Master Thesis

Law and Technology LLM

TRANSBORDER DATA FLOWS: BINDING CORPORATE RULES AS A GLOBAL TRANSFER MECHANISM AND TRUSTED DATA PROCESSING AREA

Supervising Professors:

Dr. I.E. Bayamlioglu (1st)

Mr.dr. C.M.K.C. Cuijpers (2nd)

Student: Sylwia Pietrzak

ANR: 741472

January 2017
Tilburg

Table of content

Abbreviations

APEC Asia-Pacific Economic Cooperation
BCRs Binding Corporate Rules
CBPRs Cross Border Privacy Rules
CJEU Court of Justice of the European Union
CNIL Commission nationale de l'informatique et des libertés
DPA Data Protection Authority
DPD Data Protection Directive
ECHR European Convention on Human Rights
EEA European Economic Area
EU European Union
GDPR General Data Protection Regulation
ICC International Chamber of Commerce
IDC International Data Corporation
MRP Mutual Recognition Procedure
OECD Organisation for Economic Co-operation and Development
SCCs Standard Contractual Clauses
US United States

1. Introduction

The regulation of transborder data flows has gradually evolved over the last several decades. The first such laws adopted in various European countries in the 1970s[1] tended to make transborder data flows contingent on strict conditions being fulfilled, such as that the transfer being approved by the local data protection authority. Recently more sophisticated instruments have been developed to provide protection for transborder data flows across organisations, such as Standard Contractual Clauses and Binding Corporate Rules (BCRs) – in the European Union, and the APEC Cross Border Privacy Rules (CBPRs) system,[2] endorsed by APEC[3] Leaders in 2011, currently with four participating APEC CBPR system economies: USA, Mexico, Japan and Canada.

1.1. Background

In the early 1980's Europe had two international legal instruments on Data Protection: the OECD Guidelines[4] and the Council of Europe Convention.[5] The Council of Europe Convention was particularly influential. It provided for the free movement of personal data between countries that had ratified the Convention with restrictions potentially being placed on the movement of data outside that group. Only countries whose domestic law provided equivalent safeguards to those defined in the Convention could ratify it. The Council of Europe Convention makes clear that its objective is to balance the need to provide for the movement of personal data with the need to protect personal privacy. The starting point in drafting the Convention was the European Convention on Human Rights (ECHR), particularly Articles 8 and 10, but the Council of Europe identified the need for a specific convention to deal with

[1] Christopher Kuner, "Regulation of transborder data flows under data protection and privacy law: past, present, and future", TILT, October 2010.
[2] Accessed 27 July 2016, http://www.cbprs.org/
[3] The Asia-Pacific Economic Cooperation (APEC) is a regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific, accessed 27 July 2016, http://www.apec.org/about-us/about-apec.aspx
[4] Accessed 27 July 2016, https://www.oecd.org/about/
[5] Accessed 27 July 2016 https://www.coe.int/en/web/conventions/about-treaties

the risks posed by computer processing rather than rely solely on those general principles.

In the 1990s, technological innovations completely transformed sporadic cross-border data transfer, carried out through heavy data storage medias.[6] Data transfer becomes essential for multinational corporations. Meanwhile, data protection is an important part of the rule of law in the information society.[7]

The European Data Protection Directive[8] was adopted in 1995 as a result of The European Commission realizing the goals of the single market. The EC was concerned that the free flow of data within the EU may be inhibited because the data protection standards were very different among the Member States. The Directive regulates that if any of that data is personal in nature, then its transfer outside of Europe is forbidden. Forbidden, that is, unless you have an "adequate" data export solution in place.[9]

Now after more than four years of intensive work, the European Parliament adopted the Regulation on the protection of personal data (GDPR), that will be used directly without the need for implementation into national law. On 4 May 2016, the official text of the Regulation has been published in the EU Official Journal in all the official languages. The Regulation entered into force on 24 May 2016.[10] After the entry into force of the EU Regulation on the protection of personal data the EU will reach full harmonization of laws in this area. It is also the very first time that the BCRs are regulated in an official legal act of the European Union.

1.2. Problem of global standard

Other parts of the world created their own solutions to transfer personal data abroad. Such regionally oriented system is heavily dependent on effective monitoring

[6] OECD, Report on the cross-border enforcement of Privacy Laws, 2006, accessed 12 July 2016, www.oecd.org/dataoecd/17/43/37558845.pdf.
[7] Peter Blume, "Transborder data flow: is there a solution in sight?', 8 *Int'l J L and Info Technology*, 2000.
[8] Directive 95/46/EC 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, Data Protection Directive, Official Journal L 281 , 23/11/1995 P. 0031 – 0050, 24 October 1995, art. 25(1), http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[9] Article 25, Ibidem.
[10] "Reform of EU data protection rules, European Commission, accessed 11 July 2016, http://ec.europa.eu/justice/data-protection/reform/index_en.htm

of cross-border data transfer. However, If a problem arises, such as, for example, a consumer is a victim of identity theft or her personal information is shared with third parties against her wishes, she must determine who is at fault, what laws apply, what her rights are with respect to the standard of protection in that jurisdiction, and who needs to be contacted to have the problem resolved.[11] Because of this diversity of national data protection and privacy legislation, there have been growing calls for a global legal instrument on data protection.

On the one hand, there still is no global standard concerning international data transfers, creating one could be essential to the improvement of global trade and data protection. On the other hand basing a global framework for data protection on a binding multilateral convention might be quite disadvantageous. One issue is that the drafting of any such convention would likely take many years, for example, it has been stated that the conclusion of a multilateral convention for legal harmonization seems to take a minimum of ten years,[12] and in extreme cases may take much longer.[13] Negotiation of a global multilateral convention might also lead to a lowest common denominator set of data protection standards, given the difficulties of obtaining the agreement of many states.[14] So why not use a tool that already exists and has evolved? Could BCRs be this tool?

Since the Article 29 Working Party created the Binding Corporate Rules instrument, a decent collection of publications concerning BCRs has been issued. First of all, the opinions prepared by this advisory body itself are the best source of information on BCRs. Furthermore, articles and books of influential professors and lawyers with vast academic achievements in this field, among others, Lokke Moerel and Christopher Kuner. Dozens of blogs and magazines are publishing their analysis on the matter of protecting data in times of expansion of new technologies. Many practitioners express their opinion on the best solution for global data transfer based upon their experience.

Even though this great collection explains a lot when it comes to the legal nature of BCRs, not many focus on BCRs as a global transfer solution going beyond a

[11] Miriam Wugmeister, Karin Retzer, Cynthia Rich, “Global solution for cross-border data transfers: making the case for Corporate Privacy Rules”, Morrison & Foerster LLP, 2007.
[12] Roy Goode, “Reflections on the harmonisation of Commercial Law”, Uniform Law Review, 1991.
[13] For example, the Vienna Convention on the Law of Sales of 1980 was the result of over 50 years’ work. John Goldring, “Globalisation, national sovereignty and the harmonisation of laws” Uniform Law Review 435, 437, 1998.
[14] Christopher Kuner, “An international legal framework for data protection: Issues and prospects”, Computer Law & Security Review 25, 24 January 2009.

national, territorial and regional approach. Much personal data routinely flows across national borders, and the same data processing may result in the application of multiple laws. The growing importance of data processing is reflected in the large number of countries around the world that have enacted data protection laws, and the countries and international organisations that are currently in the process of revising them to meet the challenges posed by globalisation and the rapid growth of the Internet. There are a lot of descriptions of regional solutions but not many debate which solution might become the global one.

Hardly any data protection issues cause as much uncertainty as do those of jurisdiction and applicable law. Companies are unsure of which law applies to their processing of personal data, individuals are confused about the legal standards under which their data are to be protected, and regulators have to grapple with complex jurisdictional issues to which there are often no clear answers. The global reach of the Internet greatly complicates the task of determining which courts and regulators should have jurisdiction over acts of data processing, and under which legal standards such processing should be judged.[15]

1.3. Research question

Sending myriad data was never easier. The latest news about international data flows problems indentified in the Schrems Case, invalidation of Safe Harbour Framework and upcoming changes of the data protection regulation in European Union, all together, show how rigid, outdated and territorial the binding regulations are. The question is if there is a solution, that might be an answer for global data transfer beyond borders, and that can keep up with the fast Internet growth.

Based on abovementioned issues that multinational companies are facing, the following problem statement is formulated to address the problem in this research:

Given the rapid growth of technology and data flow along with the lack of a global instrument regulating international data transfers, the question arises if BCRs could become such an instrument?

[15] Christopher Kuner „Global data transfer on the Internet: Lessons from the Ancient World", SSM, 2009

In order to completely and accurately answer the problem statement the following research questions have to be answered:

What are the strengths of BCRs and weaknesses when it comes to using it as a global transfer tool? Data will move beyond borders, leading to the question: if data transfer rules are conflicting with increasingly globalised use of data, what can businesses do to comply?

The concept of BCRs can be defined as: "a code of conduct setting forth the private policy of the entire enterprise, to which each entity included in the enterprise subscribes, enabling data subjects and other entities to enforce that code against the enterprise."[16] Many global corporations believe that codes of conduct should be sufficient for the cross-border transfer of personal data.[17]

1.4. Structure

The thesis is divided into six chapters. It starts with a description of the main features of BCRs, and how they are regulated and how they have developed. The chapter will present the trigger that caused changing the currently valid Directive to a new Regulation, hence the official recognition of BCRs. Subsequently advantages as well as disadvantages of BCRs will be addressed. First the improvements brought by the GDPR are specified, after which it is analysed if the GDPR still leaves room for improvement. Next the alternatives for BCRs are specified. To conclude, BCRs are considered as a global solution to international data transfers outside the EU. Firstly by characterizing their possibilities to follow technical developments of the market, then by demonstrating the influence of European data protection solutions on countries all over the world. Its impact is already so vast that it opens the door for the BCRs to be accepted as a data transfer global solution. Lastly, indicating possible cooperation of BCRs and other instrument that share similarities with BCRs will show BCRs as a global solution.

---

[16] Article 29 – Data Protection Working Party, "Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfer", WP 74, 3 June 2003, accessed 15 March 2016, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf

[17] David Bender, Larry Ponemon, "Binding corporate rules for cross-border data transfer", Rutgers Journal of Law and Urban Policy, 2006.

2. Worldwide data flow

Much personal data routinely flows across national borders and the same data processing may result in the application of multiple laws. The ease with which data flows internationally also means that data protection and privacy law has become a point of competition between different legal regimes, ”with each one striving to achieve the seemingly impossible goal of simultaneously protecting the privacy of individuals, striking a balance between privacy and other important values (e.g., public security), and furthering economic growth.”.[18] Due to uneven data protection levels in national sovereignties, data protection has become a major obstacle to free global data flow.

