scripted

Volume 9, Issue 1, April 2012

DATA EXPORT IN CLOUD COMPUTING – HOW CAN PERSONAL DATA BE TRANSFERRED OUTSIDE THE EEA? THE CLOUD OF UNKNOWING, PART 4

W Kuan Hon[*] *and Christopher Millard*[±]

Abstract

The lack of clarity and harmony across European Economic Area ("EEA") Member States of the data export rules under the European Union ("EU") Data Protection Directive ("DPD") gives rise to significant uncertainties relating to the use of cloud computing. The concepts of transfer and data location are especially problematic. An intense and narrow focus on data location made sense when data could be transported between countries only by physically carrying storage media across borders. With the inception of the Internet and the ease of remote access to data, the concept of "location" is increasingly meaningless as well as irrelevant to data protection.

The Directive's focus on data location should not obscure the underlying purpose of the data export restriction, namely data protection. The specific objective of this restriction was, and remains, to protect personal data against access by unauthorised persons (and unauthorised use, which depends on access). Where data are strongly encrypted and the decryption keys securely managed, the data's location should be irrelevant. Even if such encrypted data are stored outside the EEA, unauthorised persons would not be able to access the data in intelligible form without the key. Conversely, keeping data within the EEA does not guarantee better protection where data are stored unencrypted (or only weakly encrypted).

---

[*] Research Assistant, CLP. This paper forms part of the QMUL Cloud Legal Project ("CLP") available at http://cloudlegalproject.org, Centre for Commercial Law Studies, Queen Mary, University of London ("CCL"). The authors are grateful to Microsoft for generous financial support making this project possible. Views herein, however, are solely the authors'. The first three papers in this CLP data protection series covered personal data, responsibility for personal data in the cloud, and jurisdictional applicability of national laws implementing the DPD – see note 2 below.

[±] Professor of Privacy and Information Law, CCLS; Project Leader, CLP.

In this paper, we argue that the focus should be on restricting unauthorised access to intelligible data, rather than restricting data export. We suggest that the data export restriction should be replaced by requirements regarding accountability, transparency and security.

DOI: 10.2966/scrip.090112.25

1. Introduction

This paper considers how cloud computing is affected by the restrictions on transferring personal data outside the European Economic Area ("EEA") under art 25 of the Data Protection Directive 95/46/EC[1] ("DPD"), which we shall term "data export". We also suggest possible solutions to comply with or work around the data export restrictions, and make recommendations for future reform of the DPD. Various other key data protection law issues raised by cloud computing environments are addressed in related papers.[2]

The DPD aims to encourage the free movement of personal data within the EEA by harmonising national data protection provisions, while protecting the rights and freedoms of individuals ("data subjects") when their "personal data" is 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.[3] A controller may use a

---

[1] *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* [1995] OJ L281/31. The DPD extends to non-EU countries within the EEA, namely Iceland, Liechtenstein 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 L296/41, 23.11.2000. Hence, we generally use the broader "EEA" instead of "EU" in this paper.

[2] This paper forms part three of a four-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 three papers covered:

- personal data: W Hon, C Millard and I Walden, "The Problem of 'Personal Data' in Cloud Computing: What Information is Regulated?—The Cloud of Unknowing" (2011) ("CLP Personal Data Paper") available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1783577 (accessed 22 March 2012) and W Hon, C Millard and I Walden, "The Problem of 'Personal Data' in Cloud Computing: What Information Is Regulated?--the Cloud of Unknowing." (2011) 1/4 *International Data Privacy Law* 211–228;
- responsibility for personal data in the cloud: W Hon, C Millard and I Walden, "Who is Responsible for 'Personal Data' in Cloud Computing?—The Cloud of Unknowing, Part 2" ("CLP Controllers/Processors Paper") http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1794130 (accessed 22 March 2012) and W Hon, C Millard and I Walden, "Who is Responsible for 'Personal Data' in Cloud computing?--The Cloud of Unknowing, Part 2." (2011) 2/1 *International Data Privacy Law* 3-18; and
- the applicability of the DPD to cloud computing actors and the jurisdiction of data protection authorities to regulate them: W Hon, J Hörnle and C Millard, "Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3" (2011) ("CLP Applicability Paper"), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1924240 (accessed 22 March 2012).

[3] This paper will not discuss the DPD's applicability to an entity through its having the requisite EEA connection – discussed in the CLP Applicability Paper, see note 2 above.

"processor" to process data on its behalf. The DPD does not apply to certain matters,[4] where member states' national implementations may, for example, allow exemptions from certain obligations. Important national differences in data protection laws exist, such as on civil liability and penalties for non-compliance.[5] We address the DPD only at an EU level, although illustrative national examples will be given.[6]

In January 2012 the European Commission published a package of proposals including a draft General Data Protection Regulation (the "Regulation") which would replace the DPD. Cloud computing was cited as one of the factors driving reform, with the aim of producing a robust and coherent EU regulatory regime to ensure effectiveness of data protection and engender trust for cloud services providers.[7] The proposed reforms will take time to be enacted, take effect only another two years thereafter, and are likely to be amended in the legislative process. Our analyses 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 the restriction on data export is not appropriate in the internet age, and should be abolished and replaced by other more suitable controls.

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 (and references in this paper to "EU Data Protection Laws" are to the relevant national legislation, unless otherwise stated). This means that data protection laws may be, and indeed have been, implemented inconsistently in different Member States. The data export restriction is one key area where neither implementation of the DPD nor application of its requirements has led to adequate harmonisation, leading to practical difficulties.[8] Our analysis below is complicated by this lack of harmonisation. Space does not permit coverage of all Member States; we focus on the DPD and EU regulators' collective views (in the form of the Article 29 Working Party ("A29WP")[9]), 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

---

[4] E.g. national security, defence - art 3(2).

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

[6] For the text in English of various EU and other countries' national legislation governing transborder data flows, see C Kuner, *Table of Data Protection and Privacy Law Instruments Regulating Transborder Data Flows* (2011) available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1783782 (accessed 22 March 2012).

[7] European Commission, "Data Protection Reform: Frequently Asked Questions" (2012) MEMO/12/41. The draft Regulation is "Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)" COM (2012) 11 final 2012/0011 (COD).

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

[9] 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).

may well disagree with the majority view and choose not to apply the interpretations of the A29WP.

Cloud computing definitions vary, but our definition is as follows:[10]

- 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:[11]

- Infrastructure as a Service ("IaaS") - computing resources such as processing power and/or storage;[12]
- Platform as a Service ("PaaS") - tools for constructing (and usually deploying) custom applications;[13]
- Software as a Service ("SaaS") - end-user application functionality.[14]

These services form a spectrum, from low-level (IaaS) to high-level (SaaS) 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.[15] Furthermore, 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.[16] In a "layered" situation, where the provider with whom the cloud user/controller has the direct contract is a "processor" on behalf of the cloud

---

[10] S Bradshaw, C Millard and I Walden, "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services" (2010) ("CLP Contracts Paper") available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374 (accessed 22 March 2012) and S Bradshaw, C Millard and I Walden, "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services." (2011) 19/3 *International Journal of Law and Information Technology* 187–223.

[11] CLP Applicability Paper, see note 2 above.

[12] E.g. Rackspace; Amazon's EC2 and S3.

[13] E.g. Google's App Engine; Microsoft's Windows Azure.

[14] E.g. webmail services like Yahoo! Mail, social networking sites like Facebook, Salesforce's online customer relationship management service (enterprise SaaS).

[15] CLP Contracts Paper, see note 10 above, at s 3, 8.

[16] Heroku, "Can I Connect to Services Outside of Heroku?" available at http://devcenter.heroku.com/articles/external-services (accessed 22 March 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).

user, any sub-provider whose services are used by the provider, such as an underlying IaaS or PaaS service may be considered by some to be a sub-processor. However, we would argue that generally such a sub-provider (including data centre operator) is not a sub-processor, as it does not actively process data but only provides resources for use by the provider in servicing its cloud computing customers. In some cases, we argue that even the direct provider itself may not be a processor, although it is uncertain to what extent the provider's choice of sub-provider or data centre(s) used may render it a "controller".[17]

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, e.g. US government users, or UK local government), and hybrid cloud – involving a mixture, e.g. a corporation with a private cloud may "cloud burst" certain processing activities to the public cloud in times of peak demand.[18]

2. Data export restriction

Art 25(1) provides that Member States must not allow a data controller to export data to a country that does not provide for an adequate level of protection for personal data, meaning a standard in keeping with the main principles of the DPD:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

This applies whether the data are kept within the same entity, such as a branch in that country, or whether the export is to a company in the same group in that country, or to a third party in that country. It appears that this provision was intended to put third countries under some pressure to adopt data protection standards similar to those of the EEA.[19]

Note that this is a specific additional requirement under the Directive. A data export or transfer still constitutes "processing", for which a legal justification is required in

---

[17] CLP Controllers/Processors Paper, see note 2 above.

[18] CLP Applicability Paper, see note 2 above.

[19] DPD, see note 1 above, at art 25(5).

the normal way, e.g. data subject consent to the processing, even where export is permitted under art 25 or art 26.

The European Commission may declare that certain countries provide such adequate protection with the consequence that personal data may be exported freely to these countries.[20] So far only a few countries, of which several are small territories in Europe, have been declared to provide an adequate standard in this way: Andorra, Argentina, Canada (where the *Canadian Personal Information Protection and Electronic Documents Act 2000* applies), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man and Jersey.[21]

France, Portugal and Spain allow the national data protection authority to make its own adequacy findings, and in Belgium, the Netherlands, and Sweden the Ministry of Justice or government may do so, but such findings are rare, while other Member States do not even empower national authorities to make adequacy findings.[22] In practice, Member States simply confirm locally the European Commission's adequacy findings,[23] and have never issued adequacy findings for countries not already found adequate by the Commission.[24]

In essence therefore the DPD prohibits the export of personal data from the EEA to third countries (other than those listed above) unless exceptions apply or special arrangements are made to assure adequacy. The A29WP considers that this includes the transfer of personal data to a server outside the EEA.[25]

The essence of many cloud computing arrangements is remote data storage and other data processing in such a way that the geographic location of the data and/or operations on data may change and easily be replicated to other countries, including countries outside the EEA. Therefore, the rules on data export create significant challenges for cloud computing, which by its very nature is based on data transfers from the user to the cloud (and vice versa), and automated data transfers within the cloud.

