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.

has explained the reason being that the degree of protection slides down from the top with adequate protection in the whole country, to the middle only in the particular organization, and with no protection at the bottom of the hierarchy.[9] This clearly depicts the reason why it is preferred in such a manner and it is safe to assume that the ideal way is to provide adequate protection for the data transfer. Moreover, the commission has stressed how 'special precautions' must be taken in situations where the data is transferred to countries outside the EEA that do not provide EU-standard data protection. This is because without maintaining such precautions, the high standards of data protection that the EU has maintained since the directive will be undermined due to the transfers to other countries.[10] The commission has so far recognized Andorra, Argentina, Canada (commercial organizations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay as providing adequate protection.[11]

Alternatively, a business can transfer data across a border to a recipient country that does not provide adequate protection if it ensures that the place to which the data is being transferred has "adequate safeguards."[12] This involves the arrangement being made through a contract and the contract ensures that the personal data that is being transmitted is being adequately protected. This is known as a standard contractual clause (model clause) in relation to data transfer and the European Commission approved that such a method can ensure adequate safeguards for the data transferred. This is an exception to the adequate protection rule that the countries are required to adopt.

This article will discuss this standard contractual clause in the subsequent subsection. Moreover, it is worth mentioning that if the companies often send and transmit data to the export company, adopting a BCR is an easier option. BCRs have received strong support from the EU's data privacy regulators, which have published a number of guidance papers over the years to make it easier for industry to implement BCRs. This BCR will be discussed in detail in the final section of this article.

Despite the clear rules mentioned above, there are still discrepancies in the transferring of personal data to a third country. This is because the nature of cloud computing is not suitable for Article 25[13] DPD the case by case procedure because most of the data is transferred each millisecond. It is said that the rules regarding transfers to third countries are greatly limiting the seamless transfer of data.[14] Furthermore, the protection of personal data is not assured if one takes into account that the contracts of a large cloud computing company run on a take it or leave contract basis.[15] The new regulation however has made attempts to make some changes to the position of the cross border transfer of personal data.

2.2. *Improvement of the position of the adequacy protection rule in the General Data Protection Regulation*

On April 27 2016, the General Data Protection Regulation (GDPR) replaced the Data Protection Directive and it will take effect in the EU on May 25 2018.[16] The new GDPR is intended to strengthen the data protection rights of individuals within the EU (e.g., data portability, right to be forgotten, profiling, etc.) and, most importantly, it is meant to unify cross border data rules for organizations with footprints in more than one country.[17] Unification of the law serves as a good solution to issues in cross border data transfers since, as mentioned above, the differing law and data protection standard is the root cause of the rising fear in the general public. The GDPR adds new cross border data transfer rules to the previous Data Protection Directive which are primarily aimed at solving the discrepancies that are present in the new regulation.

Firstly, before looking at the differences between the directive and the new regulation, it is important to look at what rules have remained in the regulation; in other words, the rules that have been derived from and carried over from the old directive. The new regulation has retained the adequacy test in determining whether the country that the data is being exported to is indeed appropriate. This adequacy test is said to enable comprehensive transfers especially in those countries that are found to provide adequate protection.[18] It is also recognised that the test of adequate protection is transparent which is needed in ensuring fair and just governance.[19] This was specified in Article 25 of the Regulation. It stated that in assessing the principle of adequacy, the Commission must take into account certain elements. These elements are:

(a) *the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;*

[9] Ibid.

[10] European Commission, Commission decisions on the adequacy of the protection of personal data in third countries' <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm> accessed 8th April 2017.

[11] European Commission, Commission decisions on the adequacy of the protection of personal data in third countries' <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm> accessed 8th April 2017.

[12] Directive 95/46/EC.

[13] Data Protection Directive [1995] 95/46/EC, Article 25.

[14] B.J.A. Schellekens, 'The European Data Protection Reform in the light of cloud' (Master Thesis Tilburg University) <http://njb.nl/Uploads/2014/4/Master-thesis-Bart-Schellekens.pdf> accessed 8th April 2017.

[15] Ibid.

[16] Guidance Software, 'Cross border data privacy in' <https://www.guidancesoftware.com/docs/default-source/document-library/whitepaper/cross-border-data-privacy-in-focus.pdf?sfvrsn=6> accessed 9th April 2017.

[17] Ibid.

[18] United Nations Conference on Trade and 'Data protection regulations and international data flows: Implications for trade and development' New York and Geneva [2016]. <http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf> accessed 10th April 2017.

[19] Ibid.

(b) *the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and*

(c) *the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data*[20]

However, there are a number of struggles for instance in relation to determining whether a country has provided adequate protection. There are also struggles to accommodate jurisdictions with different approaches to data protection and in addition the test of determining the adequacy of the protection is itself a lengthy process.[21] There is also the model contract issue that has been retained. The 'model contracts' approach assesses whether the specific wording that appears in contracts provides a sufficient degree of protection for the transfer of personal data. This approach is only followed in the EU thus far. This approach has an advantage of allowing fast approval if the organization adopts this model contractual clause verbatim.[22] However, ensuring whether this model clause is up to date is cumbersome. These are some of the aspects that the new regulation has retained from the directive. In the new regulation, it has been specified that the jurisdictions which were declared adequate in the previous directive, will remain valid for a period of 5 years upon the implementation of the new regulation.[23] This applies to the model contract clauses as well.

Moreover, the new regulation has made some changes to the regulation which are aimed at solving the problems in cross border data transfers. There were changes made in the introduction of a code of conduct and certification mechanism, which are regarded as the two new safeguards of the GDPR.[24] Adherence to these codes of conduct by controllers or processors will help the controller to demonstrate its action provides adequate safeguards. This is governed by Article 31 and Article 48 which involve the approval of supervisory authority and the rules on monitoring the compliance of the code of conduct. Data protection certification demonstrates a controller's or processor's adherence to certain standards. This certification is said to be similar to the code of conduct mentioned above in respect to ensuring the adherence of the controller and processor to the data protection safeguard. Another important legitimate interests concept has been introduced as a new derogation, but its scope is very limited. The concept may be used where the transfer is not repetitive, concerns only a small number of data subjects, is necessary for compelling legitimate interests (not overridden by the rights of the data subject) and where the controller has assessed all the circumstances and adduced suitable safeguards with regard to the protection of personal data.[25] The derogation will apply if:

(a) *the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequate decision and appropriate safeguards;*

(b) *the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;*

(c) *the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;*

(d) *the transfer is necessary for important reasons of public interest;*

(e) *the transfer is necessary for the establishment, exercise or defence of legal claims;*

(f) *the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;*

(g) *the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.*[26]

This derogation, although limited in nature, has proven that the GDPR has promoted the idea of flexibility while limiting its scope to avoid any misuse of the derogation available. This is a new derogation aside from the other exceptions which are parallel to the directive. This derogation serves as an addition to the other exceptions which are available and will be discussed and analysed further on in this article.