This chapter will present the beginning of BCRs, introduce their legal nature, procedure of establishing BCRs and the changes the GDPR will bring compared to the existing DPD. To answer the question if BCRs might help the problem described above and become a global solution to free global data flows it is necessary to analyse the legal basis and legislation regulating BCRs.

2.1. Legal nature of BCRs

BCRs take the form of a set of internal documents, that contain unilateral obligation, allowing multinational corporations, international organizations and groups of companies to make transfers of personal data across borders in compliance with EU Data Protection Law. Their aim is to introduce uniform rules for the processing of personal data within the corporate group and to ensure an adequate level of protection in countries that do not guarantee it under national law. BCRs are an instrument, created under Article 26(2) of Directive 95/46/EC,[19] developed by the independent, advisory committee to the European Commission on data protection, The Article 29 Working Party.

[18] Christopher Kuner, “The global data privacy power struggle”, OUPblog, 28 January 2013, accessed 19 June 2016, http://blog.oup.com/2013/01/global-data-privacy-power-struggle/ .
[19] Data Protection Directive, op.cit. p. 2.

The Article 29 Working Party while performing the analysis of the concept of corporate rules pointed out that these rules are:[20]

- "binding" or "possible to execute in the legal way" because only the clauses of such character can be recognized as the "adequate level" of guarantees as defined in Article 26 paragraph 2 of the Directive 95/46/EC;
- corporate, because those rules are used within the framework of the international corporation, in most cases devised by the corporation headquarters;
- used for the international transfer of personal data.

The notion of "corporate group" may vary from one country to another and may correspond to very different business realities and form: from closely-knit, highly hierarchically structured multinational companies to groups of loose conglomerates; from groups of companies sharing very similar economical activities and therefore processing operations to broad partnerships of companies with very different economical activities and different processing operations.

The BCR regime as developed by the Article 29 Working Party addresses the data processing obligations of data controllers. In 2010, the European Commission adopted a new set of contractual clauses for transfers between Controllers and Processors in order to answer to the expansion of processing activities and in particular the emergence of new business models for international processing of personal data,[21] so called BCRs for Processors. Given the growing interest of industry for such a tool, the Article 29 Working Party adopted in the course of 2012 a working document laying out the elements and principles to be found in BCRs for Processors[22] and an application form for submitting BCRs for Processors.[23]

BCRs for Processors are meant to be a tool which would help frame international transfers of personal data that are originally processed by a Processor on behalf of an EU Controller and under its instructions[24], and that are sub-processed within the

[20] WP 74, op.cit., p. 4.
[21] Article 29 Data Protection Working Party, "Explanatory document on the Processor Binding Corporate Rules" WP 204, 19 April 2013, accessed 20 April 2016, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp204_en.pdf
[22] Article 29 Data Protection Working Party, "Working document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules", WP 195, 6 June 2012, accessed 20 April 2016, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf
[23] Ibidem.
[24] WP 204, op.cit., p. 7.

Processor's organisation. BCRs for Processors are, in many respects, very similar to BCRs for Controllers. For example, they must also be binding on the members of the group and employees, and create third party beneficiary rights[25] for data subjects. The BCRs must be attached to the services agreement and must be made binding towards the data controller. The data processor must only act on the instructions of the data controller, which might be a third party customer.

2.2. Content of BCRs

On 3 June 2003 the Article 29 Working Party issued working paper WP 74 specifying the idea of BCRs.[26] Other Working Papers 153, 154, 155 and 195[27] of the Article 29 Working Party provide companies with guidance on what compliant BCRs should include. For creating BCRs it is strongly recommended to use the model application form authorised by the Article 29 Working Party[28]. Those documents will be explained below.

2.2.1. Checklist

Following the opinions of the Article 29 Working Party, it can be distinguished the content that such a document should contain. BCRs should define exactly all the entities that are part of the group, in which the rules are introduced. The types and categories of data transfers should be specified as well as the countries to which the data will be transferred. In addition, the scope of the processed data should be described and the data subjects should be generally determined. Next, BCRs should describe the mechanisms that will serve the enforcement of the provisions within the

[25] More in chapter 2.4.
[26] WP 74, op.cit., p. 4.
[27] WP 195, op.cit., p. 7 and Article 29 – Data Protection Working Party "Working Document setting up a framework for the structure of Binding Corporate Rules", WP 154, 24 June 2008, accessed 15 March 2016 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp154_en.pdf
[28] Article 29 – Data Protection Working Party, "Recommendation 1/2007 on the standard application for approval of Binding Corporate Rules for the transfer of personal data", WP 133, 10 January 2007, accessed 15 March 2016, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp133_en.doc

internal and external relationship of the group. It is also necessary to indicate the legal basis to legalize collection and processing of data within the group. It should also be remembered to indicate the rights that data subjects are entitled to and to introduce mechanisms that will allow for their effective enforcement. Further, BCRs can determine what requirements will be applied to entities outside of the group, which provides the data or entrusts the processing. Finally, it is necessary to appoint the person who will be responsible for monitoring compliance with the BCRs within the group and an indication of the way in which the binding rules will be made available to data subjects and data protection authorities.

Binding Corporate Rules must at least relate to the "content principles", set out by the Article 29 Working Party in Working Paper WP 12[29] on transfers of personal data to third countries, among others: the purpose limitation principle, the data quality and proportionality principle, the transparency principle, the security principle, etc.

These rules must pass through a DPAs approval procedure to ensure adequate compliance by the companies.[30]

2.2.2. Liability

The internally binding nature of the rules must be clear and sufficient to be able to guarantee compliance with them outside the EU/EEA, normally under the responsibility of the European headquarters, which must take any necessary measures to guarantee that any foreign member brings their processing activities into line with the undertakings contained in the BCRs.

The BCRs should indicate that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the Binding Corporate Rules is entitled to receive compensation from the controller for the

[29] Article 29 – Data Protection Working Party, "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive", WP 12, 24 July 1998, accessed 15 March 2016, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf

[30] Traci Biedermann, "The end of a safe harbour: The Schrems decision calls for stricter standards for protection of personal data transferred to the US", Columbia Journal of European Law, 15 February 2016, accessed 20 April 2016, http://cjel.law.columbia.edu/preliminary-reference/2016/the-end-of-a-safe-harbor-the-schrems-decision-calls-for-stricter-standards-for-protection-of-personal-data-transferred-to-the-us/

damage suffered. In addition to this general right, the rules must also contain provisions on liability and jurisdiction aimed at facilitating its practical exercise.[31]

The headquarters (if EU-based) or the European member with delegated data protection responsibilities should accept responsibility for, and agree to take the necessary action to remedy, the acts of other members of the corporate group outside the Community and, where appropriate, to pay compensation for any damages resulting from a violation of the Binding Corporate Rules by any member bound by the rules.

Moreover, BCRs must state that the entity that has accepted liability will also have the burden of proof to demonstrate, that the member of the group outside the EU is not liable for any violation of the Binding Corporate Rules, which has resulted in the data subject claiming damages. If the entity that has accepted liability can prove that the member of the group outside the EU is not responsible for the act, it may discharge itself from any responsibility.

If the headquarters of the corporate group were not established in the EU/EEA, should delegate these responsibilities of the headquarters to a member based in the EU. Thereby the effective adducer of the safeguards remains responsible for the effective compliance with the rules and guarantees enforcement[32]. This member would accept liability for breaches of the rules outside of the EU/EEA.

Liability under BCRs is generally based on the accountability principle. The main purpose of accountability is to use the law to hold businesses accountable for taking their responsibilities seriously by using various mechanisms to encourage or force businesses to put internal governance structures and management systems in place. Accountability appears in the new GDPR.[33]

The BCRs for Processors identify which member of the corporate group with delegated data protection responsibilities will accept responsibility for and agree to take the necessary action to remedy the acts of other members of the organisation established outside the EU and, where appropriate, to pay compensation for any

[31] "Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries", accessed 15 March 2016, http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

[32] WP 74, op.cit., p. 4.

[33] Lokke Moerel, "Binding corporate rules: Fixing the regulatory patchwork of data protection", p. 190, Tilburg University, 2011.

damages caused. In case no member of the organisation is established in the EU, the headquarters of the group, located outside of the EU, will take this liability.

The delegated member will subsequently have to seek redress for any breaches of the BCRs by a group company. For those purposes most multinationals have intra-company arrangements in place to back up the BCRs with intra-group agreements, either in a multi-party agreement in which all group companies participate, or each group company has a separate identical contract with the parent.[34]

2.3. Procedure for acceptance of BCRs

On April 14, 2005 the Article 29 Working Party adopted the working paper WP 108[35] containing a checklist for approval of the Binding Corporate Rules. Establishing BCRs requires the involvement of several European data protection authorities (DPAs) at the same time.[36] In order for BCRs to be accepted, the draft of the BCRs must be sent together with the standardised application forms to the lead authority, which is the contact point and which will handle the procedure for the review of the BCRs by all DPAs.[37] In order to officially designate an authority as the lead authority, the company needs to fulfil form WP 133 Part I and to communicate it to the authority it intends to designate. This authority then informs all of the supervisory authorities in EEA member countries where affiliates of the group are established, although their participation in the evaluation process of the BCRs is voluntary, data protection authorities concerned should incorporate the result of the evaluation into their formal licensing procedures. The lead authority starts the EU cooperation procedure by circulating the BCRs to the relevant DPA, i.e. of those countries from where entities of the group transfer personal data to entities located in countries, which do not

[34] Moerel 2011, op.cit., p. 10.
[35] Article 29 Data Protection Working Party, "Working document establishing a model checklist application for approval of Binding Corporate Rules", WP 108, 14 April 2005, accessed 20 April 2016, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp108_en.pdf
[36] WP 154, op.cit., p. 8 and Article 29 Data Protection Working Party, "Working document setting up a table with the elements and principles to be found in Binding Corporate Rules", WP 153, 24 June 2008, accessed 20 April 2016, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp153_en.pdf
[37] WP 133.op cit., p. 8.

ensure an adequate level of protection. The EU co-operation procedure is closed after the countries under mutual recognition[38] have acknowledged receipt of the BCRs and those which are not under mutual recognition have considered that the BCRs comply with the requirements set out by WP29 (within one month). Once the BCRs have been considered as final by all DPAs, the company shall request authorisation of transfers on the basis of the adopted BCRs by each national DPA.[39]

In order to simplify the proceedings, corporate groups interested in a licence for similar types of data export from several Member States may make use of a coordinated procedure. Such a procedure has been developed by the Article 29 Working Party.[40]

The main idea behind these procedural arrangements is to allow companies to go through one process of application for authorisation via the data protection authority of one Member State (leading coordinator authority) that will, through the coordination process between the data protection authorities involved, lead to the granting of the required authorisations, in accordance with the respective national laws, by all the different data protection authorities of the Member States where this company operates.