This causes problems for data controllers established in the EEA, but can be even more problematic where the data controller is not established in the EEA. This is because the DPD applies by virtue of art 4(1)(c) not only to processing in the context of an EU establishment but also where a data controller based outside the EU is using "equipment" or "means" such as a cookie on the user's computer, or is using an EEA

---

[20] *Ibid,* art 25(6).

[21] For the relevant Decisions see http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm (accessed 22 March 2012).

[22] European Commission, *Analysis and Impact Study on the Implementation of Directive EC 95/46 in Member States* (2003), at 32.

[23] *Ibid*.

[24] LRDP Kantor Ltd, see note 8 above, at 78.

[25] A29WP, "Opinion 2/2010 on Online Behavioural Advertising" (2010) *WP 171*, at 5.4; and see A29WP, "Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)" (2006) *WP 128* ("SWIFT"), where the A29WP considered that mirroring (automatically copying) personal data to a Belgian entity's US-located server was a "transfer". See note 105 below.

data centre or EEA provider.[26] Combining the jurisdictional provisions with the provisions on data export may mean that a cloud provider with no establishment in the EEA may nevertheless be subject to the EU data export regime when attempting to transfer data back from the EEA to its place of establishment or some other location outside the EEA, even if the data were originally collected outside the EEA and relate to non-EEA individuals.

This may have the result that the DPD prevents non-EEA cloud computing service providers offering their services remotely to users in the EEA, unless the provider complies with the requirements of the relevant national implementation(s) or an exception applies. It also raises serious issues about the enforceability of EU Data Protection Laws in practice.[27] For example, a cloud provider based in the US offering remote storage and processing of photographs in the cloud with data centres based at various locations in the US would not be allowed to offer this service to users in the EEA (unless exceptions / special arrangements apply - see below). However it is difficult to see what EEA national data protection authorities would do to enforce the law against this remote cloud provider in the US. The A29WP has not recommended any solutions to this problem, but has merely stated that "existing tools regulating the conditions for transfers should be further reflected upon".[28]

Similarly, through the establishment or equipment nexus, EU Data Protection Laws may apply to non-EEA customers of cloud computing services that use data centres or providers in the EEA.[29] However, enforcement against them may again not be practicable.

It should also be noted that while some discussions centre on the jurisdiction of establishment of the cloud provider (many of whom are US corporations), in practice most cloud computing processing occurs using equipment housed in data centres or server farms, which may be situated in different geographical locations around the world. One might say that cloud computing is "data centre-centric".

While the popular view seems to be that in cloud computing data moves around the world continuously and almost randomly, so that it is not possible to know where a specific user's data are located at any one time (another reason to call it the "cloud of unknowing"), in practice this is often not so. In most cases, data are usually copied or replicated to different data centres, for business continuity/backup purposes, rather than being "moved" by being deleted from one data centre and re-created in another. Also, the primary copy of a set of related data (e.g. for a specific user, or a particular SaaS application etc, depending on the provider's setup and systems) will often be stored in the same data centre. This will typically be the one geographically closest to the user in question, for latency reasons (speed of access and response for users), albeit perhaps data may be stored in fragments distributed amongst different storage hardware within that data centre. Often the provider will know where a user's data fragments (e.g. for a particular application) are stored, at the data centre if not

---

[26] CLP Applicability Paper, see note 2 above.

[27] A29WP, "Opinion 8/2010 on Applicable Law" (2010) *WP 179*, at 25.

[28] *Ibid*.

[29] CLP Applicability Paper, see note 2 above.

equipment level. However, in most cases, whether for security or other reasons, providers do not disclose their data's location to users.[30] Some providers do allow users to check certain location information.[31] As technology improves, costs reduce and customers increasingly demand greater transparency for regulatory compliance and other reasons, perhaps more providers will offer users capabilities to monitor data location and other matters, whether as a standard or additionally-priced feature, in order to maintain or increase their market competitiveness.[32]

With increasing globalisation, a non-EEA entity could well own or rent space and/or equipment in a data centre located within the EEA. If it uses that data centre to provide cloud computing services, transfer of personal data to it might not constitute transfer of data outside the EEA, even though the entity is not established in the EEA. Conversely, if an EEA-established entity uses a non-EEA data centre for cloud computing, then transferring personal data to that entity for cloud computing could constitute data export, as discussed below.[33] Also, recall that, behind the scenes, many cloud services involve the use of sub-providers and even sub-sub-providers etc, so that the relevant data centre location would be that of the data centre ultimately used by the sub-provider in the lowest layer of the cloud "stack" (which may not even be a cloud services provider as such, but a data centre services provider).

Given these issues and complexities, in any analysis it is important to be clear as to whether what is being considered is the physical location of the data, the physical location of the provider to whom a controller transfers data, and/or the laws of a jurisdiction where the provider is incorporated or established or where data are located. Regarding the latter, the wording of the DPD's data export restriction, and of many national implementations, focuses on the third country ensuring an adequate level of protection, seemingly envisaging that this be achieved through that country's data protection and privacy laws. The DPD's wording does not envisage the possibility that exported data could be adequately protected by other means, such as strong encryption or other measures taken by the controller/exporter or the recipient/importer. The DPD restriction is thus based on the assumption, exemplified

---

[30] For one attempt to identify the locations of various providers' data centres, see C Gaun, "Sniffing Out the Geographic Location of Cloud Service Data Centers" (2011) *Ideas Insights* available at http://ideasint.blogs.com/ideasinsights/2011/05/sniffing-out-the-geographic-location-of-cloud-service-data-centers-.html (accessed 22 March 2012).

[31] For instance, Salesforce enables users to check the data centre location of the virtual machine "instance" their organisation is using, see http://trust.salesforce.com/trust/status/ (accessed 22 March 2012) - which also enables monitoring of performance and maintenance data. It is not said whether a user's data, when saved to persistent storage, would be located in the same data centre, although that is probable for latency reasons.

[32] Current techniques for users to verify the geographical location of their data independently are not straightforward or reliable. Even when the location is given by the provider, users must trust that the information is accurate; and, even if is accurate location of data in one place does not exclude the possibility of copies also being located elsewhere. However, the issue of how cloud users may obtain independent, accurate verification of the location of their data is increasing in profile. Z Peterson, M Gondree and R Beverly, "A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud" *Proceedings of HotCloud 11*, Portland, Oregon, USA, 14-17 June 2011.

[33] See para containing note 44 below.

by the German regulator's view mentioned below,[34] that data physically located in a particular country are at risk of being accessed by unauthorised third parties located in that country.

However, technological developments, particularly the Internet, have undermined this assumption, and some national implementations take a different approach. For instance, the UK Information Commissioner ("ICO") considers that a controller is entitled to assess for itself whether protection is adequate in the circumstances, so that, for example, it is reasonable to decide adequate protection exists where an employee takes a laptop containing personal data outside the EEA, as long as the information stays with the employee on the laptop and the employer has effective procedures to address security and other risks of using laptops (including the extra risks of international travel).[35] The German federal law, discussed below,[36] focuses on adequacy of protection offered by the data recipient in the third country, rather than under the laws of that country.

3. What is a "Transfer"? Who makes the Transfer?

Given the importance of data transfers in cloud computing, it is necessary to consider what a "transfer" is, what are the exceptions for making international data transfers possible, and whether and how these exceptions might apply to cloud computing.

The Directive does not define "transfer", although some national laws do. As mentioned above,[37] the A29WP considers that a transfer of personal data to a server outside the EEA would be considered a regulated data export for DPD purposes. Therefore, it might seem reasonable to take the view that, in considering whether a data export has occurred in a cloud computing operation, one should first ascertain the geographical location of the equipment used for the processing, i.e. in practice the location of the data centre(s) used to provide the cloud computing service in question.

However, in the analogous situation of web hosting, unfortunately the Directive

> does not lay down criteria for deciding whether operations carried out by hosting providers should be deemed to occur in the place of establishment of the service provider or at its business address or in the place where the computer or computers constituting the service's infrastructure are located.[38]

---

[34] See para containing note 48 below.

[35] ICO, "Sending Personal Data outside the European Economic Area (Principle 8)" available at http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_8.aspx (accessed 22 March 2012).

[36] See para containing note 47 below.

[37] A29WP, see note 25 above.

[38] *Bodil Lindqvist,* [2003] ECR I-12971 (ECJ), at 67 (hereafter, *Lindqvist*).

Pragmatically, the ECJ has noted that treating uploading of personal data to a web host as a "transfer" to a third country would lead to impracticable and unrealistic results.[39] It concluded there was no data export

> where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.[40]

The ECJ carefully confined this holding to the uploading of data to a host "established in" a member state, stressing that the question referred to it concerned only the uploader's activities, not hosting providers', although it recognised that the host's infrastructure might be and indeed often was located in other countries. The ECJ considered it "unnecessary to investigate whether an individual from a third country has accessed the internet page concerned or whether the server of that hosting service is physically in a third country". Although the ECJ did not discuss when the transfer happens, the ICO considers "a transfer was only deemed to have occurred where the Internet page was actually accessed by a person located in a third country".[41]

How does this apply to cloud computing services involving data centres or server farms inside and/or outside the EEA, particularly where the cloud computing services provider is established in the EEA? *Lindqvist*[42] seems to suggest that if a cloud customer uploads personal data to an EEA-established cloud provider, there is no data export by the customer, irrespective of the location of the provider's data centres. However, even the ICO, generally thought one of the more pragmatic regulators, considers that if a controller uploads data to a UK-based web server intending that the information will be accessed by website visitors outside the EEA, that upload is a regulated transfer.[43] Thus, the focus in the UK is seemingly on *intention* to allow non-EEA entities to access data, although the "intention" aspect was not spelled out either in the DPD or the UK implementation.

On that basis, data export restrictions may be relevant to web hosting activities primarily because data are uploaded to a public website. Conversely, if a controller uploads personal data to an EEA-established cloud provider intending to store or operate on the data using cloud computing, but not intending the data to be publicly

---

[39] If art 25 of *Directive 95/46* were interpreted to mean that there is "transfer [of data] to a third country" every time that personal data are loaded onto an Internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the Internet. The special regime provided for by ch IV of the Directive would thus necessarily become a regime of general application, as regards operations on the Internet. Thus, if the Commission found, pursuant to art 25(4) of *Directive 95/46*, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the Internet.

[40] *Ibid*, at 69-71.

[41] ICO, *The Eighth Data Protection Principle and International Data Transfers v4.0* (2010), at 1.3.4. Commentators also share this view that transfer involves actual receipt of information in a third country, not potential ability to access it, e.g. C Kuner, see note 5 above, at 4.08.

[42] See note 38 above.