Moreover, the EU has also improved the position of Binding Corporate Rule (BCR) in their new regulation. BCRs are internal rules adopted by a multinational group of companies which define its global policy with regards to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection.[27] Unlike the DPD, the GDPR has provided some guidance in regards to BCRs, which can be seen in Rec.108, 110; Art.47(1)-(3) which states that in order for a BCR to be legally binding on a group it must:

[20] General Data Protection Regulation [2016], Article 25.

[21] United Nations Conference on Trade and 'Data protection regulations and international data flows: Implications for trade and development' New York and Geneva [2016]. <http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf> accessed 10th April 2017.

[22] Ibid.

[23] General Data Protection Regulation [2016] 2016/679 Article 40 and Article 41.

[24] Anna Meyers, 'Top 10 operational impacts of the GDPR: Part 4 – Cross-border data transfers' (IAPP, Jan 16 2016) <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/> accessed 14th June 2017.

[25] General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), Article 49.

[26] Ibid.

[27] European Commission, 'Overview on Binding Corporate rules' <http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm> accessed 9th April 2017.

- *specify the purposes of the transfer and affected categories of data;*
- *reflect the requirements of the GDPR;*
- *confirm that the EU-based data exporters accept liability on behalf of the entire group;*
- *explain complaint procedures; and*
- *provide mechanisms for ensuring compliance (e.g., audits).*[28]

This helps to clarify the issue of the requirements for the BCR to be effective since it entails several advantages in relation to transferring data. Furthermore, the Data Protection Authority (DPA) must approve that BCRs fulfil the criteria set out in the GDPR[29] which are different from the directive because the directive did not specify any requirement for the approval of the BCR.

Moreover, there is also a change in regard to consent that must be obtained from the end user. The GDPR sets a higher standard for consent, but the biggest change is what this means in practice for the consent mechanisms.[30] The GDPR is clearer than the directive that an indication of consent must be unambiguous and involve a clear affirmative action[31] which is set by the directive. Tightening the rule surrounding consent ensures that there will always be genuine consent and ongoing control over how a data user uses their data, and ensuring an organization is transparent and accountable.[32] However, it is opined that the shift from unambiguous consent to "explicit" consent is unlikely to make very much practical difference for most organizations.[33] This is because they share great similarities but nevertheless do contain subtle differences.[34] The differences can be seen in situations where the data user has not explicitly consented but has provided an affirmative act that implies consent. This is accepted in the new regulation based on recital 32 which states that 'statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed'[35] connotes to consent. Thus, it can be seen that there is a subtle difference in both explicit and unambiguous consent.

On the other hand, the GDPR also allows cross border data transfer if the controller has a legitimate reason for the transfer. This distinguishes the GDPR from the old directive because the directive does not permit such transfers. This was specified in GDPR Rec.113; Art.49(1), (3), (6) A Cross-Border Data Transfer may take place if:

- *none of the other lawful bases applies;*
- *the transfer is not repetitive;*
- *it only concerns a limited number of data subjects;*
- *the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by those of the data subject; and*
- *the controller has adduced suitable safeguards for the transferred data.*[36]

Although narrow in nature, the GDPR allows another legitimate reason for the transfer of cross border data. Based on this, the GDPR has recognised the recent development and made an attempt to address this advancement. However, one might safely say that the GDPR did not make an extraordinary change from the position of the old directive. In fact, the GDPR has failed to acknowledge certain discrepancies such as the EU-US Safe Harbor which has recently been replaced by the US-EU Privacy Shield. The EU-US Safe Harbor principle can be referred to as an exception to the 'adequate protection' which is stated in Article 25.1 of the directive and the Article 25 of the regulation. There are two other exceptions to the adequate protection rule which are the BCR and the standard contractual clause. This article will embark on a discussion of the exception to the adequate protection rule, and whether the exception sufficiently ensures the appropriate data protection for the transferred data.

3. Exception or derogations to the 'Adequate Protection' rule

Based on the above section one can see how adequate protection is governed based on the directive as well as the new regulation. However, not all countries can meet the criteria required for adequate protection. Holding off the transfer of personal data because a country lacks in terms in data protection can be undesirable to both organizations and individuals. In such situations there are a few exceptions that may apply. The discussion that follows involves a detailed analysis of these exceptions.

3.1. *Standard contractual clause*

As mentioned above, in order for the transfer of data to occur, there has to be adequate protection accorded to the personal data that is being transferred. However, there are a number of exceptions, one of these being the protection accorded through the model clause (which is also referred to as a standard contractual clause). This is pursuant to Article 26(2) of the Directive which states that 'a Member State may 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 Article 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

[28] General Data Protection Regulation [2016] 2016/679, Recital 108.
[29] General Data Protection Regulation [2016] 2016/679, Recital 108.
[30] Information Commissioner's Office, '*Consultation: GDPR consent guidance*'<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf> accessed 11th April 2017.
[31] Ibid.
[32] Ibid.
[33] White & Case, 'Chapter 13: Cross-Border Data Transfers – Unlocking the EU General Data Protection Regulation' (22 JUL 2016) <https://www.whitecase.com/publications/article/chapter-13-cross-border-data-transfers-unlocking-eu-general-data-protection> accessed 10th April 2017.
[34] Phil Lee, 'The ambiguity of unambiguous consent under the GDPR' June 7, 2016 <http://privacylawblog.fieldfisher.com/2016/the-ambiguity-of-unambiguous-consent-under-the-gdpr/> accessed 4th May 2017.
[35] General Data Protection Regulation [2016] 2016/679, Recital 32.
[36] General Data Protection Regulation [2016] 2016/679, Rec.113; Art.49(1), (3), (6).

safeguards may in particular result from appropriate contractual clauses'.[37] Thus, this standard contractual clause can be considered as an adequate protection according to the directive.