It is important to note that the coordination procedure is not a system of mutual recognition.

In order to speed up the EU procedure of cooperation for the BCRs review by data protection authorities, a mutual recognition procedure (MRP) has been agreed. Under this procedure, once the lead authority considers that BCRs meet the requirements as set out in the working papers, the DPAs under mutual recognition accept this opinion as a sufficient basis for providing their own national permit or authorisation for the BCRs, or for giving positive advice to the body that provides that authorization. At the moment, twenty one countries are part of the mutual recognition procedure.[41]

---

[38] Explained later in this chapter.
[39] European Commission, "Procedure", accessed 12 February 2016, http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/procedure/index_en.htm
[40] Article 29 – Data Protection Working Party, "Working document setting forth a cooperation procedure for issuing common opinions on adequate safeguards resulting from binding corporate rules", WP 107, 14 April 2005, accessed 15 March 2015, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp107_en.pdf
[41] European Commission, „What is mutual recognition?" accessed 20 April 2016 http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/mutual_recognition/index_en.htm

The MRP requires that one of the DPAs is appointed as the Lead DPA. This Lead DPA will be assisted by one or two other of the relevant DPAs to co-review the BCRs (Co-Leads). The Co-Leads should be the DPAs of a Member State where the relevant multinational has “a strong presence”. Shortly, the multinational submits its BCRs application to the DPA. This DPA will subsequently contact the other DPAs involved to solicit their consent, that it indeed may act as Lead DPA. Then the consultation phase starts, where the BCRs are reviewed by the Lead DPA and discussed with the multinational. After the consultation phase has ended the BCRs will be informally approved by the Lead DPA. The comments of the Co-Leads may lead to further consultations with the multinational and possible changes to the BCRs. The so-finalised BCRs will then have to be formally adopted by the ultimate parent of the multinational. After having been formally adopted by the multinational, the BCRs will be submitted for formal approval by the Lead DPA. Upon formal approval by the Lead DPA, the BCRs will automatically be recognised by the other DPAs that are part of the MRP. [42]

Other members states, not part of the MRP, will be also involved by the lead authority and will apply their own independent review process within a limited timeframe.

2.4. Enforcement

Data subjects covered by the scope of the BCRs for Processors must become third party beneficiaries by means of inclusion of a third party beneficiary clause within the BCRs, which must be given a binding effect either by unilateral undertakings (where possible under national law) or by contractual arrangements between the members of the Processor’s group.

BCRs for Processors must state that all Controllers shall have the right to enforce the BCRs for Processors against any member of the Processor’s group for breaches it caused. The Controller should also have the power to enforce the written agreement against any external sub-processor at the origin of the breach.[43]

[42] Moerel 2011, op.cit., p. 10.
[43] WP 204, op. cit. 7.

In any case, data subjects should be entitled to enforce compliance with the rules against the Controller both by lodging a complaint before the data protection authority or before the court competent for the EU Controller.[44]

However, in case data subjects are not able to bring a claim against the Controller, they may also take action against the Processor. If this choice is not practicable (for instance, there is no Processor establishment within the EU), data subjects shall be entitled to lodge a complaint to the court of their place of residence.

Information about third party beneficiary rights should be easily accessible for the data subject. The existence of third party beneficiary rights and their content is an important option for a data subject when considering what remedies are available to them[45].

Binding corporate rules must contain a commitment that when a member of the corporate group has reason to believe that the law applicable to it prevents the company from fulfilling its obligations under the BCRs and has substantial effect on the guarantees provided by them, it will inform the EU headquarters or the EU member with delegated data protection responsibilities (except where prohibited by criminal law), and that when there is conflict between national law and the commitments in the BCRs, the company must "take a responsible decision on what action to take" and consult the competent DPAs in case of doubt.[46] Informing other members of the company or the DPAs about conflicts with third country law can by itself provide no protection to data processing, and DPAs can take no action to do so besides blocking data transfers outside the EU, which does not provide effective protection on a large scale and raises legal issues of its own.[47]

At present certain DPAs lack certain enforcement rights which they try to obtain via the BCRs regime. If the enforcement regime were properly harmonised, this would no longer be necessary. As equal enforcement powers do not also guarantee a harmonised enforcement strategy, it is important to further develop a common enforcement strategy for the Lead DPAs to ensure a common approach.[48]

---

[44] Article 29 – Data Protection Working Party, "Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules", WP 155, 24 June 2008, accessed 15 March 2016, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp155_rev04_en.pdf

[45] WP 74, op.cit., p. 4.

[46] WP 154, op.cit., p. 8.

[47] Christopher Kuner, "Reality and illusion in EU data transfer regulation post Schrems, March 2016, University of Cambridge.

[48] Moerel 2011, op.cit., p. 10.

Both the general principles of compliance, as well as the opinions of the Article 29 Working Party, clearly confirm that the mere implementation of BCRs will not ensure its effectiveness. For this purpose it is necessary to introduce mechanisms for effective enforcement of regulations being implemented. Such activities include among others: regular assessment of the level of involvement of employees in compliance with the standards of the organization, and taking into account ethical behavior in the context of mechanisms of assessments of the personnel; transparent internal communication (i.e. plain language), and regular training for employees in the existing standards and procedures; implementation of procedures for internal reporting and controlling, including ensuring the possibility of anonymous notification of violations (i.e. whistleblowing); informing the public of the action taken and the results of controls, e.g. in the form of information posted on the websites of organizations. [49]

The above mentioned activities are not unique to the BCRs, but are the core system of compliance management in enterprises. It can therefore be concluded that the implementation of BCRs in companies that have not benefited so far from this solution, but who have created effective systems of managing compliance in relation to other aspects of its activities, should not be a big challenge and can bring measurable benefits in the form of compatibility of actions of the group with the regulations on personal data protection and reduce the risk of liability in this respect.

2.5. New BCRs

The ruling on 6 October 2015 of the Court of Justice of the European Union (CJEU) invalidating a decision of the European Commission that established the EU-US privacy Safe Harbour Principles has affected BCRs.[50] In October 2015 the Commission gave full support to BCRs. Most EU Member States require authorisation of BCRs, in order to facilitate and quicken that process a standardised

[49] Christine Parker, “Meta-regulation: legal accountability for corporate social responsibility”, Cambridge University Press 2007.
[50] Safe Harbour Principles see chapter 4.1.

application form can be used coupled with a procedure, under which one DPA will act as lead to handle the authorisation process.[51]

Further consequence was that the German DPA would issue no new approvals for BCRs and ad hoc data export agreements to the US.[52] More surprisingly, the DPA stated that "for now" not any new approvals for BCRs will be issued. This put businesses in a difficult position that were considering implementing BCRs as a replacement for Safe Harbour and intended to rely on BCRs for transfers of data from Germany to the US.[53] Businesses thus did not have many alternatives but to implement EU Standard Contractual Clauses, and wait for further development of replacement of the Safe Harbour. Other countries stated that organisations could continue to use other tools such as SCCs and BCRs for transfers to the US.[54]

The Schrems case raised the bar required for an adequacy decision to "essential equivalence."[55] The overall impression is that the EU „adequacy" requirement is not possible to be adopted by the world and cases of sending data based on "adequacy" will thus become incidental.

The obtain situation in which gaining the adequate level of data protection is almost impossible makes some space left to strengthen position of BCRs. Recognition of this issue we can find in the latest text of the General Data Protection Regulation (GDPR),[56] where BCRs, for the first time, were recognized in official EU document, demonstrating their necessity and validity to the lawful data transfer all over the world.

---

[51] Communication from the Commission to the European Parliament and the Council on the transfer of personal data from the EU to the United States of America under Directive 95/46/EC following Judgment by the Court of Justice in case C-362/14 (Schrems), 6 November 2015, accessed 15 May 2016, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf

[52] Der Hessische Datenschutzbeauftragte, accessed 15 May 2016, https://www.datenschutz.hessen.de/ft-europa.htm#entry4521

[53] Christoph Zieger, Daniel Ashkar, Marcus Evans, "German Data Protection Authorities suspend BCR approvals, question Model Clause transfers", Data Protection Report, 26 October, 2015, accessed 15 May 2016, http://www.dataprotectionreport.com/2015/10/german-data-protection-authorities-suspend-bcr-approvals-question-model-clause-transfers/

[54] Mark Young, Monika Kuschewsky, Kristof Van Quathem, Joseph Jones, "EU DPA enforcement guidance post – Schrems", Inside Privacy, 18 February 2016, accessed 15 May 2016, https://www.insideprivacy.com/international/european-union/eu-dpa-enforcement-guidance-post-schrems/

[55] Para. 73, Schrems Case 2015, op.cit., p.16.

[56] Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), 27 April 2016, accessed 15 May 2016, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Explicit legal recognition of BCRs in the new General Data Protection Regulation is to be welcomed, so that any remaining legal barriers to their use under member state law will be removed. The GDPR lists BCRs as an appropriate safeguard in Article 46 and provides detailed conditions for transfers by way of BCRs in Article 47. Those provisions specify that BCRs require approval from a supervisory authority in accordance with the consistency mechanism in Article 63 and govern what must be included in BCRs at a minimum, such as structure and contact details for the concerned group, information about the data and transfer processes, how the rules apply general data protection principles, complaint procedures, and compliance mechanisms.

According to Article 4, subsection 20, of the new Regulation BCRs "means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings." Use of BCRs is limited to companies in "the same corporate group of undertakings".[57] "Group of undertakings" means a controlling undertaking and its controlled undertakings.[58]

It also uniforms criteria for BCRs approval that apply across the EU and makes the BCRs approval process subject to the consistency mechanism specified in the GDPR.[59] The GDPR also removes any obligation to obtain additional approval from data protection authorities for transfers of personal data based on BCRs.

The GDPR recognises BCRs for Controllers and Processors as a means of legitimising intra-group international data transfers,[60] although, the final position of the European Parliament (from March 2014) suggested removing the reference to data Processors and replacing it with wording recognizing BCRs only for the "Controller's group of undertakings and those external subcontractors that are covered by the scope of the binding corporate rules," which might cause confusion among companies.[61] The final GDPR text keeps Processors in the definition of Binding Corporate Rules.[62]

[57] Recital 110, GDPR, op.cit., p. 16.
[58] Article 4 (19), Ibidem.
[59] Article 47(1), Ibidem.
[60] Article 4(20), Ibidem.
[61] General Data Protection Regulation (Provisional Draft, P7_TA-PROV(2014)0212), March 2014, Article 43(1)(a) and (f), accessed 23 June 2016,

The BCRs must be legally binding and apply to[63] and be enforced by every member of the group of undertakings/enterprises engaged in a joint economic activity, including their employees. They must expressly confer enforceable rights on data subjects.[64] The approach will be more streamlined with a clear list of requirements. [65]

The requirements for BCRs contained in Article 47 are generally similar to those that have been set forth already by the Article 29 Working Party.