[43] ICO, see note 411 above.

accessible, it could be arguable, based on *Lindqvist*, that the controller is not exporting data even if the provider uses a *non*-EEA data centre (or non-EEA provider) to provide its services. Whether the *provider* exports data by doing so is yet another issue; it might even risk becoming a controller through taking the decision to use a non-EEA data centre or non-EEA provider.[44]

Another question is the relevance, if any, of the controller's knowledge that the provider will be using a non-EEA data centre for the processing. If the controller knows that the provider uses only non-EEA data centres, does this mean that the controller "intended" to export data? Must the controller inquire as to the location of the data centre(s) used, in order to avoid the risk of breaching the data export restriction? Can intention to export be attributed to it from lack of inquiry? What is the controller's position if the provider declines (for example, for security reasons) to name the locations of all data centres which could be used to process data for that controller? The same questions arise where a controller uses a non-EEA provider that may use non-EEA data centres. Similarly, where the direct provider provides its cloud computing service using sub-providers (or even sub-sub-providers, etc) who use non-EEA data centres – for example, where an EEA SaaS provider builds its service on an IaaS provider's platform or infrastructure and the IaaS provider uses non-EEA data centres.

A further issue is the possible ability of the provider (and of any sub-provider, e.g. IaaS provider) to access cloud users' data. As discussed in a previous paper,[45] where data stored with providers are not encrypted, or only weakly encrypted, most providers have the technical ability to access the data in intelligible form. Most providers also contractually reserve the right to do so, e.g. for service/support reasons or if disclosure is compelled or requested by law enforcement authorities. If the controller/cloud customer knows that the provider has the ability and legal right to access its data, and the provider is established outside the EEA, does this mean that the controller "intended" to allow non-EEA entities to access its data? Must the controller investigate the extent of the provider's ability to access its data? [46]

In this connection it is interesting to note that the German Federal Data Protection Act defines "transfer" as "the revealing to a third party of personal data which are stored or have been obtained by data processing in such a way that (a) the data are given to the third party or (b) the third party views or accesses data which is made available for view or access…."[47] Thus, again, the emphasis seems to be on "transfer" involving a third party knowing or accessing data. However, where the cloud provider is outside Germany or the EEA, at least one German regulator seems to consider that cloud computing necessarily involves data export. He did not discuss the possibility that a non-EEA provider might nevertheless use an EEA-located data centre for certain

---

[44] SWIFT, see note 25 above; see also note 105 below. The ability to make "critical decisions", including on the location of SWIFT's operating centres, was considered a factor.

[45] CLP Personal Data Paper, see note 2 above.

[46] If the provider is considered a controller through its ability to choose sub-providers, location of data centre(s) used and/or security measures, the same issues regarding its knowledge, "intention" to export, sub-provider's ability to access data, etc, would be relevant equally to the provider as controller.

[47] C Kuner, see note 5 above, at 2.44.

processing, but took the view that, if data are processed in another country, persons in that country, such as law enforcement authorities, may be able to access users' data, including by demanding decryption keys for any encrypted data.[48]

Also of interest are the views of Denmark's Data Protection Agency ("Datatilsynet"). In connection with proposed use of Google Apps (SaaS) by the Danish municipality Odense, it ruled that, while transmission to Google Ireland Limited acting as a data processor and to data centres located in EU member countries or EEA countries would not be a third country transmission, transmission to data centres in the USA and certain countries in Europe would constitute regulated transfers subject to Danish data protection law export restrictions (the "*Odense*" decision).[49] The Datatilsynet does not appear to have considered the question of intention to allow access to data.

Therefore, if, for processing personal data, an EEA controller uses a cloud provider (even one established in the EEA) which has data centres both inside and outside the EEA, such that data may flow to third country data centres, the cautious view, and the one generally adopted in practice, is that export restrictions would apply to that use. This is one driver behind cloud providers increasingly offering customers the option to confine data to EEA servers only.[50]

What of the not uncommon situation where a provider uses a sub-provider's platform or infrastructure to provide cloud computing services to an EEA customer? If the provider is treated as a processor, its sub-provider, e.g. underlying IaaS or PaaS provider, might well be treated as a sub-processor, in which case the previous discussion on the customer's intention/knowledge of the location of the data centre(s) ultimately used may be relevant. If a non-EEA data centre is used, it will also be necessary to consider whether there is a data export by the customer, by the provider, or indeed by the sub-provider. If none of the providers are regarded as processors, then it seems the export would be effected solely by the cloud customer, assuming it has any necessary intention. The question may arise whether, by choosing to use a non-EEA data centre or sub-provider with non-EEA data centre, the provider thereby becomes a controller. However, equally it could be argued that it is the cloud user who controls the means by choosing to use a cloud provider who (ultimately) uses a non-EEA data centre.

The Appendix contains tables and notes regarding some possible permutations of countries involved, illustrating the complexities of international data transfers in cloud computing. It should also be noted that data export may occur in situations other than deliberate upload of data to a cloud provider. A German state regulator has required website owners in that state to deactivate certain features such as fan pages and the "Like" plug-in from the social networking website Facebook. These services transfer content and traffic data to Facebook in the USA, with limited web analytics information (on number of visitors to their page etc) being provided to the website

---

[48] E.g. the regulator for the German state of Schleswig-Holstein, T Weichert, "Cloud Computing and Data Privacy" (2011) *The Sedona Conference*: "If we include entities outside the European Union, the data transfer that is inevitable with cloud computing - and which has no legitimacy under data privacy law - makes clouds inherently impermissible."

[49] Datatilsynet, *Processing of Sensitive Personal Data in a Cloud Solution* (2011), at 3.3.

[50] See s 0 below.

owner, enabling Facebook to track and profile visitors for two years. The regulator considered that this conflicted with German communications and data protection laws unless website users' informed consent had been given before the data transfer to Facebook. Logically, this could extend to non-EEA analytics services other than Facebook's, such as Google Analytics, and indeed other web-based services such as social bookmarking. It is therefore relevant to some SaaS services as well as German and perhaps other EEA websites generally, and is "only the beginning of a continuing privacy impact analysis of Facebook applications".[51]

Finally, the purpose of the data export restriction merits consideration. It aims to ensure that personal data are protected, by not allowing the data to enter countries deemed to have inadequate protection. There is a view that if a non-EEA data importer is subject to the DPD through the application of art 4,[52] and therefore has to protect the imported personal data in accordance with DPD requirements, the data export restriction should not apply.[53] However, notwithstanding this view, Member States' authorities tend to treat the data export restriction as a separate stand-alone requirement.

4. Data Export Exceptions/Derogations

We now consider situations where the Directive, notwithstanding lack of adequate protection, permits export.

4.1. Consent

According to art 26(1) (a), if the data subject has given his or her unambiguous consent to a data transfer, it may go ahead notwithstanding the lack of adequate protection. However, the consent must be a freely given, specific, informed and unambiguous indication of the data subject's wishes, which the A29WP has interpreted quite strictly.[54] While art 26(1)(a) may be used to allow one-off transfers where the requisite data subject's consent has been "specifically given for the particular transfer or a particular category of transfers in question", in relation to

---

[51] Schleswig-Holstein Data Protection Commissioner's Office, "ULD to Website Owners: 'Deactivate Facebook Web Analytics'" (2011) available at https://www.datenschutzzentrum.de/presse/20110819-facebook-en.htm (accessed 22 March 2012).

[52] CLP Applicability Paper, see note 2 above.

[53] C Kuner, see note 5, at 4.33.

[54] Art 2(h). Not all national implementations include this wording in their definition of "consent". The UK Data Protection Act 1998, for example, does not. A29WP, *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive,* (1998) *WP12* 24 and A29WP, *Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995,* (2005) *WP 114*, 10-12 ("WP114") explains the A29WP's views on the pre-requisites for valid "consent" to exporting data to a country without "adequate protection", for example properly informing the data subject of the particular risk that his/her data are to be transferred to a country lacking adequate protection. Implied consent, such as notification of transfer and failure to object, is unlikely to be considered sufficient. For detailed discussion of the general concept of "consent", see A29WP, "Opinion 15/2011 on the Definition of Consent" (2011) *WP187*.

repeated or structural transfers, the A29WP has expressed the view that in practice consent is unlikely to provide a satisfactory long-term framework:

> In fact, particularly if the transfer forms an intrinsic part of the main processing (e.g. centralisation of a world database of human resources, which needs to be fed by continual and systematic data transfers to be operational), the data controllers could find themselves in insoluble situations if just one data subject subsequently decided to withdraw his consent.[55]

Consent as a justification may also be difficult in practice as the A29WP considers that, for advance consent to future transfers to be valid, details of the transfer must be "already predetermined, notably in terms of purpose and categories of recipients", as well as notified to data subjects, and that consent may be withdrawn at any time (which would require isolating the personal data concerned and preventing its export).[56] Therefore, for regular or repeated transfers made as part of a business or other commercial relationship, such as when using cloud computing, it may be better to try to find a justification other than consent.

Reliance on consent also raises the question of who is the data subject from whom consent must be obtained, and who is actually transferring the personal data.

On the one hand, if a user of a cloud SaaS service, such as a social networking site, is both a data subject and a joint controller knowing that his or her personal data will be transferred, processed and stored in a third country without an adequate standard of protection, it could be argued that this user has given consent as data subject.

On the other hand, if the user of the cloud service is not the data subject of the data transferred, then it may be impossible to rely on the consent derogation in art 26(1)(a). For example if a business uses a cloud application to process customer data (such as orders), then it may be more difficult to rely on an argument that the data subject (the customer) has given consent.

The same may apply where an EEA user of a SaaS service such as a social networking site posts personal data of other individuals, such as friends' photographs or names. Individuals may benefit from the "household exception" (processing personal data for a purely personal or household activity).[57] However, the A29WP considers that "A high number of contacts could be an indication that the household exception does not apply", so the user would be a data controller subject to data protection law requirements. Similarly, where access to profile information is available to all site members (or indeed the public) and/or indexable by search engines, or the user takes an informed decision to extend access beyond self-selected friends.[58] In that event, when users post personal data of others, including non-members of the site, they must comply with data protection laws including data export restrictions.

---

[55] *Ibid,* WP114 at 11.

[56] *Ibid,* WP114 at 12.

[57] DPD, art 3(2).

[58] A29WP, "Opinion 5/2009 on Online Social Networking" (2009) *WP 163*, at 3.1.1-3.1.2.