This model clause came into play in December of 2004 when the European Commission recognized a set of standard contractual clauses proposed by seven leading business associations (including ICC) as satisfying the "adequate level of data protection" under the EU Data Protection Directive 95/46/EC for transferring personal data outside the EU.[38] There are a number of advantages that the model clause entails and below are some of the advantages that the standard contractual clause has to offer;

- Firstly, the standard contractual clause can be implemented quickly because it is preapproved as a successful method that complies with the Data Protection Directive in regards to transfer of personal data out of the EU
- Furthermore, the standard contractual clause commands automatic recognition by the Data Protection Authorities (DPA) and hence does not require any additional authorization
- Moreover, standard contractual clauses may be used for transfers to any countries (unlike the Safe Harbor which is confined to transfers to the US)
- Finally, the standard contractual clause can be used for external transfer and also works for intra-company transfer, which means it is not limited to corporate groups like the BCR.[39]

The European Commission has issued two sets of standard contractual clauses for transfers from a data controller in the EU/EEA to a data controller established outside EU/EEA and one set of model clauses for the transfer to a processor established outside of the EU/EEA.[40] The standard contractual clause explains the obligation of the importer and the obligation of the data exporter as well as the set of liabilities set by the European Commission. This aids in ensuring accountability and promotes responsibility to the parties involved. The liability involves the details of the party enforcing their rights as well as obtaining compensation. The clause also includes the option of dispute resolution being available to the parties through mediation. It also includes clauses that explain the governance of the personal data that is being transferred. Furthermore, the model clauses by the European Commission explain the termination of the contract according to the situation at hand.

The possibility for the controller or processor to use the standard data protection clauses adopted by the Commission or by a supervisory authority should not prevent the controller or processor from including a standard data protection clause in a wider contract nor does it prevent them from adding on other clauses. There can be variations to the contract adopted by the European Commission as long as it does not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.[41] However, the model clauses do entail a number risk in terms of data protection because the regulator has very limited rights to block model clause transfers. The authorities are only allowed to block model clause transfers when the clauses are not being complied with, or in some cases where the laws of the recipient's country mean that intended safeguards provided by the clause could be omitted or disregarded.[42]

The General Data Protection Regulation has permitted cross border data transfer if the controller or processor adduces appropriate safeguards in the form of model clauses. The new regulation has removed any further authorization from the DPA. This is the only change made in the new regulation in relation to the rule governing the model clauses. Moreover the new regulation has noted that the Commission may update or replace the existing model clauses. The existing model clauses during the era of the directive remain effective and valid up till today.

Based on this it can be seen that using model clauses is an approach which is workable and has served its purpose to date. Model clauses assist transfers which fail to satisfy the 'adequate protection rule'. However, the limited power for the authority to block does create concern in terms of data protection. The law should take a more pragmatic approach in determining the action which is required if any form of threat exists in the transfer of such personal data. Another method that aids in the transfer of data is the Safe Harbor principle which governs the transfer of data. The following subsection will discuss the issues surrounding this method of transfer.

3.2. *Cross border transfer between US and EU*

Before discussing the Safe Harbor principle, one must look at the different characteristics that led to attention being paid to this. As it can be seen above, the EU law is governed by a rule that gives enormous priority to data protection and ensures that the data is sufficiently protected before permitting a transfer to a third country. However, the position in the US is different as they do not have a single, overarching data privacy and protection framework. Many describe US data privacy laws as a

[37] Data Protection Directive, Article 26(2).

[38] International Chambers of Commerce, 'Final Approved Version of Alternative Standard Contractual Clauses for the Transfer of Personal Data from the EU to Third Countries (controller to controller transfers)' <https://www.inforights.im/media/1066/icc-data-controller-to-data-controller-contract-clauses.pdf> accessed 10th May 2017.

[39] Melinda L. McLellan and William W. Hellmuth, 'Safe Harbor is dead, long live standard contractual clause' (Data Privacy Monitor 2015) <https://www.dataprivacymonitor.com/enforcement/safe-harbor-is-dead-long-live-standard-contractual-clauses/> accessed 12th May 2017.

[40] This standard contractual clause can be found in European Commission, Model Contracts for the transfer of personal data to third countries <http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm> accessed 14th May 2017.

[41] European Commission, *Model Contracts for the transfer of personal data to third countries* <http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm> accessed 14th May 2017.

[42] Paula Barrett, Model Clauses and Data Transfers – What you need to know in summary (Eversheds 2015) <http://www.eversheds-sutherland.com/global/en/what/articles/index.page?ArticleID=en/Data-Protection/model-clauses-data-transfers-summary261015> accessed 9th May 2017.

"patchwork" of federal and state statutes due to the absence of a single regulatory rule governing transfers. For example, issues concerning how the federal government manages personal information in its possession led to the enactment of the U.S. Privacy Act of 1974, while the Electronic Communications Privacy Act of 1986, extended government restrictions on telephone wire taps to include computer transmissions of electronic data.[43] Many officials prefer this system rather than the EU's approach of one size fits it all as it helps to promote and sustain the technological innovations.[44] Furthermore many scholars and judges also prefer this system, due to the rapid change of information technologies and majority rule. However, this argument is based on the assumption that the Congress is able to establish and enforce effective oversight mechanisms or that Congress will step in with legislation, when the courts fail to act. Nevertheless, it is said that no such effective mechanisms have been brought forward in recent times.[45] The long awaited USA Freedom Act 7 was opined to have not brought meaningful reform in the sense of improving the actual level of privacy.[46]

As it can be seen, the EU and US have different ideas regarding protection of personal data. However, this difference can not disrupt the transfer of data between these two countries. Thus, this led to a negotiation in which the parties ultimately agreed on a mechanism that would allow US companies to meet the "adequate level of protection" required by the DPD. In 2000, the US Department of Commerce issued the Safe Harbor Privacy Principles, which were subsequently recognized by the European Commission.[47] The Safe Harbor scheme does not necessarily fall within the scope of an exception of the adequate protection rule. However, when you look at it as a whole, the main reason for the commission to adopt the Safe Harbor scheme is the fact that the US's privacy law did not provide a sufficient level of protection for European citizens' personal data.[48] In this scheme, although the country by itself does not meet the 'adequate protection', US companies who receive the data transferred from the EU must meet the "adequate level of protection" required by the DPD. For this purpose, this article will refer to this as an exception to the adequate protection rule which is expected from the country itself. The companies could self-certify annually to the Department of Commerce that they had complied with the seven basic principles and related requirements that have been deemed to meet the data privacy adequacy standard of the EU.