The most significant procedural change under the GDPR is that the BCRs approval process will trigger the ‘‘consistency mechanism’’, for ensuring that the current cultural differences do not affect the interpretation of and enforcement of the Regulation. Article 63 states, “[i]n order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism.”

The consistency mechanism is a new concept, which means that the data protection authorities are required to co-operate with each other and, where relevant, with the European Commission that enhances and formalizes the cooperation of DPAs through their participation in the European Data Protection Board. It will replace the mechanism that European DPAs have developed to cooperate in the context of approving BCRs (i.e., mutual recognition procedure).

At present, the Working Party requires that the BCRs contain a duty for the EU headquarters of the company, or a delegated subsidiary in the EU, to assume liability for violations.[66] By contrast, the Regulation does not expressly require that the EU headquarters or a delegated subsidiary assume liability, but refers to acceptance of liability by a “Controller or Processor established on the territory of a Member State”[67], which gives companies more flexibility in structuring their liability schemes.[68]

---

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN

[62] Article 4(20), GDPR, op.cit., p. 16

[63] Article 47(1)(a), Ibidem.

[64] Article 47(1)(b), Ibidem.

[65] Article 47(2), Ibidem.

[66] WP 153, op.cit., p. 11.

[67] Article 47(2)(f), GDPR, op.cit., p. 16.

[68] Christopher Kuner, “the European Commission’s proposed Data Protection Regulation: A Copernican revolution in European Data Protection Law”, Bloomberg, 6 February 2012.

Countless data transferred between corporations placed all over the world is raising, the problem of the safety of the data subjects will not solve by itself. Flexible legal nature of BCRs adjusted to the market demands is a huge advantage. The Article 29 Working Party has issued papers based on the current situation, for example WP 12, making the process of application easier. Liability rules based on the accountability principle make all companies subject to the strict European law and make claiming damages clearer and accessible for the data subjects. The procedure is getting easier and faster thanks to the co-operation procedure and mutual recognition, soon replaced by the new consistency mechanism formalizing the cooperation of DPAs. Third party beneficiaries make the enforcement easier for the data subjects. Other recommendations to improve enforcement of data protection rights are: regular assessment of the level of involvement of employees in compliance with the standards of the organization, and taking into account ethical behaviour in the context of mechanisms of assessments of the personnel; transparent internal communication (i.e. plain language), and regular training for employees in the existing standards and procedures. The Schrems Case made the EU legislator aware of the need of modern codification and influenced quick modification of data protection regulation and also questioned cross-border data transfers on the ground of BCRs, that is why it was needed to be officially recognized. The new GDPR gives clarity and increases simplicity introduced in relation to BCR, it is likely that more businesses will opt for BCRs as a means of legitimising international transfers of personal data. In general the BCRs recognition and upcoming changes demonstrate that the EU wants to keep its strict data protection policy, however EU also notices global market needs and so tries to make data transfer solutions more adjustable.

Abovementioned implies that we already have a promising global data transfer tool. However, companies are quite reluctant about implementing the rules. This might be due to disadvantages like BCRs being too burdensome and discouraging, a lack of transparency and insufficient information. Moreover, is possible that organisations simply find the BCRs' solutions to international data transfer impractical.

3. Analysis of positive and negative aspects of BCRs and upcoming changes

The BCRs process has certainly evolved over time, but in the more than ten years of its evolution, it has become much more streamlined.

The main advantage of BCRs over other means of providing adequate safeguards is that, once developed and operational, BCRs can provide a framework for a variety of intra-group transfers to meet your organisation's requirements. However, if one makes changes to his company or the data flows that go beyond the scope of the authorisations, he will have to reapply for authorisation for all or part of the processing.

This chapter takes a closer look on what works against and in favour for BCRs to become a global instrument of data transfer and features that hinder this development. The chapter clarifies if there is a reason for organisations to stay so reluctant to implement this solution.

3.1. Disadvantages

Since the first set of BCRs was pioneered in 2005, fewer than 30 companies have, at year 2012, submitted applications that have been approved across Europe[69]. As of the beginning of 2015, 65 companies have formally adopted BCRs and by now (May 2016) the number increased to around 85.[70]

The reason of this primary aversion to adopt BCRs could be fear of costs, also due to the time consuming nature of establishing BCRs and most of all – early applicants might discourage the later ones.

[69] Rohan Massey, Heather Egan Sussman, Alison Wetherfield, "Binding corporate rules as a global solution for data transfer", Lexology, 19 June 2012, accessed 19 June 2016, http://www.lexology.com/library/detail.aspx?g=353eff70-2fd3-4c7e-a8ab-571893b4b6a1

[70] "Overview on Binding Corporate Rues", European Commission, accessed 19 June 2016, http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm

The original BCRs system was overly bureaucratic and costly. When the BCRs system first started, the applicant would have to seek authorization from each Data Protection Authority in the EU.

Peter Fleischer called BCRs: data protection for the rich.[71] In 2012 the system was more streamlined with five to seven DPAs as reviewer with a single DPA acting as the lead. This shrank the time in obtaining BCRs from a few years to around 9 months.[72] What is not changing is the core set of principles available to all multinationals since 1980, nor the commitment by the EEA to make the process of approving BCRs simpler and more accessible.

The European Commission explanatory memorandum[73], states that Article 43 (now 47) of the Regulation deals specifically with transfers by way of BCRs and it is "based on the current practices and requirements of supervisory authorities." Despite all the steps taken, the process might still seem expensive and cumbersome, what might be discouraging small and medium – sized enterprises.

Under the current procedure, each national DPA can demand specific changes at the BCRs' draft which can result in a very lengthy and costly approval period for the company. In coming soon GDPR, the BCRs' procedure outline seems simplified. The minimum content of Binding Corporate Rules is decreased compared to the more comprehensive requirements currently presented in the guidance of the Article 29 Working Party.[74]

Also, under the current regime, the review procedure has been designed to have one lead authority which means that the applicant company does not need to approach each individual DPA separately, but if the DPAs do not participate in the mutual recognition procedure the company might organize meetings with them to close their BCRs approval process. Under the GDPR, the co-reviewer process will no longer be the case, since the consistency mechanism ensures the opinion of all

[71] Mehmet Munur, "Binding Corporate Rules and the proposed EU Data Protection Regulation", Tsibouris Privacy + Technology Blog, 23 December 2011, accessed 23 June 2016, http://blog.tsibouris.com/2011/12/binding-corporate-rules-and-proposed-eu.html
[72] Ibidem.
[73] Proposal for a Regulation of the European Parliament and of the Council, 25 January 2012, accessed 15 July 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN
[74] Article 47, GDPR, op.cit., p. 16.

DPAs to align. Dealing with one DPA is very positive for companies, as they can build relationships and trust with their DPA before starting a BCRs project.[75]

Since the GDPR does not contain DPA notification and authorization requirements for data transfers, the national authorizations of BCRs will be abolished, where they exist, thus providing a more flexible mechanism in which approval of BCRs and commencement of transfers under the approved BCRs can be merged to occur at the same time. [76]

What is not going to change under new GDPR, but could be an advantage for development of BCRs as a global data transfer instrument, is that BCRs only cover intra-group data transfers. The applicant from the group must demonstrate in its application that the BCRs are binding on all members within the group: this requires the company to examine the structure of its group and the applicable law to each member of the group.[77]

An organization may have to develop or review its strategy for handling data transfers to non-members of the group since non-members would not be bound by the BCRs. For example, the organization should assess whether additional contracts should be implemented to cover non-member recipients.[78]

Some other reason that might discourage potential, global users of BCRs is the liability regime.

The Working Party 29 BCR proposal paper stressed that the data subject must be given third party beneficiary rights no less extensive than those granted to him under the SCCs.[79] However, the Working Party's paper was drafted before the European Commission accepted the ICC's liability regime amendment to the Controller-to-Controller SCCs, which changed that liability regime for data exporter

---

[75] Anna Pateraki, "EU regulation Binding Corporate Rules under the GDPR – what will change?", Bloomerg BNA, March 2016, Accessed 18 June 2016, 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

[76] Anna Pateraki 2016, Ibidem.

[77] Philip Rees, Dominic Hodgkinson, "Transfers of personal data and Binding Corporate Rules. Binding Corporate Rules: a simpler clearer vision?", Computer Law & Security Report 23, 2007.

[78] Myriam Gufflet, Anna Pateraki, "Why do we need Binding Corporate Rules? A look to the future", Bloomberg BNA, 3 February 2015, accessed 20 June 2016, https://www.wsgr.com/eudataregulation/pdf/pateraki-0315.pdf.

[79] WP 74, op.cit., p. 4.

and importer from joint and several to liability based liability. Unfortunately, every sub-sequent Working Party paper on the BCRs does not address this issue. Therefore the BCRs liability regime is potentially more unattractive to multi-national companies than the revised SCC.[80]

In some Member States the legal enforceability of a third party beneficiary clause contained in unilateral declarations does not raise any doubts, however in other Member States the situation is not hat clear and unilateral declarations might not be sufficient as such. Where unilateral declarations cannot be considered as granting legally enforceable third party beneficiary rights, the organisations would have to put in place the necessary contractual arrangements[81] allowing for that. Contractual arrangements can be legally enforced under private law in all Member States. [82]

Most state regulation is aimed solely at protecting individuals in the territory of this state, whether the offensive acts are performed in the territory or aimed at the citizens in the relevant territory.[83]

3.2. Advantages

What actually was discouraging companies from implementing BCRs and thus becoming a global instrument? Firstly, lack of harmonization. Directive 95/46/EC, by its status, leaves little margin for Member State implementation, which might cause quite significant differences in law application.[84] The European Commission stated that existing rules do not provide the degree of harmonization required and that there is a substantial lack of harmonization in important areas.[85] The principle that data protection standards are uniform among the Member States is thus a legal fiction, and there is a gulf between the presumption of harmonisation among Member State laws and the reality on the ground.[86]

[80] Rees, Hodgkinson 2007, op.cit., p. 22.
[81] Contractual arrangements are written mutual agreements, enforceable by law, between two or more parties that something shall be done by one or both.
[82] WP 204 rev. 01, op.cit., p. 7.
[83] Moerel 2011, op.cit., p. 10.
[84] Kuner 2012, op.cit., p. 18.
[85] European Commission, “Safeguarding Privacy in a Connected World”.
[86] Kuner 2016, op,cit., p. 14.