The difficulties regarding data subject consent to others' processing of their personal data, let alone unambiguous consent to data export, were highlighted when Germany's Hamburg data protection authority took proceedings against social networking SaaS service Facebook. Facebook encouraged its members to use its "Friend Finder" tool to import their email address books, thereby giving Facebook access to the personal data of members' contacts (their email addresses etc). Facebook used that information to send unsolicited emails to members' contacts inviting them to join Facebook – without the contacts' consent. After discussions, Facebook agreed to make changes, including allowing email recipients to block further emails from Facebook.[59]

Obtaining data subject consent when a cloud customer wishes to use cloud computing services involving export of third party personal data may thus be problematic. It is possible, but the customer would have to show that the data subjects' consent to the transfer was freely given, specific, informed and unambiguous, and it may prefer not to have to rely on this exception.

4.2. Other Derogations Contained in Art 26

The transfer may also be justified if it is necessary for the performance of a contract between the data subject and the data controller, according to art 26(1) (b). For instance, a data subject who is the cloud customer may know the service is provided from outside the EEA, and cannot be provided within the EEA, but chooses to use it nonetheless. An often used example of "necessity" involves a travel agent sending an individual's personal data to the third country hotels concerned when an individual books a trip abroad.[60]

The A29WP considers that derogations, e.g. for "necessity", should be construed restrictively,[61] and, as the ICO has noted, cost-efficiency does not amount to necessity.[62] There is nothing intrinsic to cloud computing that necessitates transfer of data to a particular jurisdiction or a jurisdiction without an adequate standard; in fact, some cloud providers provide regional clouds to avoid the issues surrounding transfer.[63]

None of the other derogations mentioned in art 26 seem particularly relevant to cloud computing.

5. Ways to Meet the Adequacy Requirement

Where no exception can apply, it may still be possible to export personal data from the EEA if the adequacy requirement can be met. In fact EU regulators prefer

---

[59] Spiegel Online International, "Facebook Agrees to Change 'Friend Finder' Feature" (2011) available at http://www.spiegel.de/international/business/0,1518,741027,00.html (accessed 22 March 2012).

[60] WP114, see note 54 above, at 13.

[61] *Ibid*.

[62] ICO, see note 41 above, at 25.

[63] See note 50 above.

adequacy as the basis for export, considering use of a derogation to be less satisfactory as personal data loses protection once exported through derogation.[64]

5.1. EU-US Safe Harbor Principles[65]

The US and the EU have made arrangements by way of a self-regulatory regime which allows organisations in the US (including cloud service providers) that import personal data from the EU to demonstrate an adequate standard of protection for the purposes of art 25 by participating in a Safe Harbor programme. According to some reports the popularity of the Safe Harbor programme has increased with the advent of cloud computing.[66]

The only types of entities that may participate in the Safe Harbor are US organisations that are subject to the jurisdiction of the US Federal Trade Commission ("FTC") or US air carriers and ticket agents subject to the jurisdiction of the Department of Transportation ("DOT"). Thus, many types of organisations are not able to make use of the Safe Harbor because they are not subject to relevant regulatory oversight by the FTC or DOT, including, for example, telecommunication common carriers and financial institutions.

To obtain Safe Harbor status a US organisation has to either (i) join an existing self-regulatory privacy programme or (ii) develop its own privacy scheme that complies with the requirements. The US organisation has to (i) self-certify annually that it is Safe Harbor compliant to the US Department of Commerce, which publishes a list of all Safe Harbor participants, and (ii) state, in its publicly-accessible privacy policy, its adherence to the Safe Harbor principles (of Notice, Choice, Transfers to Third Parties, Access, Security, Data Integrity and Enforcement). Duly-certified and listed organisations are often called "Safe Harborites".

The Safe Harbor regime is primarily enforced by the private sector, backed up by government enforcement. Participating US organisations must (i) establish self-assessment or third party assessment audit procedures for verifying compliance with the Safe Harbor and (ii) provide dispute resolution for complainants. The dispute resolution procedures must provide for sanctions, publicity and deletion of data, as well as suspension of Safe Harbor status. Dispute resolution may either be provided for by a private dispute resolution provider[67] or in co-operation with a panel provided by the relevant European Union data protection authority. The FTC and the DOT have

---

[64] WP114, see note 54 above; C Kuner, see note 5 above, at 4.12.

[65] Finding of adequacy for Safe Harbor, effective on 30 November 2000, under *Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*, 2000/520/EC OJ L215/7, 25.8.2000.

[66] Scott Sanchez, "Location, Location, Location - Storing EU Data with Safe Harbor" (2010) *Cloud Computing Journal* available at http://cloudcomputing.sys-con.com/node/1562070 (accessed 22 March 2012).

[67] Such as the Judicial Arbitration and Mediation Service and the American Arbitration Association. US Department of Commerce, *Safe Harbor Workbook* available at http://export.gov/safeharbor/eg_main_018238.asp (accessed 22 March 2012).

powers to enforce the Safe Harbor regime where an organisation's failure to comply is an infringement of state or federal laws prohibiting unfair or deceptive acts.[68]

It might be thought that as, currently, most large cloud providers are US-based or headquartered entities, Safe Harbor would be the obvious mechanism to facilitate use by EEA data controllers of the services of US cloud providers. However, doubts have been raised about the Safe Harbor framework.

There is some uncertainty regarding whether the Safe Harbor framework applies to transfers to a US processor (as opposed to controller), such as a cloud provider. The better view is that it does, and that Safe Harbor requirements such as notice and choice may be met by the controller-exporter giving notice of the processing to data subjects, etc, or instructing the processor to do so.[69] We assume that mere processors may indeed become Safe Harborites.

Furthermore, a 2008 study found only about 70% of organisations on the Safe Harbor list were currently certified, and only some 20% of listed organisations met even basic requirements, with 13% choosing non-affordable dispute resolution providers.[70] In 2009, the FTC moved against seven US businesses which falsely claimed current Safe Harbor certifications.[71] In 2011 it took its first action for breach of substantive Safe Harbor principles, against Google in relation to its Buzz SaaS service – for failing to give users of its SaaS webmail service Gmail any notice before, or choice about, Google's use of information collected for Gmail for a purpose other than that for which it was originally collected.[72]

The Safe Harbor adequacy Decision by the European Commission should permit transfers to the US "without additional guarantees being necessary".[73] Indeed, some UK educational institutions use Google Apps for Education on the basis of the Safe Harbor and Google's standard terms.[74] However, the group of sixteen German federal state data protection regulators known as the Düsseldorfer Kreis[75] now require

---

[68] Such as *US Federal Trade Commission Act*, s 5.

[69] C Kuner, see note 5, at 182.

[70] C Galexia, *The US Safe Harbor - Fact or Fiction?* (2008).

[71] FTC, "Court Halts U.S. Internet Seller Deceptively Posing as U.K. Home Electronics Site" (2009) *FTC File No. 092-3081* and FTC, "FTC Settles with Six Companies Claiming to Comply with International Privacy Framework" (2009) *FTC File No. 0923137.*

[72] FTC, "FTC Charges Deceptive Privacy Practices in Google's Rollout of its Buzz Social Network" (20011) *FTC File No. 102 3136.*

[73] Safe Harbour Decision, see note n 65 above, Recital 2.

[74] E.g. University of Cambridge, which made its contract available publicly at http://www.ucs.cam.ac.uk/googleapps/google-apps-cambridge-contract.pdf (accessed 22 March 2012). Similarly Portsmouth University relied on Safe Harbor – Kable, "Portsmouth Uni Students get Google Apps Service" (2009) *ZDNet* available at http://www.zdnet.co.uk/news/networking/2009/09/04/portsmouth-uni-students-get-google-apps-service-39739504/ (accessed 22 March 2012).

[75] http://www.datenschutz-berlin.de/content/deutschland/duesseldorfer-kreis (accessed 22 March 2012).

German controllers to conduct and document certain checks before transferring personal data to Safe Harborites.[76]

Another question is, may personal data safely be exported to an US entity because it is a Safe Harborite? Or must the exporter nevertheless inquire further regarding where the Safe Harborite intends to store the exported data (US only, or outside?) and/or to whom the Safe Harborite intends to or may transfer or disclose the data? The first issue, regarding the location of data attempted to be exported under Safe Harbor, was discussed in *Odense*, mentioned earlier. There, the Datatilsynet considered that, as Google, Inc had subscribed to the Safe Harbor, the Safe Harbor permitted transfers of personal data to Google's US data centres – but not transfers to "data centres located in other insecure third countries than the USA". Without confirmation that Google's European data centres were in the EEA, the authority considered that the transfer provisions were not complied with. It considered however that transfer would have been permissible had model clauses, covered below, been used.[77] On this basis, it is insufficient merely to check that the proposed provider is a listed Safe Harborite; the controller also needs to check that data centres to be used by the Safe Harborite to process the controller's data are located only in the USA and/or EEA.

This ruling typifies the regulatory focus on location of data, rather than of the Safe Harbor-certified entity. With portable physical data storage media such as a hard drive, CD-ROM or USB stick, the fixation on data location may be understandable, but with cloud computing it is jurisdiction over the data importing entity that is much more significant for data protection oversight purposes than data location, as discussed below.[78] Interestingly, German law generally focuses on adequacy of protection offered by the recipient in any third country, rather than by the country's legal system,[79] but that approach is not followed through in other respects.

We now consider so-called "onward transfers", Safe Harbor parlance for the increasingly common "disclosure" of exported information by Safe Harborites to third parties.[80] Where an EEA controller exports data to a US cloud provider which is a Safe Harborite ("Safe Harborite provider"), is there an "onward transfer" if the provider utilises a sub-provider's infrastructure to process the data, such as where a

---

[76] *Decision by the Supreme Supervisory Authorities for Data Protection in the Non-public Sector on 28/29 April 2010 in Hannover (revised 23 August 2010) - Examination of the Data Importer's Self-certification According to the Safe-Harbor-Agreement by the Company Exporting Data*.

[77] "Odense Municipality and the individual data centres may enter into an agreement based on the EU Commission's standard contractual clauses, or Odense Municipality may grant Google Ireland Limited a clear mandate to enter into agreements, in Odense Municipality's name and on behalf of Odense Municipality, based on the EU Commission's standard contractual clauses with the individual data centres" - but the Datatilsynet assumed that there were no such agreements as it was not informed of any. Datatilsynet, see notes 49 above and 111 below.

[78] See note 117 below.

[79] European Commission, *Analysis and Impact Study on the Implementation of Directive EC 95/46 in Member States* (2003), at 31.

