COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Cross border data transfer: Complexity of adequate protection and its exceptions

Pardis Moslemzadeh Tehrani *, *Johan Shamsuddin Bin Hj Sabaruddin*, *Dhiviya A.P. Ramanathan*

Faculty of Law, University of Malaya, Kuala Lumpur, Malaysia

Keywords:
Cloud computing
Cross-border data
General data protection regulation
US
EU

A B S T R A C T

The majority of the fear that exists about the cloud arises due to the lack of transparency in the cloud. Fears have persisted in relation to how the data are frequently transferred in a cloud for various purposes which includes storing and processing. This is because the level of protection differs between countries and cloud users who belong to countries which provide a high level of protection will be less in favour of transfers that reduce the protection that was originally accorded to their data. Hence, to avoid client dissatisfaction, the Data Protection Directive has stated that such transfers are generally prohibited unless the country that data is being transferred to is able to provide 'appropriate safeguards'. This article will discuss the position of the Data Protection Directive and how the new General Data Protection Regulation differs from this Directive. This involves the discussion of the similarity as well as the differences of the Directive and Regulation. In summary, it appears that the major principles of the cross border transfer are retained in the new regulation. Furthermore, the article discusses the exceptions that are provided in the standard contractual clause and the reason behind the transition from Safe Harbor to the new US-EU Privacy Shield. This article subsequently embarks on the concept of Binding Corporate Rule which was introduced by the working party and how the new regulation has viewed this internal rule in terms of assisting cross border data transfer. All the issues that will be discussed in this article are relevant in the understanding of cross border data transfer.

1. Introduction

When one speaks about the cloud, one is aware of the responsibility that exists because of the data that is being stored. It is important to see how such data is administered and the methods used in preserving the data that is being stored. It has been an ongoing issue that the public fears data governance in the cloud, in particular concerning access to personal data that is accorded to any third parties who do not have permission to access such data. This fear is amplified when the cloud transfers personal data across the border of the jurisdiction that the data was initially stored in. Although there are fears of the data being in the wrong hands, restricting and limiting the flow data is also an undesirable outcome. This is because, global transfers of information are now a common

* *Corresponding author*. Faculty of Law, University of Malaya, Jalan Universiti, Wilayah Persekutuan, 50603 Kuala Lumpur, Malaysia.
E-mail address: pardismoslemzadeh@um.edu.my (P.M. Tehrani)

https://doi.org/10.1016/j.clsr.2017.12.001

and essential component of our daily lives which drive the global economy and a seamless transfer of information is crucial for the growth and success of the global economy.[1]

Nevertheless, it is not easy to safely manage data transfers since each respective country has separate data protection rules that are used for the governance of personal data. Hence, the rigidity and level of protection also differs between countries. It is indeed undesirable to have the data protection standard lowered due to the need to transfer the data across a border. Thus it can be seen that the issue of jurisdiction is a vital area in cloud computing. Despite the fact that the cloud is described as something abstract, distant and obscure, in reality, it uses the physical computer, with physical storage facilities housed in physical structures[2] which can be subject to misuse. This requires appropriate data protection procedures in order to ensure the privacy and security of such data.

This article begins with a discussion of cross border transfers which includes the approach taken by both the directive and new regulations. The article later advances to a discussion of the exceptions, that have long lasted in the transfer of data, which is the model clause, Safe Harbor and Binding Corporate Rule (BCR). This discussion will also involve the discrepancies and problems faced within it. Finally, this article will conclude by mentioning how the BCR is an ideal method to curb the problem in cross border data transfers and the advantages and disadvantages that are entailed in this corporate rule.