Further, forcing organizations to comply with the strictest regimes may discourage them from adopting BCRs. Additionally, many Member States have adopted differing views on the binding nature of BCRs and in some Member States, such as Spain, there is no provision in the law for recognizing Binding Corporate Rules.

The Article 29 Working Party, has issued extremely clear and helpful working papers that demystify and assist the process: WPs 74, 108, 133, 153, 154 and 155 in particular.[87] These enable businesses to do an enormous amount of research internally and cost effectively.

However, it is going to change. The GDPR explicitly acknowledges as valid the current requirements for BCRs for controllers and processors, which will be helpful for data transfers involving those member states that do not as yet recognize BCRs.

The GDPR will be directly applicable. It would provide as near complete harmonization as is possible under EU law. It would also make companies with operations in multiple EU member states subject to the jurisdiction of a single DPA. Commonly binding regulation leads to a greater degree of harmonization, since it immediately becomes part of a national legal system, without the need for adoption of separate national legislation; has legal effect independent of national law; and overrides contrary national laws.[88] Data transfer instruments, like BCRs, might become more powerful thanks to new clarity and unification.

What makes BCRs convenient, as a data transfer instrument, is that once the BCRs have been submitted, approved and implemented in accordance with the procedure, a company is free to transfer data globally within its affiliates, without the need to use the SCCs each time such data are transferred.[89] The BCRs will create a "safe haven" by removing the country borders for the transfers within the members of the corporate group.[90] It is practical for most corporations, as the information does not flow uncomplicated and stable paths, but moves along multiple courses through the exchange of e-mail and access to databases.

[87] European Commission, Opinions and Recommendations, accessed 27 July 2016, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

[88] Paul Craig and Gráinne de Búrca, "EU Law: Text, Cases, and Materials", Oxford University Press, 2011.

[89] Rees, Hodgkinson, 2007, op.cit., p. 22.

[90] Christopher Kuner, Chair Robert Bond, International Chamber of Commerce. "ICC report on Binding Corporate Rules for international transfers of personal data", ICC, 28 October 2004.

"The BCR is really the glue, putting together all the different modules necessary for a company" said Daniel Pradelles[91], HP's privacy officer for Europe, the Middle East and Africa, who facilitated the BCRs application process under the supervision of HP's lead data protection authority for the certification, France's CNIL.[92] Uniformity is important for a company the size of HP, operating in as many jurisdictions as it does and trying to tell its thousands of employees how to handle data.

BCRs can meet all of the cross-border requirements in non-EU jurisdictions, such as Japan, Australia and Argentina; at the same time, an organization may have to provide protections greater than those required in non-EU jurisdictions [93] and there is no set wording for the BCRs, so companies can tailor them to suit their own needs, and indeed can base them on any existing data handling policies they have, which can also aid employee comprehension and ensure fewer breaches.

BCRs also gain a competitive advantage thanks to the structure of their documents: companies may regulate other issues in them, not only data protection, such as direct marketing and children's privacy. In this way, the company can achieve a global privacy policy even in jurisdictions without any specific data protection laws, and with less paperwork, administrative and legal complexities than under the contractual solution.[94] SCC's regime creates a large number of contracts, do not offer complex uniformisation and demands renewals whenever the data details of data processing change.[95] The BCRs impose no obligation on the data exporter to warrant and undertake that he has used reasonable efforts to determine that the data importer is able to satisfy its legal obligation, so different affiliates do not have to carry out checks on each other: some critics commented that US companies in particular might object to such checks being carried out on them by their UK affiliates.[96]

Compliance is a way of organizing the company, the aim of which is to ensure compatibility of business activities with the ethics and law. Implementation of compliance helps to reduce the legal risks associated with running business and

[91] Angelique Carson, "Hewlett-Packard first to win certification for BCRs, CBPRs", The International Association of Privacy Professionals, 25 November 2014, Accessed 21 June 2016, https://iapp.org/news/a/hewlett-packard-first-to-win-certification-for-bcrs-cbprs/
[92] Angelique Carson 2014, ibidem.
[93] Wugmeister, Retzer, Rich 2007, op.cit., p. 2.
[94] Wugmeister, Retzer, Rich 2007, Ibidem.
[95] SCCs see chapter 4.2.
[96] Rees, Hodgkinson 2007 , op.cit., p. 22.

helps effectively protect the company from the negative consequences of unlawful conduct of employees.[97]

One of the areas of compliance is the issue of IT security, including matter related to developing outsourcing services and data protection. In the case of large capital groups, the number of documents that regulate the transfer can pile up to several hundred (privacy policy and security, the agreement transfer, instructions, etc.). A large amount of documentation and frequent lack of its internal cohesion raises the potential to abuse and hinders the education of employees in this respect. Thanks to BCRs number of documents is significantly reduced and easier for workers to understand and apply in practice the rules governing the processing of personal data.

The laborious BCRs process also seems to be only its reputation. Pradelles said that this is more myth than truth.[98] "There is often a confusion between building the infrastructure supporting the BCR that a company should and must have in place, BCR or not, and the BCR itself, which is the documentation. Often people are mixing them together," he claimed.

HP VP and Chief Privacy Officer Scott Taylor, said there was nothing about the BCRs process that was difficult, laborious or challenging. "A company should have similar data protection processes in place in any case, he said, so simply documenting that it does, using guidance documents like Working Document 153 and 154 under the general BCR framework, isn't particularly taxing."[99]

BCRs bring also convenience for the individuals. Since a multinational company adopts globally the same privacy rules, the data subjects are granted with rights also in jurisdictions without any data protection legislation. In case they want to file a complaint for a data breach, they can do so at their local office of the corporate group, in their native language, no matter where the data breach took place and which corporate member was responsible for it. [100]

---

[97] Anna Partyka – Opiela, Wiążące reguły korporacyjne (BCR) jako element efektywnej polityki compliance", Domański Zakrzewski Palinka sp.k, accessed 7 August 2016, https://www.dzp.pl/files/Publikacje/Prawne_aspekty_us%C5%82ug_chmurowych_2015.pdf
[98] Carson 2014, op.cit., p. 25.
[99] Carson 2014, Ibidem.
[100] Wugmeister, Retzer and Rich 2007, op.cit., p. 2.

Under the BCRs, on the companies lies the burden of ensuring compliance (accountability). Both, the existing data protection framework and the GDPR seek to achieve compliance by the threat of penalties in case of violations.[101]

It is unfortunate, however, that the provisions concerning BCRs fail to propose any way to lessen the burden on SMEs of complying with the data transfer restrictions.[102]

Lately, there are opinions that an easier BCR procedure and lower costs might encourage medium-sized companies.[103] BCR authorization as safe processors should enable cloud service providers to provide cloud services to other companies using their BCRs. Using the older BCR system, companies were only able to obtain BCR authorization applying to data for which they were the data controllers. With this new system, BCRs for data processors should also be possible. As a result, BCRs should become a true option for midsize companies and processors of all kinds--and quite likely a favoured option for cloud service providers.[104]

Analysis of pros and cons of BCRs as a global instrument for the vast amount of personal data speaks in favour of them. Some of the solutions, that already exist, do not need improvement, such as transferring data beyond country borders, the high standard of EU regulation that meets other regions requirements and that BCRs are tailor-made solution satisfying different needs of different companies. BCRs might be a document of compliance, reducing number of documentation, increases accountability and makes enforcing one's rights easier, others are already revised by GDPR which will be directly applicable and will harmonise the European Law, so problem of different legal regulations is eliminated; also improved by opinions issued by Article 29 Working Party on simplifying and accelerating the BCRs application and award procedure.

At the same time current flaws are being revised. The lack of harmonisation will become lesser problem, because of no need for national implementation. At the national level will be left nuances to regulate such as differences in interpretation and national choices, like age of child to give consent (between 13 and 16). There are still

[101] Kuner and Bond 2004, op.cit, p. 24.
[102] Kuner, 2012, op.cit., p. 18
[103] Gufflet, Pateraki 2015, op.cit, p. 22.
[104] Munur 2011, op.cit., p. 21.

opinions among entrepreneurs regarding the BCR procedure, derived from outdated opinions, that it is still time consuming and costly. It requires decent information campaigns, that might also encourage SME’s to give up other solutions.

4. Other EU methods for data transfer and their validity for becoming a global instrument

Under the new Regulation there are three categories of mechanisms that may legalize international data transfers, namely a Commission adequacy decision under Article 45; the use of "appropriate safeguards" under Article 46 (which include BCRs under Article 47 and SCCs); or the application of a derogation under Article 49.

The European legal system on cross-border data flows prohibits transfer of personal data to third countries which do not have an adequate data protection level, but allows the European Commission to issue decisions recognizing such countries as providing an "adequate" level of data protection.[105] Compared to the DPD, the GDPR includes a much more detailed definition of what constitutes "adequacy" for data transfers to third countries, which incorporates the standards adopted by the CJEU in Schrems.[106]

Assessment of the adequacy of data protection in third countries by the European Commission faces numerous difficulties. Countries which have effective data protection acts are rare. Those that follow the European model and could pass the assessment are even rarer. As a result, the guiding effect of regulation concerning adequacy is decreased.[107] A few states, such as the United States, Canada, and Australia, have federal legal systems. Variations exist with regard to data protection in the states.[108]

It is not completely forbidden to transfer personal data to the countries that do not ensure an adequate level of protection. If there is one of the following solutions, the data flow to a third country may be justified, even without adequacy:

1) The EU-US Privacy Shield – a framework for transatlantic exchanges of personal data for commercial purposes between the European Union and the United States, which replaced the US-EU Safe Harbour Principles – a voluntary privacy framework for US-based importers of data,[109]

[105] Article 25 (1), DPD, op.cit, p. 2.
[106] Article 45, Recital 104, 106, GDPR, op.cit., p. 16.
[107] Lingjie Kong, "Data protection and transborder data flow in the European and global context", European Journal of International Law, 2010, accessed 23 March 2016, https://ejil.oxfordjournals.org/content/21/2/441.full
[108] Kong, ibidem.
[109] Safe Harbour, Privacy Shield see chapter 4.1.

2) EU Standard Contractual Clauses (SCCs) - standard form, non-negotiable data export agreements approved by the European Commission, or

3) Binding Corporate Rules.