[80] US Department of Commerce, *Safe Harbor Privacy Principles* (2000). The problems with onward transfers are discussed in C Kuner, "Onward Transfers of Personal Data under the US Safe Harbor Framework" (2009) 8 *Privacy & Security Law Report* 33.

SaaS provider uses a PaaS or IaaS provider? We have argued previously[81] that many IaaS, PaaS and some SaaS providers are not even processors, because they do not take actions actively, but merely provide infrastructure/resources for use by the controller. Arguably, this is the case too with sub-providers, at least where the sub-provider has no technical ability to access the data. Nevertheless, it is insufficiently clear whether use of a sub-provider involves onward transfer.

In a related vein, the onward transfer rules seem to equate "transfer" with "disclosure". However, this is not necessarily so. Transfer of data to a provider or sub-provider for storage or other processing does not necessarily involve disclosing data to it; for example, data will not be disclosed if they were strongly-encrypted or the system's design does not allow the provider to read data in intelligible form, as discussed above.[82] However, for simplicity of discussion, we assume here that "transfer" involves "disclosure".

Access by third parties to data exported to a Safe Harborite would also constitute "onward transfer", including remote access. Apart from where a Safe Harborite provider is technically able to, and does, allow third parties access to data, e.g. US law enforcement authorities,[83] onward transfers via allowing third parties to access exported data would generally be controlled by the controller-exporter, not the provider. For example, a controller could enable its employees worldwide to view data stored by it with a cloud provider in the US. However, Safe Harbor rules seem to place onward transfer responsibilities on the Safe Harborite, although, as with the arguments regarding whether processors can be Safe Harborites, arguably these responsibilities could be met through actions by the controller-exporter. Note that these issues may be relevant not just to cloud computing but also to websites of EEA entities hosted using US hosting providers.

The position regarding onward transfers is problematic, not least because Safe Harbor terminology does not reflect the DPD's "controller"/"processor" concepts. A related debate concerns whether personal data, once duly exported to a Safe Harborite, are thereafter subject only to US law Safe Harbor rules, or whether exported data and their processing (including onward transfers) remain subject to the data protection rules of the exporter's Member State, which stay "attached" to the data virtually wherever they go. The US government and US entities take the former view, many EU regulators the latter.

One issue is that Safe Harbor rules regulating onward transfers differ, depending on whether the "transfer" is to a third party which is "acting as an agent", that is "performing task(s) on behalf of and under the instructions of the organisation". "Agents" seem to map to "processors", and other "third parties" to "controllers". Requirements for non-agents involve applying the notice and choice principles, which may be difficult to fulfil in practice. For "transfers" to "agents", the Safe Harborite must first check that the agent

---

[81] CLP Controllers/Processors Paper, see note 2 above.

[82] See note 45 above.

[83] Ian Walden, "Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent" (2011) available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1781067 (accessed 22 March 2012).

> subscribes to the [*Safe Harbor*] Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles.[84]

Kuner[85] suggests that, to limit the importer/provider's risks, an "assurance agreement" with non-EEA onward transferees would be sensible.

However, the status of sub-providers as "agents"/processors or otherwise (or both) is unclear. As mentioned above, arguably many sub-providers are not even "agents", but infrastructure providers, and some may not have access to information that is "transferred" to them. Even assuming sub-providers are "third parties", it is unclear whether they are "agents" or not, and therefore it is uncertain which set of requirements must be met to enable a Safe Harborite provider to use a sub-provider. Either set may be impracticable to comply with when using cloud sub-providers. It is unclear, for instance, to what extent Safe Harborite providers in practice check that non-EEA sub-providers whose infrastructure they utilise subscribe to Safe Harbor or process the data in an "adequate" country, let alone enter into assurance agreements with them.

As for the situation where an EEA controller transfers data to a Safe Harborite provider intending future remote access to the data by third parties, the provider may not know or be able to control who those third parties are, let alone have relationships with them. This seems to put the main burden (to give notice to data subjects etc) on the controller, depending on the individual circumstances. This raises many thorny fact-dependent practical issues. The possible lack of clarity as to status of those third parties is exacerbated by the general difficulty, under current EU Data Protection Laws, of distinguishing between controllers and processors.[86]

5.2. Model Clauses

Art 26(4) provides that if a transfer of data to outside the EEA is made under contractual clauses the terms of which have been approved by the European Commission for this purpose, the protection is considered adequate, and the transfer must be permitted by Member States.

Standard contractual clauses have been issued by the European Commission for transfers of personal data (i) from an EEA-established controller to a controller in a third country,[87] or (ii) from EEA-established controller to a third country processor.[88]

---

[84] Safe Harbor Principles, see note 80 above. It is also uncertain whether an organisation may "subscribe" to Safe Harbor principles, i.e. agree to follow them, without formally being a Safe Harborite.

[85] C Kuner, see note 80 above.

[86] CLP Controllers/Processors Paper see note 2 above.

[87] There are two set of clauses for controller-controller transfers, under *Commission Decision of 15 June 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, under Directive 95/46/EC (2001/497/EC)*, OJ L181/19, 4.7.2001, and *Commission Decision of 27 December 2004 amending Decision 2001/497/EC as Regards the Introduction of an Alternative Set of Standard Contractual Clauses for the Transfer of Personal Data to Third Countries (2004/915/EC)*, OJ

The latter clauses were replaced in 2010[89] and now cover transfers by a third country processor to a third country sub-processor, sub-sub-processor, and etc.

5.3. Binding Corporate Rules

Binding Corporate Rules ("BCRs") are codes of conduct dealing with the international transfer of personal data within the same corporate group at a multinational level, subject to the authorisation of the relevant data protection authorities, devised by the A29WP under art 26(2) of the Directive with industry input.[90]

Transfers to third countries under approved BCRs are permissible. However, the process for obtaining regulatory approval is currently long and expensive, with different Member States having their own procedures, and some States' data protection authorities nevertheless taking the view that each transfer under an approved BCR still requires individual approval.[91] BCRs might be helpful for facilitating data transfers within a corporate group's private cloud.

5.4. Other Options

Finally, it may still be possible to transfer personal data to a third country, even if none of the above applies, by virtue of art 26(2). This allows a Member State to:

> authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of art 25(2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

While such authorisations should be notified to the European Commission and other Member States, very few have been notified in practice.[92]

L385/74, 29.12.2004. Either set may be used, although controllers prefer the latter set as it incorporates some of their requested changes.

[88] Under *Commission Decision of 27 December 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, under Directive 95/46/EC (2002/16/EC)*, OJ L6/52, 10.1.2002.

[89] By *Commission Decision of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries under Directive 95/46/EC of the European Parliament and of the Council (2010/87/EU)*, OJ L39/5, 12.2.2010 – the clauses in this Decision superseded the 2001 standard controller-processor clauses, which may no longer be used.

[90] For a list of the main A29WP working papers on BCRs please see European Commission, "Available Tools" available at http://ec.europa.eu/justice/policies/privacy/binding_rules/tools_en.htm (accessed 22 March 2012).

[91] C Kuner, see note 5, at 4.120-4.154.

[92] European Commission, *First Report on the Implementation of Directive 95/46/EC COM (2003)265 final* (2003), at 4.4.5 note 17, and European Commission, see note 22 above, at 13.6.

The ICO does not require transfers to be pre-authorised, but as mentioned above allows data controllers to make their own adequacy assessments.[93] Obviously, where a transferor makes its own assessment, it runs the risk that a data protection authority may later take the view that its assessment was wrong. The more thorough its assessment, however, the more likely it is that it will be able subsequently to justify it.

However, most Member States are not willing to permit data controllers' own assessments. Indeed, in Austria, Greece, Luxembourg, Portugal and Spain, absent an European Commission adequacy finding, only national authorities can determine the adequacy of a third country, which means transfers to countries not found adequate by the European Commission or relevant national authority are not possible unless a derogation applies.[94] In such cases, it may be possible to request the authority to approve an ad hoc contract for the data export, although this has time and costs implications, and the authority might decide not to approve the contract.

6. Possible Solutions for Cloud Computing

There are several possible solutions or workarounds that may enable cloud computing to be used to store or otherwise process personal data, notwithstanding the data export restriction. Sometimes, a combination of these methods may be used for "belt and braces" purposes, particularly in the not uncommon situation where the status of the provider as processor or controller is not entirely clear.

6.1. Anonymisation or Encryption

The data export restriction applies only to "personal data" within the DPD's definition. If information is not, or ceases to be, "personal data", for example because it has been adequately anonymised or strongly encrypted, it may be exported and otherwise dealt with free of the DPD's restrictions. Furthermore, data fragments stored in the cloud may not be "personal data" in the provider's hands if the provider is unable to read the fragments, although they would remain "personal data" as regards the cloud user storing the data, who by logging into their account with the provider may re-unite the fragments.[95]

It might seem therefore that a cloud user could strongly encrypt or anonymise personal data before storing it in the cloud, even with a provider that uses data centres located outside the EEA.

---

[93] ICO see note 35 above, at 2.3 – although permitting controllers to make their own assessments seems out of line with the A29WP's views: D 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" (2010) *European Commission Comparative Study on Different Approaches to New Privacy Challenges in Light of Technological Developments* 92.

[94] LRDP Kantor Ltd in association with Centre for Public Reform, "New Challenges to Data Protection- Final Report" (2010) *European Commission* 75.

[95] For detailed discussion of these issues, see CLP Personal Data Paper note 2 above, as supplemented by Hon, "'Personal Data' in the UK, Anonymisation and Encryption" (2011) available at http://www.cloudlegal.ccls.qmul.ac.uk/Research/49700.html (accessed 22 March 2012).

However, whether the data have truly become "anonymous" depends on the effectiveness of the anonymisation, which may change over time as reidentification techniques improve, and similarly the effectiveness of the encryption (including security of key management) affects whether the data remain "personal data". It is also uncertain whether, even if anonymised or encrypted information is treated as anonymous data in a provider's hands, it may still be considered "personal" data as regards the cloud user uploading the data.[96]

Until these uncertainties are resolved in all Member States, it is not clear whether controllers could store encrypted or anonymised data in cloud computing data centres outside the EEA without breaching the data export restriction.