2. The legal issues in cross border data transfer

As known to many, the cloud can work as a seamless and borderless entity which is not restricted to one area or jurisdiction. This phenomenon however, is not ideal because the information that the cloud deals with involves the personal and sensitive data of the end user. This increases concerns regarding the privacy and security of the data since there are already fears that cloud services permit users to upload, share and download copies of software and other files without the authors' permission and to access copyrighted works beyond or in violation of access limitations.[3]

There are many qualms that exist pertaining to the cross border transfer of personal data in the cloud. However, the key concern of governments is ensuring adequate protection of personal electronic data across borders as the government has implications for the ability to transmit and send information across borders.[4] This is because each country has a different approach to protecting the privacy of particular data. This can be seen by the fact that the European Union has prevented the export of data to countries with less strict data privacy laws.[5] This law was introduced to address the different levels of data protection that are available within the EU itself.

Furthermore, there is also a growing risk of cyber-attacks either by individuals, organised criminal networks or governments. Moreover, due to its wide accessibility, there is also concern about intellectual piracy and illegal copying of any data that is available. These concerns increase in cross border transfer cases since there is no transparency in the cloud regarding the act of transfer. This means the personal data that is concerned may be subjected to inadequate data protection. Hence, upon learning about the importance of data protection and the fears that exist, this article will discuss how both the Data Protection Directive (DPD) and the General Data Protection Regulation (GDPR) deal with the issue of cross border transfers.

2.1. *Adequate protection rule in Data Protection Directive's position 95/46/EC*

It should be borne in mind that the General Data Protection Regulation will not take effect until 25 May 2018 due to the two year transition period. Thus, the data protection in EU is still governed by the former Data Protection Directive and the directive is still in force in issues regarding the cross border transfer of personal data in the cloud. In the Data Protection Directive (DPD), the directive prohibits any transfer of personal data to a third country if the third country has not provided an adequate level of protection of the personal data. This can be seen in Article 25(1) of the Directive which prohibits the transfer of personal data to a third country (i.e. a country or territory outside the European Economic Area (EEA)) unless that third country provides an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.[6] If the adequacy of the country has not yet been accessed by the European Commission, the Commissioner carries out the authorization procedure and the adequacy procedure. This can be described in a hierarchy because it starts with Article 25(1) which requests adequate protection in the country that the data is being transferred to, followed by the 'adequate safeguards' method under Article 26(2), then use of the exceptions[7] at the bottom.[8] The article '*A walk in to the cloud and cloudy it remains: The challenges and prospects of 'processing' and 'transferring' personal data*'

[1] Hunton & Williams, 'Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity' US Chamber of Commerce [2014] <https://www.hunton.com/images/content/3/0/v2/3086/Business_without_Borders.pdf> accessed 4th May 2017.

[2] Hon, W. Kuan and Millard, Christopher, 'Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4 'SCRIPT-ed, Vol. 9:1, No. 25; QMUL Research Paper No. 85 [2011] <https://ssrn.com/abstract=2034286> accessed 18th April 2017.

[3] Lothar Determann, 'What Happens in the Cloud: Software as a Service and Copyrights', 29 Berkeley Tech. L.J. [2015].

[4] Joshua Meltzer, 'The Internet, Cross-Border Data Flows and International Trade' Issue 22 (2013) <https://www.brookings.edu/wp-content/uploads/2016/06/internet-data-and-trade-meltzer.pdf> accessed 6th April 2017.

[5] Directive [1995] 95/46/EC.

[6] Sullivan, Clare Linda, 'Protecting Digital Identity in the Cloud: Regulating Cross Border Data Disclosure (2014). Computer Law Review and Technology Journal' [2014] Vol. 30, No. 2.

[7] Example; Safe Harbor EU-US.

[8] Samson Yoseph Esayas, A walk in to the cloud and cloudy it remains: The challenges and prospects of 'processing' and 'transferring' personal data Volume 28, Issue 6, December 2012, Pages 662–678 <http://www.sciencedirect.com/science/article/pii/S0267364912001756> accessed 7th April 2017.

Please cite this article in press as: Pardis Moslemzadeh Tehrani, Johan Shamsuddin Bin Hj Sabaruddin, Dhiviya A.P. Ramanathan, Cross border data transfer: Complexity of adequate protection and its exceptions, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.001