These requirements consist of seven basic principles that can deem that the US company has complied with the data privacy adequacy standard of the EU. The first basic principle is ***notice*** where an organization is required to inform data users about the purposes for which it collects and uses information, how to contact the organization with inquiries or complaints, and the types of third parties to which it discloses the information. Secondly, ***choice*** is important for an organization to be given the discretion to decide what can be done with their personal information. This is particularly important for sensitive information as such information is more private and often the data users prefer these data not to be used for any purpose other than those intended by the data users themselves. ***Onward transfers*** are also important to ensure the same level of privacy protection is accorded either by subscribing to Safe Harbor, adhering to the Directive or another adequacy finding, or entering into a contract that specifies equivalent privacy protections. Besides that, ***security*** has to be ensured by taking reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction. Moreover data ***integrity*** is important to ensure that data is reliable for its intended use, accurate, complete, and current. Additionally, access is also one of the principles which allows individuals to obtain information about themselves that an organization holds and must be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense would be disproportionate to the risks to the individual's privacy or where the rights of others would be violated. Finally, ***enforcement*** is necessary to ensure compliance, and to provide solutions to non-compliance and remedial measures of the damages suffered as a result of that.[49]

Unfortunately, despite the ambitious attempt at facilitating the transfer of the data, the Safe Harbor has received numerous criticisms. The system of self-certification in the EU-US Safe Harbour can be said to be patchy as what may be agreed in an online form can be far apart from what exists in practice. It is said that an independent body should supervise to ensure that this problem is curbed.[50] Moreover, in lieu of the notice principle, a number of privacy policies did not describe the processing operation sufficiently and clearly.[51] In addition to that the choice principle is also not upheld adequately because there are a number of companies who did not give the individuals choice to opt out or were not clear about the choice given to the individual.[52] Most importantly, problems surround the enforcement principle. This principle requires the organization to choose either the EU panel or an alternative dispute resolution to hear individual complaints. The

[43] Martin A. Weiss, Kristin Archick 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield' May 19, 2016 <https://fas.org/sgp/crs/misc/R44257.pdf> accessed 10th April 2017.

[44] Natasha Singer, "Data Protection Laws, An Ocean Apart," New York Times, February 2, 2013 <http://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html?_r=0> accessed 11th April 2017.

[45] Wischmeyer, Thomas, 'Faraway, So Close!' – A Constitutional Perspective on Transatlantic Data Flow Regulation "Obama's Court: Recent Changes in U.S. Constitutional Law in Transatlantic Perspective" 2017 <https://ssrn.com/abstract=2877548> accessed 28th September 2017.

[46] Ibid.

[47] Commission Decision 2000/520/EC, of July 26, 2000.

[48] Congressional Research Service, *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield* (R44257) 5.

[49] Martin A. Weiss, Kristin Archick 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield' (2016) <https://fas.org/sgp/crs/misc/R44257.pdf> accessed 2nd September 2017.

[50] Alexander Zinser Dr,' International data transfers between the United States and the European Union: are the procedural provisions of the Safe Harbor solution adequate?' Computer Law & Security Review Volume 20, Issue 3, May–June 2004, 182–184.

[51] James Grant, 'International data protection regulation Data transfer e safe harbor' Computer Law & Security Report (2005) 21, 257–261.

[52] Ibid 259.

organizations that selected the EU panel failed to state their commitment to comply with the advice of the EU panel as required by the FAQs, or to indicate how the EU panel could be contacted. Those selecting ADRs often failed to inform individuals of the arrangements for taking up complaints with the ADR.[53] On August 17 2015, the Federal Trade Commission (FTC) stated that it had "brought more than two dozen cases alleging false claims regarding Safe Harbor compliance."[54] The non or weak adherence to the principles could be the most common reason for such cases to be brought. The case that brought light to this issue was the case of *Schrems*.[55] In this case, Mr. Schrems, an Austrian Facebook user, filed a complaint to the Irish Data Protection Commissioner, following the revelations of former CIA agent Edward Snowden that the US National Security Agency ('NSA') had tapped into servers of several American companies, arguing that the Safe Harbor, did not provide an adequate protection from surveillance by public authorities of individuals and companies. In this case the Court of Justice of the European Union (CJEU) found that the Safe Harbor was invalidated and urging them to investigate cases which had privacy concerns. The high court confirmed that the US engaged in indiscriminate mass surveillance of European citizens.[56] The Irish High Court has also proposed two main questions for the ECJ to consider the first being whether an existing Commission finding of adequacy binds the Commissioner when investigating a complaint.[57] The second question was whether the Commissioner had the authority or was required to conduct an investigation based on factual developments that had occurred in the time since the adequacy finding was made.[58] Besides these two questions, the ECJ has also looked at broader issues of Safe Harbor and its consistency with EU law.[59] This case shows how many problems Safe Harbor has and how it failed to provide adequate data protection.

Upon a rigorous negotiation to put this issue to rest, the European Commission and the US Government have finally agreed on a new framework regarding transatlantic data transfers: The EU-US Privacy Shield was agreed upon. It provides a "mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce". On July 12 2016, the EC formally adopted the Privacy Shield Framework (Commission Implementing Decision (EU) 2016/1250), declaring it adequate to enable data transfers under EU law.[60] This Privacy Shield is meant to have more supervision thus preventing any data from being transferred before passing the adequacy test.

The Privacy Shield is meant to address the problems faced by the previous Safe Harbor. Based on *Kuner,* the Privacy Shield is much more detailed than Safe Harbor and includes stronger protection in certain areas.[61] Firstly, it enhances commitments by making sure that a US company commits to robust obligations on how personal data is processed and that the rights of European data subjects are guaranteed. These include detailed notice obligations, data retention limits, prescriptive access rights, tightened conditions for onward transfers and liability regime, more stringent data integrity and purpose limitation principles, and strengthened security requirements.[62] Besides these, there is stronger enforcement by ensuring that compliance is monitored by the Department of Commerce. Companies that fail to meet their obligations will face sanctions or they will lose their eligibility to use the Privacy Shield to legitimize their cross-border data transfers. This is a good way to keep a check that there is an adequate protection provided throughout the privileges they enjoy under the Privacy Shield. Moreover, the Privacy Shield also provides clear safeguards and transparency as the personal data will be subject to clear limitations, safeguards and oversight mechanisms. US authorities have also, reportedly, ruled out indiscriminate mass surveillance of the personal data transferred to the United States under the new arrangement.[63] On the other hand, there is also effective protection accorded to EU citizens' rights with several redress possibilities. Citizens can take action if they consider that their data has been compromised. Under the Privacy Shield there are multiple redress possibilities, beginning with deadlines for companies to respond to individual complaints. Individuals will be able to complain: (i) directly to companies, which will have 45 days to resolve the complaint; or (ii) directly to EU DPAs, which will be able to refer unresolved complaints to the Federal Trade Commission (FTC).[64]

Nevertheless, despite the advantages stated, WP29 has listed some of the areas that were omitted or failed to be addressed. These concern the commercial aspects, the WP29 regrets, for instance, the lack of specific rules on automated decisions and of a general right to object. It also remains unclear how the Privacy Shield Principles shall apply to processors.[65]

---

[53] Ibid 259.