Under the GDPR certain bureaucratic requirements, such as notification of data processing to the data protection authorities (DPAs), would be eliminated, but other ones (such as to maintain extensive internal documentation about data processing) will be introduced.[110] As well as the possibility of transferring data on a limited basis based on a "compelling legitimate interest of the data controller",[111] the possibility for EU law or Member State law to set limits for transfers of specific categories of personal data.[112] There is also a new provision with rules regarding requests for disclosure of data by third country courts and administrative authorities.[113]

Adequacy decisions are not final. The GDPR provides that the European Commission, in the context of a particular designation, would establish for a mechanism of periodic review, at least once every four years.[114] The Commission is also obliged to monitor the situation in third countries and international organisations which may influence the functioning of adequacy decisions taken by the Commission in accordance with the Directive or the GDPR.[115] The GDPR specifically provides the possibility of an adequacy decision, taken on the basis of the Directive or the GDPR being repealed, amended or suspended.[116]

Other mechanisms introduced in the GDPR to legitimise international transfers of personal data are for example:

• transfers pursuant to contractual clauses between the Controller or Processor and the Controller, Processor or the Recipient of the data in the third country (where such contractual clauses have been authorised by the competent DPA);[117]

• transfers on the basis of an approved code of conduct (e.g. a code of conduct dealing with the transfer of personal data to third countries that has been approved by the relevant DPA);[118]

[110] Kuner, 2012. op.cit., p. 18.
[111] Article 49 (g), GDPR, op.cit., p. 16.
[112] Article 49 (5), Ibidem.
[113] Article 48, Ibidem, Kuner 2016, op.cit., p. 14.
[114] Article 45 (3), Ibidem.
[115] Article 45 (4), Ibidem.
[116] Article 45(9), Ibidem.
[117] Article 46(2)(d), Ibidem.
[118] Article 46(2)(e), Ibidem.

• transfers pursuant to an approved certification mechanism (e.g. a data protection seal or mark that has been issued by specified certification bodies or by the competent DPA on the basis of criteria approved by the competent DPA or the European Data Protection Board).[119]

Under the GDPR businesses not only need to be compliant with the provisions they are also accountable for evidencing their compliance.[120]

Below the above mentioned mechanisms will be analyzed and compared to BCRs from the point of view of their suitability for becoming a global instrument.

4.1. Comparison BCRs to Safe Harbour and Privacy Shield

Personal data cannot be transferred from the EU to the US unless the US ensures an adequate level of protection for such personal data, as that phrase has been interpreted by the CJEU. Prior to the judgment of the CJEU, where the Court found that the Safe Harbour Framework is invalid, personal data could be transferred to the US under the Safe Harbour Principles, or using the SCCs or BCRs, procedures authorized by the Directive, or by relying on an exception or other derogation set out in the Directive, or by obtaining express authorization for the transfer from a data protection authority.[121]

The US rules on data protection did not receive approval of the European Commission and were considered inadequate. Therefore, in 2000 the EU and the US signed an agreement called the Safe Harbour Principles, which enables data export from the EU to the US under certain conditions. From the beginning it was generating controversy in Europe. Serious arguments were raised by national data protection authorities and in the European Parliament on the adequacy of data protection under the Safe Harbour Agreement. The European Commission Staff Working Paper, which was drawn up on the effectiveness of the Safe Harbour released in early 2002,

[119] Article 46(2)(f), GDPR, op.cit., p.16.
[120] Article 5(2), Ibidem.
[121] Barry Sookman, "Schrems, what the CJEU decided and why it is a problem for Canadian and other non-EU businesses", Barry Sookman, 12 October 2015, accessed 15 May 2016, http://www.barrysookman.com/2015/10/12/schrems-what-the-cjeu-decided-and-why-it-is-a-problem-for-canadian-and-other-non-eu-businesses/

clearly indicated concerns about both the actual implementation and the adequacy of data protection stemming from the agreement.

It was no different in the US. Ambassador Aaron made it clear: “in no way does the US government intend for these Safe Harbour principles to be seen as precedents for any future changes in the US privacy regime”[122]

However, the limitations of the Safe Harbour are not only of a legal nature. Following the Edward Snowden revelations in 2013, the Safe Harbour was criticized on a political level for allegedly allowing extensive access to EU data by US law enforcement authorities and the European Parliament asked for it to be suspended.[123]

On 6 October 2015, the Court of Justice of the European Union decided in a landmark ruling that "massive and indiscriminate surveillance" of EU citizens by US public authorities (as revealed by Edward Snowden), after their personal data has been transferred to the United States, is incompatible with the fundamental right to protection of personal data in line with European law and declared the European Commission’s Decision on EU-US Safe Harbour invalid.[124] The Court went on to note that the Commission did not state in its Safe Harbour decision that the US ensures an adequate level of protection,[125] and that the decision was accordingly invalid, without there being any need for it to examine the substance of the Safe Harbour principles.[126] Moreover, it was access to data transferred under the Safe Harbour by the US intelligence services, which was one of the main factors in the Court’s judgment.

The Court did not introduce any transitional period, as a consequence, the transfer of personal data to the US could not continue to be based on the Safe Harbour Agreement. This had certain practical consequences for data exporting or intending to transfer them to importers in the US. However, the Article 29 Working Party released an opinion, that gave the EU and US officials time to re-negotiate the

[122] Stephen J. Kobrin, “The Trans-Atlantic data privacy dispute, territorial jurisdiction and global governance”, The Wharton School, November 2002.
[123] European Parliament resolution of 12 March 2014 on the U.S. NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens’ fundamental rights and on transatlantic cooperation in Justice and Home Affairs, P7_TA(2014)0230, 12 March 2014, accessed 22 June 2016, http://bit.ly/1LwfNve
[124] Schrems Case 2015, op.cit. p. 16.
[125] Para. 97, Schrems Case 2015, Ibidem.
[126] Para. 98, Schrems Case 2015, Ibidem.

Safe Harbour framework until the end of January 2016.[127] A failure to do so would mean that the DPAs would begin to coordinate enforcement actions across Europe.[128] Those companies that were relying on the Safe Harbour had to quickly find another solution. Corporations found themselves in an uncertain position, they could not predict either it could take a long time to create substitute for Safe Harbour or it would be a fast process, as the governments felt the pressure.

After intense negotiations between the European Commission and the US Department of State, the European Commission finally adopted its updated Adequacy Decision on the EU-U.S. Privacy Shield on 12 July 2016[129]. This amends the draft decision published on 29 February 2016.[130] The Adequacy Decision is based on the political agreement that was reached by the EU and US on 2 February 2016, and intended to replace the Safe Harbour Principles.

The Privacy Shield concerns only US – EU data transfer, so in principle, it cannot become a global instrument. However, it could be an alternative for BCRs in that area.

The Commission recognises that the "level of protection afforded by the US legal order may be liable to change" and accordingly the Privacy Shield requires the Commission to "continuously monitor" the Privacy Shield (one of the criticisms of the Safe Harbour Principles was that the original adequacy decision was not reviewed until after the Snowden revelations many years later), and the companies using the Shield as well as US authorities' compliance with it. There will be a joint annual review of the functioning of the Privacy Shield, which in effect allows the Commission to annually re-evaluate whether the Privacy Shield still provides an adequate level of protection.[131] The Commission has also provided for a re-assessment following the General Data Protection Regulation becoming effective in Member States, in May

[127] Statement of the Article 29 Working Party, 16 October 2015, accessed 17 June 2016, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf
[128] Statement of the Article 29 Working Party, 2015, Ibidem.
[129] European Commission, "Restoring trust in transatlantic data flows through strong safeguards: European EU-U.S. Privacy Shield", 29 February 2016, accessed 17 June 2016, http://europa.eu/rapid/press-release_IP-16-433_en.htm
[130] European Commission Press Release, European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows", 12 July 2016, accessed 2 December 2016, http://europa.eu/rapid/press-release_IP-16-2461_en.htm
[131] Privacy Shield, accessed 2 December 2016, https://iapp.org/media/pdf/resource_center/eu_us_privacy_shield_full_text.pdf.pdf p. 72 chapter V.

2018, to ensure that the Privacy Shield meets the level of protection required under the Regulation. As a result, there is no guarantee that the Privacy Shield, in its current form at least, will enjoy the longevity of the Safe Harbour Regime.[132] The documentation that comprises the Privacy Shield is lengthy and structured in a disorganised way, making it difficult for individuals and small companies to interpret it. Many of the supporting letters from US officials are written in US legalese and will be difficult for many people in the EU to understand. The way the Privacy Shield was drafted and presented demonstrates how regulation of international data transfers is dealt with in a predominantly untransparent and bureaucratic way.[133]

According to the Working Party's Opinion from 13 April 2016[134], there is no express data retention principle mentioned in the Privacy Shield and a data retention principle cannot be clearly construed from the current wording of the Data Integrity and Purpose Limitation principle. This may give organizations the option to keep personal data as long as they wish, even after leaving the Privacy Shield, which is not in line with the EU data retention limitation principle.

The Article 29 Working Party emphasized "that onward transfers from a Privacy Shield entity to third country recipients should provide the same level of protection on all aspects of the Shield (including national security) and should not lead to lower or circumvent EU data protection principles. In case of an onward data transfer to a third country, every Privacy Shield organisation should have the obligation to assess any mandatory requirements of the third country's national legislation applicable to the data importer, prior to the data transfer. If a risk of substantial adverse effect on the guarantees, obligations and level of protection provided by the Privacy Shield is identified, the US Privacy Shield organisation acting as a Processor shall promptly notify the EU data controller before carrying out any onward transfer." In which case, the latter should be "entitled to suspend the transfer of data and/or terminate the contract." If the Shield organization is acting as a data controller, it "should not be

[132] Andrew Shindler, Zoey Forbes, "EU-US Privacy Shield: An end to uncertainty?", 19 July 2016, King & Wood Mallesons, accessed 27 July 2016, http://www.kwm.com/en/uk/knowledge/insights/eu-us-privacy-shield-an-end-to-uncertainty-20160719

[133] Kuner 2016, op.cit., p. 14.

[134] Article 29 Data Protection Working Party, "Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision, 13 April 2016, accessed 25 July 2016, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

allowed to onward transfer the data, as this would compromise its duty to provide the same level of protection" as under the Privacy Shield.[135]

In this respect, the Working Party "recalls its position that if the EU data controller is aware of an onward transfer to a third party outside the US even before the transfer to the US takes place, or if the EU data controller is jointly responsible for the decision to allow onward transfers, the transfer should be considered as a direct transfer from the EU to the third country outside the US,"[136] in which case the EU Data Protection Directive applies instead of the Privacy Shield onward transfer principle.

The Working Party "concludes that onward transfers of EU personal data are insufficiently framed, especially regarding their scope, the limitation of their purpose and the guarantees applying to transfers to data Processors (Agents)."[137]

After approval of the Privacy Shield the Article 29 Working Party delivered a verdict[138] in which they regret, 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. The Article 29 Working Party would have simply expected stricter guarantees concerning the independence and the powers of the Ombudsperson mechanism. Generally the new document seems like an experiment, the first joint annual review will therefore be a key moment for the robustness and efficiency of the Privacy Shield mechanism to be further assessed.