6.2. Safe Harbor

The Safe Harbor is widely-used to justify data export to US cloud providers such as Google, as mentioned above. However, it only applies to US entities. This may not be a huge barrier currently, as so many cloud providers are US entities. Even so, the Safe Harbor cannot be used by telecommunications common carriers, that are increasingly providing cloud computing services, and there are uncertainties as to whether the Safe Harbor applies to processors such as cloud providers. Furthermore, and perhaps more importantly, the onward transfers rules may cause difficulties when the provider uses sub-providers or when the controller wishes to allow third parties access to exported data.[97]A bigger barrier may be the doubts raised by some EU regulators about the efficacy of the Safe Harbor. Given these concerns, it is not unlikely that the EU authorities will review the Safe Harbor. The A29WP has included the Safe Harbor in its work programme for 2012-2013 in any event.[98]

6.3. Model Clauses

Model clauses are a possible method to enable a controller to use the services of a cloud provider who has non-EEA data centres. They may even be incorporated into the provider's online contractual terms. For example, in its Client-Software License Agreement for its LiveVault software, for online backup of users' data to its infrastructure, US provider Iron Mountain expressly incorporated by reference the standard EU contractual clauses that address the specific restriction on the export of personal data by its EEA customers to it as processor. This kind of approach should work for direct controller-processor transfers to a cloud provider that uses its own infrastructure.[99]

---

[96] *Ibid*.

[97] See section 0 above.

[98] A29WP, "Work Programme 2012-2013" available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp190_en.pdf (accessed 22 March 2012).

[99] See http://www.ironmountain.com/legal/client-software-license-agreement.html - as at 8 September 2011, referring to the standard 2001 controller-processor clauses, see note 88 above. However, the clauses incorporated have since been superseded by a subsequent Decision, (see note 89 above) and the version of Iron Mountain's clauses accessed 22 March 2012 no longer incorporate any model clauses.

However, there are limitations with using model clauses. They were designed for controller-to-controller or controller-to-processor transfers. They cannot be used if, as we have argued is the case in some scenarios,[100] the cloud provider is not even a processor. In such a scenario, the cloud user/controller would need to find some other exception or justification for the data export.

Also, the model clauses do not cover fully all the sub-provider scenarios that are common with cloud computing (assuming here that cloud providers are "processors"). In particular, they "apply only to subcontracting by a data processor established in a third country of his processing services to a sub-processor established in a third country". [101] This means that an EEA controller may use the model clauses for cloud computing involving non-EEA sub-providers (e.g. a SaaS or PaaS provider that utilises the infrastructure of a non-EEA IaaS or PaaS sub-provider), as long as its initial provider is established outside the EEA. However, if the initial cloud provider is established in the EEA, the model clauses cannot be used to enable data export to the provider's underlying non-EEA IaaS or PaaS sub-provider.

To enable data export in those situations, the EEA controller would have to enter into a direct contract with the non-EEA processor (or strictly, sub-processor), containing the model controller-processor clauses. Alternatively, the controller must authorise the EEA processor (e.g. in the agreement between them) to enter into a contract on its behalf with the non-EEA sub-processor incorporating those model clauses. Ad hoc contracts are another option here, but they must meet all the usual requirements, and several data protection authorities reserve the right to review any such contracts and authorise (or decline) data exports based on the contract.[102]

As the model clauses do not enable EEA cloud providers to transfer data to non-EEA sub-providers, this may incentivise EU customers to use non-EEA cloud providers, in order to achieve greater flexibility in terms of transfers to sub-processors. This seems to be a major limitation of the new model clauses and is a significant practical disadvantage as many EEA providers rely on the infrastructure or platforms of non-EEA IaaS and PaaS providers such as Amazon Web Services, Google App Engine or Microsoft Windows Azure. In order to remove the current disincentive for EEA controllers to use EEA cloud providers, it would be desirable to rectify this situation, including clarifying how processors' place of "establishment" is determined for this purpose.

Furthermore, in order for a transfer to be recognised for adequacy purposes, the model clauses must be used without modification, although they can be part of a larger

---

Iron Mountain is in fact also on the Safe Harbor list, available at http://safeharbor.export.gov/companyinfo.aspx?id=10165 (accessed 22 March 2012), so it may have decided it did not need to rely on model clauses. However, model clauses may be helpful in addition, to address other DPD requirements.

[100] CLP Controllers/Processors Paper, see note 2 above.

[101] The 2010 Decision, see note 89 above, recital 23.

[102] A29WP, *FAQs in Order to Address Some Issues raised by the Entry into Force of the EU Commission Decision 2010/87/EU of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries under Directive 95/46/EC (WP 176)* (2010).

contract whose other provisions deal with other matters. Also, the controller-processor model clauses only apply to EEA-established controllers, so they would not permit a non-EEA established controller, to whom EU Data Protection Laws may apply due to its use of equipment in the EEA (e.g. a data centre), to re-export personal data. Last but not least, many Member States insist on advance authorisation of contracts (e.g. Austria, Belgium, Bulgaria, Croatia, Denmark, Estonia, France, some German states, Greece, Lithuania, Luxembourg, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia and Spain), or the filing of contracts, sometimes in ways which effectively amount to imposing a requirement of prior approval, in some cases even though the contracts incorporate the model clauses.[103]

A final point on model clauses is that different sets must be used for controller-controller and controller-processor transfers. While cloud providers should be treated as processors (or not even that)[104] in some cases a cloud provider may risk being considered a controller. This may be the case, for example, if it uses the personal data for its own new purposes or discloses it to an unauthorised third party,[105] or perhaps even because it controls the security measures. In such a case, if the contract with the provider had utilised the processor-processor clauses, the "wrong" clauses may have been used, and the export accordingly rendered unlawful. In practice both sets of clauses are sometimes used, to address the not uncommon situation where it is unclear whether a provider is purely a processor or may be a controller, for example because it determines its security measures.

6.4. BCRs

BCRs for private cloud computing within a corporate group have been mentioned above. This is the most obvious use of BCRs in cloud computing. However, in practice BCRs are cumbersome, costly and time-consuming to obtain, so corporate groups are unlikely to go through the BCR approval procedures simply for private cloud computing purposes. The BCR approval procedures could therefore benefit

---

[103] C Kuner, see note 5, at 4.27 and Appendix 12 (list of filing requirements). The draft Regulation ch 5 would explicitly permit transfers using model clauses approved by European Commission or supervisory authorities under the specified mechanisms. This is helpful as it should mean individual authorities should no longer be able to require prior authorisation of transfers incorporating such clauses.

[104] CLP Controllers/Processors Paper, see note 2 above.

[105] For a situation where a processor was considered to have arrogated to itself the role of controller, see the SWIFT opinion, note 25 above. Here Belgian financial messaging service provider SWIFT, which facilitates transactions between financial institutions, had decided, without informing its member institutions, to comply with US subpoenas, and allowed the US Department of the Treasury to view or search data held in SWIFT's US data centre. SWIFT was considered to have become a controller as it had exceeded its authority as a processor; it had "the power to take critical decisions with respect to the processing, such as the security standard and the location of its operating centres...". Contractual terms stipulating that SWIFT was to act as a processor did not prevent it from being considered a controller on the facts.

from streamlining, harmonisation and compulsory recognition by authorities across the EEA.[106]

Potentially, BCRs could have broader utility if, for example, the A29WP were to permit BCRs for transfers within the corporate group of a processor, e.g. cloud provider. There have been calls for processor BCRs for some time.[107] It may also be worth considering whether BCRs could be used for transfers within a community cloud. Although community members are not necessarily part of the same corporate group, they may have enough interests in common, as for example government authorities or members of highly-regulated sectors like financial services or pharmaceutical companies, that it may be feasible for them to agree and sign up to a single legally-binding self-regulatory code which will be enforceable by data subjects.

It may also be possible to employ hybrid models that combine BCRs with model clauses for processors.

6.5. Regional Clouds

The easiest practical solution currently is to use a regional cloud. As mentioned above,[108] some IaaS or PaaS providers offer customers the option to select broad geographical regions where their data are to be stored or their applications hosted, often on an individual basis e.g. one application in one region, another application in another.[109] For example, a cloud user may choose to confine its data to the European region (rather than the US, for instance).

However, these providers generally do not state whether their European data centres are confined to the EEA.[110] This matters because Europe includes some countries that are not in the EEA, such as Albania and Monaco. For example, Microsoft's European sub-regions for its Windows Azure PaaS service are simply designated as "North Europe" and "Western Europe", while Google Storage for Developers only offers a

---

[106] There are signs of some States trying to streamline procedures, most recently Belgium. See Hunton and Williams LLP, "Belgium Simplifies the Authorization Procedure for Binding Corporate Rules" (2011) *Privacy and Information Security Law Blog* available at http://www.huntonprivacyblog.com/2011/08/articles/european-union-1/belgium-simplifies-the-authorization-procedure-for-binding-corporate-rules/ (accessed 22 March 2012). However, procedures need to be streamlined across all Member States if BCRs are to become more practicable. The draft Regulation arts 42(2) and 43 would explicitly recognise BCRs, which is helpful.

[107] See e.g. V Bange, "Is It Time for the European Union to Consider Binding Corporate Rules for Data Processors?" (2010) 10(6) *WDPR* 4. The draft Regulation would explicitly permit processor BCRs, which is helpful. However, the entities concerned must still be in the same corporate group.

[108] See sentence containing note 63 above.

[109] E.g. Amazon Web Services and Microsoft Windows Azure – CLP Contracts Paper see note 10 above. Google recently introduced the ability for users to specify storage of their data in "buckets" only in Europe, or only in the US - Google, "Google Storage for Developers API Overview" available at http://code.google.com/apis/storage/docs/developer-guide.html#specifyinglocations (accessed 22 March 2012), and N Joneja, "Google Storage for Developers Open to All, with New Features" (2011) *Google Code Blog* available at http://googlecode.blogspot.com/2011/05/google-storage-for-developers-open-to.html (accessed 22 March 2012).

[110] In *Odense*, see note 49 above, the Datatilsynet pointed out that "It has not been stated whether all of Google Inc.'s data centres in Europe are located within the EU/EEA".

choice of "Europe" or "United States". Amazon for EC2 does specify US East (Northern Virginia), US West (Northern California), EU (Ireland), Asia Pacific (Singapore), and Asia Pacific (Tokyo). Furthermore, even providers that allow customers to choose regions do not commit contractually, in their terms of service, to keep the relevant data or applications in the chosen region.[111]

All this suggests that, in defining regions for users to select, the providers still primarily have in mind technological issues,[112] rather than regulatory concerns. Specifying that a European region (where the provider's data centre is located) is in the EEA could make the provider more attractive to DPD-conscious users who need to keep their data within the EEA, so it seems surprising that more providers do not stipulate the specific European countries in which their regional data centres are located.