[54] Federal Trade Commission, "U.S.-EU Safe Harbor compliance: Don't run aground", Lesley Fair, [2015] <https://www.ftc.gov/news-events/blogs/business-blog/2015/08/us-eu-safe-harbor-compliance-dont-run-aground> 12th April 2017.

[55] Maximillian Schrems v. Data Protection Commissioner [2015] Case C-362/14.

[56] Kevin Cahill, Max Schrems: The man who broke Safe Harbour, <http://www.computerweekly.com/feature/Max-Schrems-The-man-who-broke-Safe-Harbour>28th September 2017.

[57] C-362/14, Schrems v. Irish Data Prot. Comm'r, 2015 E.C.R. I-650, ¶ 36, Christina Lam, Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in Schrems v. Irish Data Protection Commissioner, 40 B.C. Int'l & Comp. L. Rev. E. Supp. 1 (), http://lawdigitalcommons.bc.edu/iclr/vol40/iss3/1 accessed 27th September 2017.

[58] Ibid 5.

[59] Ibid 5.

[60] Ultimco White paper, '*Demystifying the EU-U.S. Privacy Shield – Safe Harbor, Privacy Shield & Beyond*'<https://hsm.utimaco.com/wp-content/uploads/2017/03/Utimaco-White-paper-Privacy-Shield-Demystified.pdf> accessed 9th April 2017.

[61] Christopher Kuner 'Reality and illusion in EU data transfer regulation post Schrems' (2016); Maximilian Schrems 'EU-US Privacy Shield: Towards a new Schrems 2.0 Case?' (2016) <https://free-group.eu/2016/04/06/eu-us-privacy-shield-towards-a-newschrems-2-0-case/> accessed 26th September 2017.

[62] Martin A. Weiss, Kristin Archick 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield' [2016] <https://fas.org/sgp/crs/misc/R44257.pdf> accessed 10th April 2017.

[63] Ibid.

[64] Ibid.

[65] Article 29 Working Party Statement on the 'Decision of the European Commission on the EU-U.S. Privacy Shield, Brussels' (13 April 2016) <http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/press_release_shield_en.pdf> accessed 10th April 2017.

There is also concern about the access by public authorities to data transferred to the US under the Privacy Shield, as the WP29 expected stricter and more rigorous guarantees concerning the independence and the powers of the Ombudsperson mechanism. The WP29 regrets the lack of concrete assurances that such practices do not take place.[66] The privacy shield has failed again to provide an overall assessment of the US legal order and to find that the US as "a third country ensures an adequate level of protection" within the meaning of Article 25(2) of the directive "by reason of its domestic law or of the international commitments it has entered into [. . .] for the protection of the private lives and basic freedoms and rights of individuals[67]", pursuant to Article 25(6) of the directive.

In spite of this, it appears that the Privacy Shield has indeed solved the majority of the issues that have emerged from the Safe Harbor. The Privacy Shield is expected to ensure that data protection is continuously maintained in an adequate manner. However, a way forward will indeed be the change in the US legislation that ensures the transferred data are adequately protected.[68] Upon learning of the transfer of EU and US, it seems the law is evolving and attempting to make changes to its previous position that caused encumbrances. However, this exception is very limited and it only covers transfers from the EEA to the US recipient(s) concerned. This is insufficient to prevail as a primary exception due to its limited applicability. Another new aspect of the cross border data transfer is the development of a BCR which is a code of conduct for the parties involved in the transfer. It is moreover said that despite the US's attempt to maintain a high data protection standard, it is easily possible for them to dishonour their promise in the United States.[69] Such a circumstance can cause the suspension of data transfers until a proper mechanism is brought forward.[70] As mentioned above the BCR does not apply widely as the model clause, however the BCR is praised as a good solution to the many problems faced in cross border data transfers. In the upcoming section, this article discusses BCRs and their advantages and disadvantages in a detailed manner to see what solutions this corporate rule is able to provide to the cross border issue.

3.3. *Binding corporate rule*

In the previous sections, the article has discussed the position of the EU in regards to cross border transfers and the European Commission's standard contractual clause as an exception to the adequate protection rule in the cross border data transfer. The article has also explained how the Safe Harbor Principle has operated and the reasons behind transitioning to US-EU Privacy Shield. In this section, we will discuss the BCR and how this attempts to make a change in the problem that is usually faced in cross border data transfers in a particular cloud.

BCR should not be mistaken as a new concept as it was first introduced by the European Union Article 29 Working Party more than a decade ago. A small explanation is needed to understand the intention of the Working Party when it introduced the concept of BCR as a possible solution for the complications involved in data transfers. First of all, Article 29 has provided a disclaimer that the fact that this working document focused on BCRs (or codes of conduct in more traditional terminology) should not be assumed as indicating that contractual solutions have been superseded.[71] On the contrary, this allows companies to use this instrument in a positive and encouraging way.[72] Thus it is not meant to show which method prevails, but merely to provide a better pathway for issues regarding cloud computing. This working document has explained the reasons why they have adopted the terminology. Below is the explanation:

a) binding or legally enforceable because only with such a character may any clauses be regarded as "sufficient safeguards" within the meaning of Article 26 (2).
b) corporate in the sense that they consist of the rules in place in multinational companies, usually set up under the responsibility of the headquarters.
c) for international data transfers as the main reason for their existence.[73]

This BCR requires both legal enforcement and compliance because having one in the absence of the other will not be worth implementing. The internal rule will only be worthwhile if both co-exist and are not mutually exclusive. The binding nature of the rules in practice will imply that a member of the corporate group, as well as each employee within it, will feel compelled to comply with the internal rules.[74] Furthermore, Article 29 of the Working Party attaches great importance to the concept of legal enforceability by allowing non-compliance to be subject to a complaint to be lodged to the DPA. Article 29 has explained why the right to seek judicial remedy is necessary by mentioning that it is important to realize that the duty of co-operation could never guarantee 100% compliance and how the competence of data protection authorities in the community can slightly vary from one country to the other and none of them can award compensation for damages since only