The Privacy Shield certainly does impose obligations that are similar to those that can be found under the GDPR (e.g. transparency, purpose limitation, data integrity, security, access, etc.), however the GDPR imposes a lot more accountability measures on companies that are simply not required under the Privacy Shield (e.g. data protection officers, data protection impact assessments, privacy-by-design, etc.). Max Schrems has dubbed it "little more than a little upgrade to Safe Harbour, but not a new deal".[139] Therefore, if the goal is to achieve compliance with the GDPR, the

---

[135] Article 29 Data Protection Working Party, "Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision", 13 April 2016, accessed 2 December 2016, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf, p. 57.
[136] WP 238, Ibidem, p 21.
[137] WP 238, Ibidem p. 3.
[138] Article 29 Working Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield, accessed 5 August 2016, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf
[139] Shindler, Forbes, 2016, op.cit., p. 32.

Privacy Shield alone will not be sufficient. For companies who are keen to use EU data protection law as a global compliance standard within their organisation, Binding Corporate Rules may be a better option as these already cover many of the GDPR requirements.[140] The political nature of the transatlantic disagreement is shown by the fact that the EU-US Privacy Shield was only finalised by a last-minute agreement at the highest political level on a call between European Commission First Vice-President Frans Timmermans and US Vice-President John Kerry.[141]

The Privacy Shield might also be the subject of legal challenges before the DPAs and, ultimately, before the CJEU, and will not be trusted until they are resolved. As an instrument of EU law, implementation of the Privacy Shield will have to meet strict standards of proportionality, legality, legitimate interest, and compliance with fundamental rights under the Charter.[142]

In comparison to the Privacy Shield BCRs seem to provide additional security that respond to shortcomings in the Safe Harbour system indicated by the CJEU.[143] BCRs do not provide for any specific exception for sharing with governments or law enforcement agencies outside of the EU (as the Safe Harbour decision did[144]). Rather BCRs require that where a member of the group has reasons to believe that the legislation applicable to it prevents the company from fulfilling its obligations under the BCRs and has substantial effect on the guarantees provided by the rules, such member will promptly inform the EU headquarters (except where prohibited by law). In addition, the BCRs require that where there is a conflict between national law and the commitments in the BCRs, the EU headquarters, will take a responsible decision on what action to take and will consult with the competent DPA in case of doubt.[145]

Furthermore, BCRs are subject to prior approval by the lead DPA, which means that such lead DPAs and the relevant co-leads, have the opportunity to conduct an

---

[140] Olivier Proust, “EU-US Privacy Shield comes into force”, 13 July 2016, accessed 5 August 2016, http://privacylawblog.fieldfisher.com/2016/eu-us-privacy-shield-comes-into-force/

[141] Zoya Sheftalovich, “The phone call that saved Safe Harbor”, Politico, 13 February 2016, accessed 5 August 2016, http://www.politico.eu/article/the-phone-call-that-saved-safe-harbor-john-kerry-frans-timmermans

[142] Kuner 2016, op.cit., p. 14.

[143] Lokke Moerel, "An assessment of the impact of the Schrems judgement on the data transfer grounds available under EU data protection law for data transfers to the U.S.”, Morrison Foerster, 2016.

[144] Para. 82, Schrems Case 2015, op.cit., 16.

[145] WP 74, op.cit, p. 4.

ex ante review of transfers based on BCR, whereas no such approval was required for transfers based on the Safe Harbour.[146]

There might be some lack of trust from entrepreneurs side, whether the Privacy Shield is not to suffer the same fate as the Safe Harbour.[147] Will organizations recognize the Privacy Shield document as a trustworthy alternative after all that negligence on the predecessor or will they favour more dependable solution? Those who have invested in other than Safe Harbour options seem to be now in a better condition than those who chose Safe Harbour. In other words, companies at present still need to rely on using alternative arrangements.

Another issue arose after the Safe Harbour Framework was declared invalid, as controllers needed to implement an alternative data transfer mechanism that would enable them to continue transferring data lawfully. No timeline had been set for its implementation, thus many entrepreneurs were waiting in uncertainty. Binding Corporate Rules seem to be a more solid data transfer instrument, capable of being a global privacy data transfer framework compliant with the upcoming General Data Protection Regulation.

Taking that all into account, what right-minded person would really want to entrust any transfer of data to something so complicated and unworkable in practice like the Privacy Shield? If companies want to transfer data globally, as illustrated above the Privacy Shield alone is unlikely to be good enough for companies who are operating at a global level.

4.2. Limits of Standard Contractual Clauses

In many cases, companies chose SCCs as the solution to their data export, as they seem to be "the fastest and safest way to legalize the transfer to the USA" – as emphasized by Xawery Konarski, a lawyer at the law firm Traple Konarski Podrecki & Wspólnicy.[148] However, this sub-section will illustrate several disadvantages of SCCs, strengthening the argument of BCRs providing a better global solution.

[146] "What is mutual recognition?", op.cit., p. 12.
[147] Kuner 2016, op.cit., p. 14.
[148] Sławomir Wikariak, „Transfer naszych danych do USA trzeba zalegalizować", Gazeta Prawna, 22 October 2015, accessed 20 November 2015, http://prawo.gazetaprawna.pl/artykuly/900987,po-orzeczeniu-tsue-transfer-danych-do-legalizacji.html

SCCs are contracts between two legal entities which are or are not part of the same group of companies. By definition SCCs create a framework for particular data flows, while BCRs create a framework for a large number of data flows with various purposes. Therefore multinational companies gain more flexibility with BCRs, than with SCCs, given that using SCCs result in massive paperwork.

It is worth noting that, comparing to BCRs, EU SCCs may require a large number of contracts to be produced, may lead to lengthy negotiations and burdensome administration, while BCRs constitute only one code of conduct for the entire group of companies and unlike SCCs, BCRs allow for uniformisation of the personal data protection policy within a group of companies.

In addition, SCCs may need regular renewals and amendments whenever the details of the data processing change, including updating notifications with or obtaining the approvals of regulators. Article 29 Working Party noticed that: "[I]t seems to be very common for transfers between members of the same group of companies to use the standard contractual clauses without adapting them to specific needs. When changes were made, they were not very substantial."[149] It shows that companies not precisely follow the regulations, because they are too troublesome. They lead to form an extensive network of subcontractors, exporters and importers, forming complicated labyrinth of SCCs to sign.

Further, SCCs are static documents, almost half of the EU Member States (e.g. Denmark and the Netherlands) require that such contracts be registered prior to the contract being relied on as a cross-border mechanism.[150] Many countries within the EU currently require that a company that enters into a Model Contract take an additional step of notifying the Data Protection Authority of the existence of the agreement. As a general rule, organizations who use them cannot even change them unless they seek the prior approval of the DPA of the country of origin.[151] From a company perspective it is not beneficial to seek approvals all the time. For most corporations information does not flow uncomplicated via stable paths, but moves along multiple courses. Moreover, The SCCs oblige the data exporter warrants and

[149] Commission of the European Communities, "Commission Staff Working Document on the implementation of the Commission decision on standard contractual clauses for the transfer of personal data to third countries (2001/497/EC and 2002/16/EC)", 20 January 2006, accessed 2 December 2016, http://ec.europa.eu/justice/data-protection/international-transfers/files/sec_2006_95_en.pdf p. 5
[150] Wugmeister, Retzer, Rich 2007, op.cit., p. 2.
[151] Model Clauses 2010/87/EU

undertakes that he has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations,[152] so different affiliates has to check on each others, BCRs do not have such condition.

Standard Contractual Clauses by covering a defined set of transfers make the concept completely unworkable for multiple and evolving transfers and, once the business reaches any sort of global scale, regularly signing rapidly changing numerous Model Clauses becomes very unattractive.

The basic ground for international transfers is an adequacy assessment, but for many reasons this solution is not quite businesslike. In most cases adequacy cannot be used and that is where the problem begins. Different methods to transfer data might cause confusion among entrepreneurs. They have to make a decision which one to choose and which one could be the most suitable and efficient. Because of the invalidation of the Privacy Shield, data controllers had to change to other mechanisms for their international data transfers. It is doubtful they will opt for the Privacy Shield, which is assessed as being lengthy and difficult to interpret. Moreover Privacy Shield is distrusted of European customers and regulators, who relied on Safe Harbour, especially in the field of retention periods and onward transfers which are insufficiently framed, especially regarding their scope, the limitation of their purpose.

SCCs seem to be static documents which lead to lengthy negotiation and regular revisions. They are not suited to large amounts of different kinds of data transfers and are thus unsuitable on the market. In comparison to BCRs they represent reliability, in the near future legally recognized by the regulation, and flexibility, as BCRs are adjustable to the market's needs and technological changes.

[152] Comission 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), annex, set II, I.b) http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1401799828216&uri=CELEX:32004D0915

5. The road to becoming global

Countries show a diversity of approaches to transborder data flow regulation. For years companies have relied on other data transfer mechanisms such as EU SCCs[153] and the US-EU Safe Harbour framework.[154] However, it appears that these mechanisms have certain limitations and that they cannot always efficiently cover the needs of complex company groups.

There is a range of choice between approaches based on geography (depending on the "adequacy" of data protection in foreign jurisdictions) and those that are more organisationally-based (such as under the accountability principle). In a globalised world of digital data being sent in a blink of an eye, geographically-based regulation matters less in a business and technological sense than it used to.[155]

Some non-European countries have the negative impression that the Europeans have been trying to force a particular, and narrow, approach to privacy protection on the rest of the world through the application of the transborder data flow provisions in the Directive. In this chapter firstly I want to present the influence of the EU legal system concerning data transfer and privacy on non-EU countries. Further I will present new technologies requiring more flexible solutions of international data transferring and recently born cooperation between BCRs and Cross Border Privacy Rules (CBPRs) regarding global data transfers. Separately, these data transfer instruments have already been very influential and will remain even stronger when used together.

