporated in a Member State that considers a subsidiary to be 'means', Customer risks being considered to use 'means' in that Member State also,

Public cloud[135]

	Type	Establishment and context?	Equipment?
3	Public cloud – Provider provides IaaS, PaaS or SaaS to Customer; Provider has server space in a data centre (or whole data centre)	Depends on type of service and exact nature of service, but generally use of IaaS may be more likely to constitute an 'establishment' of Customer than PaaS or SaaS, and Customer's knowledge as to use of EEA data centres and the extent of its control may be relevant. As above, it is irrelevant whether Provider owns or rents the data centre, space or servers. Similar questions as above arise on 'context', and, if Provider uses multiple EEA centres, on sufficient stability, and multiple laws possibly applying.	Depends on the service. Whether Provider owns or rents infrastructure is irrelevant. If Provider uses data centres in multiple EEA states and equipment use is attributed to Customer, multiple laws may apply to Customer.
4	Public cloud – Provider provides cloud services to Customer using Provider2's IaaS or PaaS service; Provider2 has server space or whole data centres	The EEA data centre is even more removed from Customer than in 3. Similar questions arise as in 3 as to the extent of Customer's control or knowledge of the use of Provider2's EEA data centres, but Customer would have to delve deeper into the cloud stack to find out. Should it be required to? Other issues are also similar eg context.	The extra layer may affect whether Customer has the necessary intention, but the position is unclear (see 2D). Knowledge that Provider2's data centres are in the EEA may be relevant, but the position is further removed.
5	Public cloud – Provider provides cloud services to Customer using Provider2's IaaS/PaaS service, which uses Provider3's IaaS service; Provider3 provides the servers in data centres	This illustrates that even more layers are possible, including a further layer still if Provider3 does not own the data centres but rents space/servers. As with 4, a key question is whether the further removed the data centre is from Customer, the less likely it is to be considered Customer's establishment. Again, context is an issue.	As 4, but the position is even further removed.
6	Lights out data centre	Depends more on type and nature of service, and layers between, than on whether the data centre is remotely controlled.	Depends on service and layers.

[135] The numbering is continued from the previous table for ease of reference.