[66] Ibid.
[67] Xavier Tracol, "Invalidator' strikes back: The harbour has never been safe", Computer Law & Security Review, volume 32, issue 2, April 2016.
[68] Xavier Tracol, "EU–U.S. Privacy Shield: The saga continues", Computer Law & Security Review 32 (2016) 775–777.
[69] Christopher Kuner 'Reality and illusion in EU data transfer regulation post Schrems' (2016); Maximilian Schrems 'EU-US Privacy Shield: Towards a new Schrems 2.0 Case?' (2016) <https://free-group.eu/2016/04/06/eu-us-privacy-shield-towards-a-newschrems-2-0-case/> accessed 26th September 2017.
[70] Christina Lam, Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in Schrems v. Irish Data Protection Commissioner, 40 B.C. Int'l & Comp. L. Rev. E. Supp. 1 (2017), <http://lawdigitalcommons.bc.edu/iclr/vol40/iss3/1> accessed 27th September 2017.
[71] Article 29 – Data Protection Working Party, '*Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*'(11639/02/ENWP74) <https://www.privacycommission.be/sites/privacycommission/files/documents/01.01.01.23-wp74.pdf> accessed 13th April 2017.
[72] Ibid 7.
[73] Ibid 8.
[74] Ibid 9.

the court will be able to do that.[75] On the whole, the Working Party, in their opinion paper, believes that the guidance provided by the BCR will assist in facilitating the application of Article 26(2) of the Directive which relates to cross border data transfers. It allows the simplification of the process of exchanging personal data on a worldwide basis.[76] Based on this, the Article 29 Working Party had high hopes during their proposal of the BCR. We shall now look at the BCR in the directive and the new regulation's perspective and approach to the BCR.

3.3.1. *Data protection directive 95/46/EC*

In the previous model, the Directive allowed cross border transfers only if the adequacy of safeguards was proven. Without the establishment of an adequate level of protection, the personal data cannot be transferred to the specific country. There are a few ways to ensure that adequate protection is provided and one is the BCR. To apply the BCR, the corporate entity should seek the approval of each of the EEA data protection authorities from whose country the data are to be transferred. The EU has shown their acceptance of the concept of BCR in recent years. This can be seen in the release of the opinion paper WP 107 and WP 108 which aim to significantly clarify much of what was set out in WP 74.[77]

WP107 brings forward a general procedure where a corporate enterprise keen on using the BCRs for data export from more than one EU Member State may seek to do so.[78] WP107 proposed that there should be a DPA as a lead authority for co-operation procedures.[79] There are certain criteria set out to justify the selection of the lead authority. The relevant criteria that are required are;

- *the location of the group's European headquarters;*
- *the location of the company within the group with delegated data protection responsibilities*
- *the location of the company which is best placed (in terms of management function, administrative burden etc.) to deal with the application and to enforce the BCRs in the group;*
- *the place where most decisions in terms of the purposes and the means of the processing are taken; and*
- *the member states within the EU from which most transfers outside the EEA will take place.*[80]

The corporate entity which applied to the DPA, should also provide the proposed lead authority with all appropriate information, which justifies its proposal, including the nature and general structure of the processing activities in the EU/EEA with particular attention to the place/s where decisions are made, the location and nature of affiliates in the EU, the number of employees or persons concerned, the means and purposes of the processing, the places from where the transfers to third countries take place and the third countries to which those data are transferred.[81] The proposed lead authority then considers all the information provided and decides whether to agree as a lead authority. If the lead authority (entry point) agrees to be the DPA, the other interested DPAs have two weeks to raise any objection.[82] If, however the entry point rejects the offer, they would have to provide the reason for the rejection as well as proposing the appropriate party who may be suitable to be the DPA in the situation.[83] Once the decision on the lead authority is reached, a consolidated draft will be sent to all other DPAs to allow feedback and comment to be passed.[84] Upon receiving the comments, the lead authority will discuss them with the applicant, and if the applicant is satisfied with the rectification based on the addressed comments, a final draft will be made. The lead authority will invite other DPAs to confirm that they are satisfied as to the adequacy of the safeguards proposed.[85] The Chairman of the Article 29 Working Party will be informed of this decision and will share this information with other EU/EAA DPAs.[86] This is a more rigorous approach in comparison to the model clause and it alleviates the fear of a limited right to block that existed in the standard contractual clause which affects the data protection.

In contrast to WP107, WP108 is largely a checklist for seeking approval of the BCRs. This checklist is meant to help the corporate group of companies in circumstances where it applies

[75] Article 29 – Data Protection Working Party, '*Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*'(11639/02/ENWP74) <https://www.privacycommission.be/sites/privacycommission/files/documents/01.01.01.23-wp74.pdf> accessed 13th April 2017.

[76] Ibid.

[77] Article 29 – Data Protection Working Party, '*Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*'(11639/02/ENWP74) <https://www.privacycommission.be/sites/privacycommission/files/documents/01.01.01.23-wp74.pdf> accessed 13th April 2017.

[78] David Bender & Larry Ponemon, 'Binding corporate rules for cross border data transfer' Rutgers Journal of Law&UrbanPolicyVol.3:22006 <http://www.rutgerspolicyjournal.org/sites/rutgerspolicyjournal.org/files/issues/3_2/Bender_Ponemon_Cross_Border_Data.pdf> accessed 15th April 2017.

[79] ARTICLE 29 Data Protection Working Party, '*Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules*' (05/EN WP107) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp107_en.pdf> accessed 14th April 2017.

[80] ARTICLE 29 Data Protection Working Party, '*Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules*' (05/EN WP107) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp107_en.pdf> accessed 14th April 2017.

[81] Ibid 3.

[82] Ibid 3.

[83] Ibid 4.

[84] ARTICLE 29 Data Protection Working Party, '*Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules*' (05/EN WP107) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp107_en.pdf> accessed 14th April 2017.

[85] ARTICLE 29 Data Protection Working Party, '*Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules*' (05/EN WP107) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp107_en.pdf> accessed 14th April 2017.

[86] Ibid.

for approval of its BCRs and to help in complying with WP74.[87] The WP108 also explains how to apply for the appropriate DPA and mainly focuses on geographic considerations. There is also clarification on what information is required in the application. Most importantly, WP108 explains how the data subject can seek remedy if there is any non-compliance. A data subject must be able to commence a claim, at his or her option, in the nation from which the export took place, or in the nation of the enterprise's EU headquarters.[88] The application should delineate the actual steps a data subject should take to obtain a remedy, and should confirm that the EU headquarters has assets sufficient to satisfy a claim for damages caused by any part of the enterprise.[89]

All these three opinions by Article 29 Working Party show how enthusiastic the working party is in introducing and providing a framework for the directive to be more open to the concept of BCR that eases cross-border data transfers. The following discussion will be on the Regulation and their opinion of the BCR.