In practice many users will know that, for example, Microsoft's European data centres for cloud customers are located in Ireland and Amsterdam,[113] and those users may therefore be willing to take a view on that basis. However, for users who rely on regional storage to avoid infringing the data export restriction, the most satisfactory position is that providers should undertake contractually that data designated for storage in the EEA will not be moved outside the EEA.

It is not inconceivable that in future providers could use data centres on ships flying EEA flags in international waters.[114]

7. The way forward?

The DPD's data export restriction rules are neither sufficiently clear nor harmonised effectively across Member States, particularly the concepts of transfer and data location. This causes legal uncertainties in relation to the use of cloud computing. Also, the DPD's drafting did not properly take into account the use of the Internet, let alone cloud computing. The DPD's intense and narrow focus on data location made

---

[111] Although the regionalisation may be an enforceable representation - CLP Contracts Paper see note 10 above. Note that storage of personal data in EEA data centres does not preclude its export in some circumstances, e.g. some of the provider's support staff may be located outside the EEA, but may need access to data in the EEA data centre to investigate service problems. In such a case, access by the support staff would be restricted and would require e.g. use of model clauses or Safe Harbor, or some other solution.

[112] Reducing latency, i.e. increasing speed of response. This is improved with geographical proximity of the user to the data centre storing or operating on the data.

[113] See e.g. Microsoft, "Microsoft's Cloud Data: Reliable, Resilient and Secure" (2 August 2011) *Telegraph* available at http://www.telegraph.co.uk/sponsored/technology/microsoft-cloud-computing/8667528/Microsofts-cloud-data-reliable-resilient-and-secure.html (accessed 22 March 2012).

[114] Google has patented floating data centres (CLP Applicability Paper, see note 2 above), although currently intended to be based in territorial waters. It would be possible for a country to exempt from its national laws all data processed in data centres situated on its territory (or recognise such data centres diplomatically as territory of another country) where, e.g., the data do not originate from that country and do not relate to its citizens, but are imported and re-exported. In a sense the French CNIL ruling mentioned in that Paper is a step in that direction. It remains to be seen to what extent such "data havens" may be promoted by countries wishing to encourage the building and use of data centres on their territory.

some sense when data could normally be transported between countries only by physically carrying storage media across borders. With the inception of the Internet, personal data may be emailed, instant messaged or tweeted or copied to recipients in multiple countries across the globe in an instant, as well as being made available internationally on websites. The concept of "location" is increasingly meaningless as well as irrelevant to data protection laws, given the ease of remote access to data.

The DPD's focus on data location should not obscure the underlying purpose of its data export restriction, namely data protection. In the data export restriction context, the specific objective was, and remains, to protect personal data against access by unauthorised persons. Unauthorised use is another risk, but data cannot be used without first being accessed, so, rather than focusing on data export, the DPD should consider protection against unauthorised access by third parties as the first line of defence, because preventing unauthorised access protects against unauthorised use.

We argue the DPD's rules should accordingly focus on restricting unauthorised access, rather than restricting data export. In other words, what matters most is not where information is stored, but who can read it, i.e. who is able to obtain access to it in intelligible form.

Where data are strongly encrypted and the decryption keys securely managed, the data's location should be irrelevant. Even if such encrypted data are stored in a third country, unauthorised persons would not be able to access data in intelligible form without the key.[115] Conversely, keeping data within the EEA does not guarantee better protection. Where data are stored unencrypted (or only weakly encrypted), even if the storage equipment is located within the EEA, unauthorised persons may be able to access intelligible data by hacking into the storage equipment, and/or the provider storing data on behalf of the cloud customer may technically be able to access the data by logging into the customer's account, and indeed may be compelled by a foreign law to do so. For example, the law of the provider's (third) country of incorporation may require it to disclose its customer's data (wherever stored) to its home law enforcement authorities.[116]

---

[115] We argue that the DPD should no longer legally prohibit data export as such, because that restriction is outdated given technological developments such as the internet and encryption. Discussion of encryption technicalities is beyond the scope of this paper. Those who use cloud computing to process personal data, of which they are controllers, may encrypt such data before upload for cloud storage. They therefore have the decryption key (although the provider may not). On receiving data subject access requests they may retrieve data for decryption offline in order to meet that request. As for operating on personal data in the cloud in encrypted form, work continues on homomorphic encryption - see the CLP Personal Data paper, note 2 above. Ensuring data subject rights may be met in other respects is not a data export concern as such, but raises general issues arising equally whether data are kept within the EEA or transferred outside it. Therefore we do not cover them in this paper.

[116] There was widespread reporting of Microsoft's acknowledgement, at the launch of its SaaS service Office 365, that, as US corporations must comply with US laws, it could not be guaranteed that data held in EU-based data centres would not leave the EEA should a request for such data be made under the US PATRIOT Act. This led to questions being raised at European Parliament level - S Veld et al, "Access to EU data by US Authorities" (2011) *European Parliamentary Questions 13 July 2011* available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2011-006901+0+DOC+XML+V0//EN (accessed 22 March 2012). Subsequently, Google stated that "As a law abiding company, we comply with valid legal process, and that - as for any US based company - means the data stored outside of the U.S. may be subject to lawful access by the U.S. government…".

The DPD's assumption that data can be accessed by persons in a third country, simply because data are stored in that country, is undermined not only by the Internet but by cloud computing. Depending on the setup of the system, if authorities in the third country where a data centre is located should seize one server or even all equipment in the data centre, that may not necessarily result in their being able to read any personal data in intelligible form, due to the use in cloud computing of data fragmentation, proprietary file systems, and perhaps even distribution of parts of the relevant data across different data centres. However, if third country authorities obtain the co-operation of the provider, they will generally be able to access unencrypted or weakly encrypted data, whether held in EEA or non-EEA data centres.[117]

In cloud computing, access to data in practice depends on two main factors:

- whether the user has encrypted the data strongly before its transfer (and manages the keys securely with the provider not having the key), and
- whether the design of the provider's systems gives it the technical ability to access users' data (e.g. the system could involve all data being encrypted strongly by default on the user's local computer such that only the user has the key), and, if so, who has authority or influence over the provider.

We suggest that the DPD's legal restriction on data export be abolished.[118] Art 17 DPD already legally requires controllers (and, indirectly, processors) to take appropriate technological and organisational measures for protecting personal data, to ensure a level of security appropriate to risks represented by the processing and the nature of the data, having regard to the state of the art and implementation costs. Data protection laws should, instead of restricting data export as such, focus on requiring appropriate accountability, transparency and security measures that take into account cloud computing's characteristics and many providers' status as neutral intermediaries.[119] They should do so in a technologically-neutral way, rather than in an overly prescriptive way that legally requires exact technologies which may in turn

---

L Constatin, "Google Admits Handing over European User Data to US Intelligence Agencies" (8 August 2011; updated 16 August 2011) *Softpedia* available at http://news.softpedia.com/news/Google-Admits-Handing-over-European-User-Data-to-US-Intelligence-Agencies-215740.shtml (accessed 22 March 2012). Both corporations were reported as stating that they would inform affected users of requests, "whenever possible". However, the issue raised is not new – see e.g. J Collins, "Warning against Cloud Computing Usage" (6 February 2010) *Irish Times*. Such a situation may put the provider between a rock and a hard place, as acceding to US authorities' requests may comply with US law but may breach EU Data Protection Laws – see SWIFT, note 25 above.

[117] CLP Personal Data Paper, see note 2 above.

[118] On accountability, Canada's *Personal Information Protection and Electronic Documents Act 2000* does not prohibit data export or restrict data location per se, but instead makes clear that organisations are responsible for personal information under their control, even when transferred to a third party for processing, and must use contractual or other means to provide a comparable level of protection during such processing. In *Odense*, see note 49 above, the Datatilsynet considered that a controller cannot ensure security measures are met unless it knows at all times the location of its data. With respect, this view seems not to take into account technological realities of encryption and cloud computing architecture and operations. However, the lack of transparency by cloud providers as to their storage and security policies and techniques has not assisted the debate.

[119] CLP Controllers-Processors Paper, see note 2 above.

become outdated. However, the proposals on security and accountability in the draft Regulation, which for example would impose direct security requirements on processors, are beyond the scope of this paper.

Although we argue that the data export restriction should be replaced by requirements regarding accountability, transparency and security, if the restriction is retained then it is important to clarify:

- whether it applies to the location of personal data (i.e. location of the underlying data centre(s) used) or the geographical location of the recipient (and if so, which – principal place of business, or jurisdiction of residence or incorporation?), including the issue left open in *Lindqvist*;[120]
- what is meant by "adequate protection" – the laws of the third country, the measures taken by the recipient/importer, etc?
- the significance, if any, of the exporter's knowledge and/or intention regarding the relevant location should be clarified.

The draft Regulation would, rather than abolish data export restrictions, create additional restrictions on transferring personal data outside the EEA. Without an adequacy decision by the European Commission, transfers would be permissible only by adducing "appropriate safeguards" for data protection in a "legally binding instrument". It is envisaged in particular that transfers may be based on BCRs, model clauses adopted by the Commission, or clauses adopted or authorised by a supervisory authority. BCRs must be approved, however, and contracts must either be pre-approved, by the Commission or a supervisory authority, or a specific prior authorisation must be obtained on a case by case basis[121] This may eliminate the ability for authorities to allow controllers to make their own decisions on adequacy[122] and seems retrograde as it could increase bureaucracy and requests for pre-approvals, consequently increasing the workload of regulators whose resources might be better spent on investigating and enforcing breaches than approving routine transfers. It seems unfortunate that the opportunity was not taken to permit appropriate safeguards to be adduced by technological means, such as by the controller using encryption and taking its own backups.

One positive aspect is that the draft Regulation art 44(1)(h) would introduce a derogation permitting transfers necessary for "the purposes of the legitimate interests pursued by the controller or the processor". However, that would only apply where transfers are not "frequent or massive" and the controller or processor has, based on assessing "all the circumstances surrounding the data transfer operation or the set of data transfer operations", adduced appropriate safeguards to protect personal data where necessary. While a 'legitimate interests' justification could be helpful, the exclusion of transfers that are "frequent or massive" might undermine substantially the practical utility of the justification. It is insufficiently clear what transfers would qualify as "frequent or massive". The focus should instead be on adducing appropriate

---

[120] See paragraph containing note 38 above.

[121] Draft Regulation, art 42.