3.3.2. *General Data Protection Regulation*

The General Data Protection Regulation, unlike the old directive, clearly lists BCRs as an appropriate safeguard in Article 46 and provides detailed conditions for transfers by way of BCRs in Article 47 (mentioned above). In Article 26, the regulation states competent supervisory authority shall approve BCRs in accordance with the consistency mechanism set out in Article 63:

(a) *are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;*
(b) *expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and*
(c) *fulfil the requirements laid down in paragraph 2.*[90]

The regulation has also specified the criteria needed in the BCRs. If the BCRs meet the requirements set out in the GDPR, they will be approved, and no further DPA approval will be required for transfers of personal data made under the BCRs.[91] However, the most significant change that the GDPR has brought is having a consistency mechanism in BCR. Today, the European DPAs have developed specific mechanisms to cooperate in the context of approving BCRs.[92] The consistency mechanism is intended to cover a variety of multijurisdictional issues under the GDPR.[93] However, this mechanism is criticized because of the numerous procedures involved and the short timeframes.[94] It is said that the BCR is better off promoting the idea of consistency rather than making it a mechanism that needs to be followed. Based on this discussion above, it is apparent that the new regulation has decided to implement the BCR, thus indirectly condoning the concept of internal rule. The BCR has a few advantages and the GDPR has amplified the advantages by emphasizing the application of the BCR as an appropriate safeguard.

3.3.3. *Advantages and disadvantages of BCR*

One of the main advantages of having a BCR is that upon the implementation of the BCR and its approval, the companies are free to transfer the personal data across borders.[95] This is important in a cloud environment which requires flexibility and cannot be constrained in a rigid environment. Moreover, the BCR harmonizes the practices relating to the protection of personal data within a group and it prevents the risks resulting from data transfers to third countries.[96] Besides that, BCR helps to address privacy concerns and raise awareness of data protection. This is due to the fact that there is a need to consider the type of personal data that is being transferred and how one can make the staff aware and respect the rules when applying the application.[97] Through BCR, one can make certain that the staff is well educated with the type of personal data that is being dealt with which is an essential component of authorization.[98]

Furthermore, the BCR under GDPR has a number of other benefits to offer. Firstly, the process was simplified by engaging only one DPA to coordinate the BCR in contrast to the old position which required one lead DPA and two co-reviewer DPAs. Also, the current regime has removed the process of reaching out to various DPAs since the consistency mechanism ensures the opinion of all DPAs is considered. In addition, the new regulation has removed the national DPA authorization from some countries. This provides a more flexible mechanism in which approval of BCRs and commencement of transfers under the approved BCRs can be merged to occur

[87] ARTICLE 29 Data Protection Working Party, '*Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules*' (05/EN WP108) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp108_en.pdf> accessed 15th April 2017.

[88] David Bender & Larry Ponemon, 'Binding corporate rules for cross border data transfer' Rutgers Journal of Law&UrbanPolicyVol.3:2[2006] <http://www.rutgerspolicyjournal.org/sites/rutgerspolicyjournal.org/files/issues/3_2/Bender_Ponemon_Cross_Border_Data.pdf> accessed 15th April 2017.

[89] Ibid.

[90] General Data Protection Regulation [2016] 2016/679, Article 47.

[91] White & Case, 'Chapter 13: Cross-Border Data Transfers – Unlocking the EU General Data Protection Regulation (22ndJuly2016) <https://www.whitecase.com/publications/article/chapter-13-cross-border-data-transfers-unlocking-eu-general-data-protection> accessed 10th April 2017.

[92] Ibid.

[93] Bloomberg DNA,' EU Regulation Binding Corporate Rules Under the GDPR – What Will Change? <https://www.hunton.com/files/Publication/d50d633d-04b0-4df1-9c6d-94b53b7ff820/Presentation/PublicationAttachment/b8e227a7-7224-44d1-9ea3-9a8c7741622f/EU_Regulation_Binding_Corporate_Rules_Under_the_GDPR.pdf> accessed 15th April 2017.

[94] Ibid.

[95] Philip Rees, Dominic Hodgkinson, 'Binding Corporate Rules: A simpler clearer vision?' Volume 23, Issue 4, 2007, Pages 352–356 <http://www.sciencedirect.com/science/article/pii/S0267364907000301> 16th April 2017.

[96] European Commission, '*Overview on Binding Corporate rules*' <http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm> 16th April 2017.

[97] Information Commissioner's Office, 'Binding corporate rules' <https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/> accessed 2nd September 2017.

[98] Ibid.

at the same time.[99] On the other hand, the GDPR provides flexibility by allowing the commission to create procedural rule if needed. Harmonization is also reached in the BCR because the new regulation is applicable to all EU members.

There are several aspects that need to be assured to practice this BCR. Most importantly, it is vital for BCR to be binding both in practice as well as legally. It is necessary to guarantee that sufficient legal effect applies in BCR to avoid any unduly application of law during the enforcement. This could happen if the enforcement is weak in the BCR Despite the fact that the BCR carries many advantages such as flexibility and the ability to be tailor made for particular transactions, there are a few impediments that prevent entities from considering this option of transfer. One such drawback is that the BCR is said to be disproportionately costly which may deter individuals from taking this option. This is due to the fact that there is a requirement that they are underpinned by a detailed compliance and audit programme. This could place additional demands on internal resources in respect of both costs and time.[100] Moreover, there is also a great obstacle concerning the finding of a sufficiently good means of "legally-bindingness" *unilaterally* in all EEA countries. This is due to the fact that the laws of some EEA countries do not enable third party beneficiary rights or binding obligations to be created by unilateral undertakings alone. In other words, the legal theories required for BCRs acceptable to the Working Party may not apply or even exist in some EEA countries.[101] It is said with the change of structure of the group, that the effectiveness of using BCRs may diminish,[102] however this can be curbed by drafting the BCRs wide enough that it is able to accommodate changes in the company structure and any variation to the types of data flow. Moreover, it is indeed difficult to use this transfer to the US because BCRs are only intra-group agreements hence lacking an appropriate solution for such transfers.[103]

Hence, upon the analysis of the BCR, the new General Data Protection Regulation has put high hopes in this corporate rule to function in cases of cross border data transfer by reducing the risk that was involved. The old directive did state explicitly about BCR, and BCR was implemented merely by following the guideline that was provided by Article 29 Working Party. The new regulation however has specified the rules and criteria of the BCR which will rectify the previous problems faced in the BCR during the governance of the directive. However, like any rule, there are certain setbacks that exist in this option. Thus, to understand the appropriate method, one should weigh both the pros and cons of all the exceptions. In the next section, this article will discuss the exception in general and provide an opinion for the exception to be followed.