[122] Discussed at s 0 above.

safeguards whatever the size or frequency of transfers. Guidance as to what would be appropriate safeguards in this situation, and that safeguards may be technological not just legal, would assist here.[123]

Additionally, the detailed rules on data export need harmonising across the EEA, for several reasons. Full harmonisation would reduce compliance burdens for entities operating in several Member States. Furthermore, it would address any concerns of 'leakage' of personal data by a transfer of data to another EEA State, which transfer must be permitted under the DPD, and thence outside the EEA, where the transferee's restrictions on data export are less stringent than those of the originating EEA State. The draft Regulation aims to harmonise the position, being in the form of a regulation with direct effect rather than a directive but, in its current form at least, would be unlikely to achieve this objective due to lack of both clarity and certainty.

In relation to the Safe Harbor, the many uncertainties discussed above need to be addressed in order for the Safe Harbor to be a truly safe framework enabling EEA controllers to use US cloud providers. In any review of the Safe Harbor it would be desirable to clarify that processors may use the Safe Harbor. It would also be important to clarify the mapping of EU controller/processor concepts and responsibilities to Safe Harbor principles, and indeed the controller/processor distinction more generally needs attention.[124] The US and EU need to agree clearly which country's rules apply to data exported under the Safe Harbor, and to what extent. In relation to onward transfers, the position and requirements need clarification, e.g. the meaning of "subscribes to" Safe Harbor principles. The rules should take account of the potential use by Safe Harborite providers of non-US data centres and/or of sub-providers (US or otherwise), and the situation where providers may have possession of data but not access to intelligible data (i.e., that transfer does not always equate to disclosure). The inconsistencies in Safe Harbor acceptance across the EU Member States also need to be eliminated. Agreeing these issues is unlikely to be a quick process.

The position of processors and sub-processors in the context of exported data also needs specific consideration. Specific issues include the extent to which a cloud provider may become a controller through choosing to use a data centre located outside the EEA, or through choosing to use a sub-provider; how a processor's or sub-processor's state of establishment is determined, and which Member State's security requirements, if any apply, to providers.[125] Possible solutions may involve the promulgation of processor-to-processor model clauses to enable use of layered cloud computing, in particular allowing EEA processors to transfer data to non-EEA sub-processors, BCRs for processors, and clarification regarding the Safe Harbor uncertainties. The draft Regulation would permit BCRs for processors, but other uncertainties remain to be addressed.

In summary, restricting data export per se rather than emphasising security, accountability and transparency (wherever in the world data are processed) may hold

---

[123] Art 44 (7) of the draft Regulation would empower the Commission to adopt delegated acts "for the purpose of further specifying… the criteria and requirements for appropriate safeguards".

[124] CLP Controllers/Processors Paper, see note 2 above.

[125] CLP Applicability Paper, see note 2 above.

back the efficient use of cloud computing, and the draft Regulation would exacerbate this.

Appendix. Practical Application: Common Scenarios

The tables below illustrate the issues discussed, using alternative cloud computing scenarios involving a cloud user Customer, being a controller of personal data that are to be processed in the cloud.

Key to abbreviations:

Customer	Customer or user of cloud computing services; The Customer will usually be a controller of personal data.
Provider	Provider of cloud computing or related services.
Multiple	Several data centres in different countries are used between which personal data may flow automatically.

For each alternative scenario we consider whether EU Data Protection Laws would permit a data export. For simplicity we assume, unless otherwise stated, that in scenarios where Customer is subject to EU Data Protection Laws, any export would be from, and under the law of, the Member State which applies to Customer due to its being established or using "equipment" or "means there".[1]

[1] For detailed discussion of data protection jurisdiction raised by these scenarios, see CLP Applicability Paper, note 2 above.

1. Private Cloud (Self-Hosted)

With a self-hosted private cloud, we assume Customer controls the location of the data centre(s) used, even though it may not be the legal owner of those data centre(s) and/or of the equipment used.

	Cloud customer established in	Data centre location	Position
1	EEA	EEA	No data export issue.
2	EEA	Non-EEA	Data export issue – customer must find an exception, or a way to ensure adequacy of protection (see part 6, above).
3	Non-EEA	EEA	Customer may become subject to the DPD if, through its use of an EEA data centre, it is considered to have an "establishment" in the EEA or to make use of equipment in the EEA for processing personal data. If so, it would then have to comply with the data export restrictions and other DPD requirements, even if it initially "imported" data to the EEA data centre for processing and re-export following the processing, and even if the data originated outside the EEA and related to non-EEA persons.[127]
4	Non-EEA	Non-EEA	No DPD issues if the customer has no other EEA connection.
5	EEA	Multiple	If personal data are confined to EEA data centres – see 1. If personal data could be processed in non-EEA data centre – see 2. Furthermore, differences in data export rules in different Member States could mean that personal data may legally be exported from a data centre in one State in circumstances when it could not be from a data centre in another. This might, for instance, motivate Customer to use only (or as the "end point") data centres in States with less stringent restrictions.

[127] CLP Applicability Paper, see note 2 above.

6	Non-EEA	Multiple	Example: a US corporation with a private cloud using multiple data centres, including in the EEA. If personal data could never be processed in the EEA – see 4. If personal data could be processed in EEA data centre – see 3 and, in relation to "export" from different Member States, see 5.

2. Using Provider[128]

The table below may apply to several possible models, where in each case Customer uses the services of a third party Provider, involving:

- a dedicated private cloud hosted/managed by the Provider or a third party. (We assume that, with a dedicated private cloud, a third party controls the location of data centre(s) used, although the location may be stipulated or restricted by Customer);
- a community cloud (e.g. entities in same corporate group); or
- a public cloud service.

We do not provide a separate table for situations where Provider uses a sub-provider (e.g. SaaS provider utilising IaaS/PaaS infrastructure). This is because, when a sub-provider is used, then, assuming Provider is not considered a controller through its choice of sub-provider or another reason,[129] the situation will essentially be as in the table below, but with Provider choosing the sub-provider used, and "Data centre location" referring to the location of the sub-provider's (or its ultimate sub-provider's) data centre. However, the more layers of providers there are, the less likely it is perhaps that Customer would be taken to know or intend any export, as discussed in the main body of this paper.

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

[129] This possibility has already been discussed - see note 17 above. If Provider is a controller, then the analysis regarding Customer's position applies to Provider equally, if Provider is subject to EU Data Protection Laws through being "established" in the EEA or using "equipment" or "means" in the EEA – see CLP Applicability Paper, see note 2 above.

	Customer established in	Provider established in	Data centre location	Position
7	EEA	EEA	EEA	No data export issue for either Customer or Provider. Customer must obviously comply with the relevant national implementation of the DPD ("EU Data Protection Laws"), including as regards its contract with Provider if Provider is its "processor".
8	EEA	EEA	Non-EEA	Customer - no data export issue if *Lindqvist* is followed (on the analogy of uploading data to an EEA web host), although other DPD requirements will apply. However, under *Odense* there would be an export, and in practice the cautious view would be to assume an export, and seek a solution enabling export. This suggests Customer ought to inquire as to the location of the data centre ultimately used by Provider. Provider - if Provider is considered to determine the "purposes and means" of processing, for example because it chose the sub-provider or chose (or, perhaps even, did not inquire into) the location of the data centre used, it risks being considered a "controller" - see the SWIFT scenario[127] – and thus would be subject to the data export restriction and other data protection rules.
9	EEA	Non-EEA	EEA	Customer - no data export issue, assuming the initial transfer was to the EEA data centre. This is the "regional data centre" solution used by some non-EEA providers. Provider – no export issue similarly.[128]

[127] See notes 25, 44 and 105 above. See also CLP Applicability Paper, note 2 above.

[128] However, if Provider determines the purposes and means of processing the data, it risks being considered to use equipment in the EEA to process personal data and thus being caught by the DPD as controller. See CLP Controllers/Processors Paper, note 2 above. We argue that in many cases a provider should not be treated as a processor: *Ibid*. A separate question is whether an EEA court would accept jurisdiction over Provider, which it may be more likely to do if Provider owns (or perhaps even just uses) an EEA data centre.

	Customer established in	Provider established in	Data centre location	Position
10	EEA	Non-EEA	Non-EEA	Customer - data export issue, see 8. Provider - see 8; but if Provider has no EEA data centre and no other EEA connection an EEA court may be less likely to accept jurisdiction over it and there may be issues regarding whether any EEA judgment could be enforced against Provider, in practice.
11	Non-EEA	EEA	EEA	Customer - re-export issue may arise as in 3, if the data are to be transferred outside the EEA after the cloud processing. Also, Customer risks being subject to EU Data Protection Laws if, through its use of an EEA provider or EEA data centre Customer is deemed to make use of equipment in the EEA, as with Provider in 8. However, the same issue arises as for Provider in 8 regarding whether an EEA court would accept jurisdiction over Customer or whether any EEA judgment could be enforced against Customer in practice. If Customer is subject to EU Data Protection Laws, there may be a re-export issue as in 3. Provider - no data export issue even if it is a controller.[129]
12	Non-EEA	EEA	Non-EEA	Customer - no data export issue (if data are never processed in any EEA data centre, there should be no issue of a "transfer" to outside the EEA) and (assuming use of an EEA provider is not using "means" in the EEA), if it has no other EEA connection, should not be subject to EU Data Protection Laws. Provider - if Provider is a controller, Provider could be subject to EU Data Protection Laws wherever in the world processing takes place (although if data were never in the EEA, there is no data export issue).
13	Non-EEA	Non-EEA	EEA	Customer - as 11. Application of EU Data Protection Laws may perhaps be less likely if its only EEA connection is through its non-EEA provider using an EEA data centre. Provider - as 9.
14	Non-EEA	Non-EEA	Non-EEA	No DPD issues for either Customer or Provider if it has no other EEA connection.

[129] Also, when acting for EEA controllers the Provider should have certain contractual obligations imposed on it by the controller, in particular implementing appropriate technical and organisational measures to protect personal data as defined by the laws of the Provider's EEA State of establishment (under art 17(3)). The Provider may apply similar measures when processing data for other customers.

	Customer established in	Provider established in	Data centre location	Position
15	EEA	Anywhere	Multiple	Similar issues to above, depending on whether data can be restricted to EEA data centres or can move to non-EEA data centres, and (for Provider) whether EU Data Protection Laws apply to it. Differences in different Member States' export restrictions may be relevant, as in 5.
16	Non-EEA	Anywhere	Multiple	Similar issues to above, depending on whether EU Data Protection Laws apply to Customer through use of EEA provider or data centre, and/or to Provider through use of EEA data centre, and also depending on whether data can be kept within only non-EEA data centres or may move to non-EEA centres or be re-exported after the processing. If EU Data Protection Laws apply and personal data may be exported, differences in national data export restrictions may be relevant, as in 5.