4. Concluding remarks

Without a doubt it can be seen that cross border data transfers are a common phenomenon in a cloud environment. This article has shown the changes that have been made from previous years until now. Firstly, it can be seen that the new regulation has maintained the appropriate safeguard rule which was the previous situation in the directive. It is surprising how the regulation has chosen to maintain a rule which was introduced years before and how the development of new technology did not give rise to a change of rule. The new regulation did include a new derogation for transferring data when there is compelling legitimate interest to do so. This has promoted flexibility in the transfer of data across borders. It is fair to say that there are only cosmetic changes to the new regulation. This can be seen in the retention of the adequacy rule and the subtle difference made in terms of the consent. The amendment made is minimal compared to the privacy factor which has undergone major changes i.e., holding the processor accountable for any misconduct and the need for a proper consent in the new regulation. However, this may not be the appropriate step since the protection accorded in the transfer of data should be more rigorous due to the consequences that would result if there was any mishap during the transfer of personal data. Thus, it can be seen that the cross border data transfer lacks in improvement made by the General Data Protection Regulation and there may be discrepancies.

Based on the later discussion of this article about the exceptions available for the adequate protection principle, the pros and cons of each of the exceptions can be seen and allow an organization to conclude which option is more preferable to adopt. This article discusses the Safe Harbor, which leads to an argument that it is also an exception to the principle of adequate protection, and how it has transitioned to the new Privacy Shield. This Privacy Shield is meant to solve the discrepancy that was present in the Safe Harbor and also provide a robust inspection on the obligation in protecting the data that was transferred especially in the EU. This shows that the exception should not be taken lightly and any action that connotes to lesser protection will not be tolerated in cross border data transfers. Nevertheless, the Privacy Shield, although an improvement from the previous Safe Harbor, still lacks in providing specific rules on automated decisions and of a general right to object. They have also failed to provide an overall assurance on whether the US has provided an adequate level of protection. This method of exception cannot be deemed preferable because in addition to its disadvantages, it is a limited exception that only applies to transfers from EEA to the US.

[99] Bloomberg DNA,' EU Regulation Binding Corporate Rules Under the GDPR – What Will Change? <https://www.hunton.com/files/Publication/d50d633d04b04df19c6d94b53b7ff820/Presentation/PublicationAttachment/b8e227a7722444d19ea39a8c7741622f/EU_Regulation_Binding_Corporate_Rules_Under_the_GDPR.pdf> accessed 15th April 2017.

[100] Taylor Wessing, 'Understanding Binding Corporate Rules' <https://united-kingdom.taylorwessing.com/globaldatahub/article_binding_corporate_rules.html> accessed 6th September 2017.

[101] Bristows, 'Transferring Personal Data from the E.U.: Are Binding Corporate Rules the Answer?' <https://www.bristows.com/news-and-publications/articles/transferring-personal-data-from-the-eu-are-binding-corporate-rules-the-answer/#nogo> accessed 8th September 2017.

[102] Taylor Wessing, 'Understanding Binding Corporate Rules' <https://united-kingdom.taylorwessing.com/globaldatahub/article_binding_corporate_rules.html> accessed 6th September 2017.

[103] Geppert, Nadine, Could the 'EU-US Privacy Shield' Despite the Serious Concerns Raised by European Institutions Act as a Role Model for Transborder Data Transfers to Third Countries? (August 31, 2016). <https://ssrn.com/abstract=2928064> accessed 1st October 2016.

Moreover, it is said that privacy shield's adequacy is likely to be challenged in Court of Justice of the European Union, so its legal uncertainty will continue.[104] Skepticism continues to surround the new Privacy Shield despite the formal approval of the European Commission.[105] Based on this, it can be seen that it is highly unlikely this exception would be considered the preferable method. The real competition for an ideal method of exception is between the standard contractual clause and BCR.

As stated before, the GDPR has facilitated the process of model clause by removing further authorization from the DPA. However, the limitation on the authorities blocking transfers can serve as a major drawback. BCR and the Model Clause both share the similar objectives of promoting flexibility whilst maintaining an adequate level of protection. The major change thus far, in respect to cross border data transfer, is the inclusion of BCR in the regulation itself. This differs from the previous position as mentioned above. BCRs provide for a pragmatic method of integrating data protection into the DNA of a company and demonstrating accountability. In this article, it is suggested that BCR is the future of data transfer. This article opines that in terms of the exception to the adequate protection rule, the BCR is regarded to be the better option in comparison to the other derogations available which includes the model clause. One of the main pluses of the model clause is that it incurs a lesser cost in comparison to BCR which involves costly auditing. However, although the model clause can be an easy and a cheaper option in a smaller company, it can be costly and cumbersome in a large multinational company. A multinational company is composed of many companies and affiliates which require a number of model clauses.[106] Many have also opined that there is better compliance in BCR in comparison to the model clause which involves difficulty in achieving genuine compliance. Thus, weighing this argument, it can be seen that BCR is 'the way to go' because it carries many benefits, it also ensures effective compliance which is necessary in the adoption of any rule. A method that fails to enforce and ensure that compliance is effective will fail to meet its objective eventually. Hence, based on all the latest amendments and development, it can be seen that the law makers are making an attempt to cope with the fast-growing area of technological development and the issue of protection of data, particularly transfer of data across jurisdictions, is being addressed by creating rules which are strict but also allow flexibility. Hence, it can be seen in this article that the law makers are making an attempt to deal with the fast-growing area of technological development and the issue of protection of data. The ideal concept of transfer of data across jurisdictions should involve strict rules in maintaining the data protection standards as well as a flexible approach to prevent obstacles in allowing legitimate transfers.

Acknowledgement

The University of Malaya, Grant Number BK034-2016, has supported this work.

[104] Hogan Lovells, 'EU Data Transfers to the U.S.: Considering Your Options after Privacy Shield' (22nd July2016) <http://www.hldataprotection.com/2016/07/articles/international-eu-privacy/eu-data-transfers-to-the-u-s-considering-your-options-after-privacy-shield/> accessed 10th September 2017.

[105] Ibid.

[106] Allen & Overy, 'Binding Corporate Rule' (2016) <http://www.allenovery.com/SiteCollectionDocuments/BCRs.pdf> accessed 18th September 2017.