5.1. Brussels effect

Professor Graham Greenleaf to show influence of European Data Protection Law on the rest of the world demonstrated "European" elements in the national laws of countries outside EU and correlation between them. In some cases, national laws

[153] European Commission, "Model Contracts for the transfer of personal data to third countries", accessed 20 June 2016, http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm
[154] Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7-47 (EC), (Safe Harbour), accessed 16 June 2016, http://export.gov/safeharbor/
[155] Kuner 2010, op,cit., p. 1.

are more strict than the European requirements. For example, South Korea requires consent for all data exports, with no automatic right to export data to 'adequate' jurisdictions. Korea also requires consent (i.e. 'opt in') for any direct marketing uses of personal data.[156]

We cannot not notice that outside Europe, something reasonably described as "European standard" data privacy laws is becoming the norm. Scholars believe, among others Professor Greenleaf, that the EU Directive has the most significant overall influence on the content of data privacy laws outside Europe. The influence is gradually strengthening, partly because of the desire of non-European countries to have their laws recognized as "adequate", but also because of Non-Europeans aspiration that should be recognized as providing the highest international standard of privacy protection.[157]

The influence of the European regulation is also pointed out by a Canadian Report about precisely the question of extraterritoriality in the age of Globalization[158]: „in some cases, measures are designed to have extraterritorial reach by influencing the actions of other Nations. For example, the European Data Protection Directive specifically provides that EU member states must legislate so that there could be no trans-border movement of data for processing abroad unless the target country had enacted legislation establishing substantially equivalent data protection norms. Although such legislation would have no overt extraterritorial reach, the threat of loss of trade as a result of the Data Protection Directive was a strong motivating factor for the Canadian Government's decision to enact the Personal Information Protection and Electronic Documents Act."[159]

The USA has many privacy laws and some effective enforcement, but no comprehensive privacy law in the private sector, nor much prospect of one. It is not the case that the USA does not have any standards for private sector data privacy,

---

[156] Graham Greenleaf, "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108", International Data Privacy Law, 2012, accessed 7 August 2016, http://www.coe.int/t/dghl/standardsetting/DataProtection/Global_standard/GG_European_standards2010.pdf

[157] Greenleaf 2016, Ibidem.

[158] Steve Coughlan, Robert J. Currie, Hugh M. Kindred, Teresa Scassa, "Global reach, local grasp: constructing extraterritorial jurisdiction in the Age of Globalization", Dalhousie Law School, 23 June 2006, accessed 19 June 2016, https://dalspace.library.dal.ca/xmlui/bitstream/handle/10222/10268/Coughlan_Currie%20et%20al.%20Extraterritoriality%20EN.pdf?sequence=1&isAllowed=y

[159] Yves Poullet, "Transborder data flows and extraterritoriality: The European position", 21 March 2007.

but they must be interpreted from many scattered pieces of legislation. Fundamental differences in US and European contexts have led to very different data privacy norms. Americans believe in self-regulation[160] of the marketplace and privacy is seen as a transferable good subject to the market. In contrast, the European approach considers privacy to be inalienable, a fundamental human right.[161]

It is possible that the US approach to privacy will change. A Federal Trade Commission survey reveals that between 97 and 99% of all websites collect personal identifying information from and about consumers.[162] The Snowden scandal strain the trust of customers and the way to build it up is protecting privacy. Pew Research Center's surveys[163] show that Americans now are more worried about the security of their personal data and are more aware that larger volumes of data are being collected about them. Those views have intensified in recent years, especially after big data breaches at companies such as Target[164], eBay[165] and federal employee personnel files[166]. But for now American business firms' have expressed objection to being "subject" to European law and there is concern among both businesses and the Administration about European law becoming the de facto standard for data privacy in the U.S.[167]

---

[160] Joel R. Reidenberg, Thomas H. Davenport, "Should the U.S. Adopt European – Style Data – Privacy Protections?", The Wall Street Journal, 10 March 2013, accessed 2 December 2016, http://www.wsj.com/articles/SB10001424127887324338604578328393797127094

[161][161] Phil Lee, "How do EU and US privacy regimes compare?", Field Fisher, 5 March 2014, accessed 2 December 2016, http://privacylawblog.fieldfisher.com/2014/how-do-eu-and-us-privacy-regimes-compare/

[162] The FTC concludes that "Most of the sites surveyed, therefore, are capable of creating personal profiles
of online consumers by tying any demographic, interest, purchasing behavior, or surfing behavior information they collect to personal identifying information" (Bureau of Consumer Protection 2000, p.10).

[163] Lee Rainie, Shiva Maniam, "Americans feel the tensions between privacy and security concerns", Pew Research Center, 19 February 2016, accessed 2 December 2016, http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/

[164] Greg Wallace, Julianne Pepitone, James O'Toole, Chris Isidore, Jose Pagliery, "Target" 40 million credit cards compromised", CNN, 19 December 2013, accessed 2 December 2016, http://money.cnn.com/2013/12/18/news/companies/target-credit-card/

[165] Andrea Peterson, "eBay asks 145 million users to change passwords after data breach", The Washington Post, 21 May 2014, accessed 2 December 2016, https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/?utm_term=.6b4d1ee1cf90

[166][166] Meredith Somers, "OPM notifies 3.7 million cyber attack victims about data protection services", Federal News Radio, 28 October 2015, accessed 2 December 2016, http://federalnewsradio.com/cybersecurity/2015/10/opm-notifies-3-7-million-cyber-attack-victims-about-data-protection-services/

[167] Kobrin 2002, op.cit., p. 32.

Bradford has referred to the so-called "Brussels effect", in which the EU is engaged in unilateral regulation of global markets,[168] which can be seen in the influence that EU data protection law has had on the development of data protection legislation in many third countries.[169] The Schrems judgment can be seen as an indirect example of the Brussels effect, since it seems to be based on the rationale that withholding recognition of data transfers to the US may result in the US adopting standards closer to the European model.[170]

5.2. Trusted data processing area

More and more data moves online, is stored in the cloud, and gets transmitted all around the world. According to the ACI Information Group,[171] we created five exabytes of content on a daily basis in 2013. That is the same amount of data that was created from the beginning of the world until 2003. By 2020, the International Data Corporation (IDC)[172] estimates the size of theworld's digital data will be nearly forty zetabytes. At the same time governments become ever more determined to introduce territorial restrictions limiting the movement of data. The law of the protection of personal data is extremely territorial – everything refers to the level of countries.

Article 3 of the GDPR states that the Regulation applies to the processing of personal data of data subjects residing in the EU, even if the controller or processor is not established in the EU, provided that the processing relates to the offering of goods or services to the data subjects, or the monitoring of data subjects' behaviour. This basically means that any company that markets goods or services to EU residents may be seen as subject to the GDPR, regardless of whether the company is located or uses equipment in the EU or not.

---

[168] Anu Bradford, "The Brussels Effect", 107 Northwestern University Law Review 1, 2013.
[169] Kuner 2016 op.cit., p.14.
[170] Kuner 2016, Ibidem.
[171] Susan Gunelius, "The data explosion in 2014 minute by minute – infographic", ACI, 12 July 2014, accessed 12 July 2016, http://aci.info/2014/07/12/the-data-explosion-in-2014-minute-by-minute-infographic/
[172] "The historical growth of data: why we need a faster transfer solution for large data sets", SIGNIANT, accessed 12 July 2016, http://www.signiant.com/articles/file-transfer/the-historical-growth-of-data-why-we-need-a-faster-transfer-solution-for-large-data-sets/

Under Article 3(2), data controllers not established in the EU may be subject to EU law when their processing activities are related to "the offering of goods or services" to data subjects residing in the EU, or to the monitoring of the behaviour of EU residents; the abandonment of the "use of equipment in the EU" test contained in Article 4(1)(c) of Directive 95/46 as the criterion for jurisdiction over non-EU data controllers is welcome. The effect of these changes is to bring more non EU-based companies offering services over the Internet within the reach of EU law. The territorial scope of EU data protection law with regard to processing by non-EU data controllers is explicitly limited to individuals "residing" in the EU, but it is not explained whether such residence must be permanent or may only be temporary, and what protection, if any, would be enjoyed by individuals who may have a residence both inside and outside the EU. [173] Indeed, the emphasis in this and other articles (e.g., Articles 41(2)(a) and 41(5)) on residence in the EU is surprising, given that the Proposed Regulation states elsewhere that its protections should apply regardless of nationality or residence.[174]

The GDPR applies when an entrepreneur is planning services to be offered in at least one Member State. The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data.[175] This provision essentially makes the GDPR a worldwide law. In contrast, the Directive was not as expansive in its geographic reach.

As the global regulation is not achievable yet, BCRs may play a role here. If it is possible to make a choice of law and forum in BCRs, it would be possible to have BCRs supervised and enforced by one "lead" DPA only, preferably the authority of the place of establishment of the headquarters of such multinational. BCRs may thus function as a private regulatory response to the inherent limitations of rules on applicable law and jurisdiction.[176]

A reasonable solution would be to treat corporations that have introduced such Binding Corporate Rules concerning the processing of personal data as a kind of counterpart countries. So treating, for example, the provider of the cloud, as a trusted

[173] Kuner 2012, op.cit., 18.
[174] Recitals 2 and 14, GDPR, op.cit., p. 16.
[175] Recital (12), Ibidem.
[176] Moerel 2011, op.cit., p. 10.

data processing area. This is a solution that is possible and discussed in opinions of the Article 29 Working Party.[177]

"The underlying principle of territoriality whereby a physical connection is required to a territory is no longer suited to be applied in the current day reality"[178] or as phrased by Stephen J. Kobrin, "Extraterritorial reach not only becomes the norm, the concept itself looses meaning as the distinction between domestic and international affairs blurs to the point where it is no longer meaningful and territoriality becomes problematic as the organizing principle underlying the international political system."[179]

BCRs may also be a response to the new technical challenges related to the protection of personal data, among others processed in the so-called computing clouds. The term "cloud computing" has entered common usage and has been used to describe a wide range of services offered over the Internet.[180] According to the European Commission cloud computing "means accessing computer capacity and programming facilities online or "in the cloud". Customers are spared the expense of purchasing, installing and maintaining hardware and software locally."[181]

In this context rules for Processors are gaining importance. In view of the widespread practice of locating servers in different parts of the world and the free and unfettered flow of entrusted data between locations, ensuring a proper and uniform level of security is necessary.

It If the provider of the cloud created Binding Corporate Rules for himself, then it stops to be relevant where the data centre is, because when there is applied the principle of the protection of personal data sufficient for the European Union, then such a transfer will be able to take place. Thus, the solution of the legal and organizational nature solves the technical problem.

---

[177] Marcin Maj, an Interview with Polish DPA, "GIODO: Przetwarzanie danych osobowych w chmurach jest dopuszczalne, ale..." Dziennik Internautów, 24 May 2011, accessed 18 September 2015, http://di.com.pl/giodo-przetwarzanie-danych-osobowych-w-chmurach-jest-dopuszczalne-ale-38127

[178] Moerel 2011, op. cit., p. 10.

[179] Kobrin, 2002, op.cit., p. 32.

[180] Renee Berry, Mathew Reisman, "Policy challenges of cross-border cloud computing", Journal of International Commerce and Economics, May 2012.

[181] European Commission, Cloud Computing Contracts, accessed 7 August 2016, http://ec.europa.eu/justice/contract/cloud-computing/index_en.htm

As an exception to the territory-based system of the EU, the EU introduced the BCR regime that reflects the organisational (i.e. the accountability) approach to regulate inter-company data transfers. As soon as a multinational with BCRs transfers data outside the company group to a third party in a non-adequate country, the regular EU data transfer rules have to be complied with.[182]

The accountability approach "ensures that the original collector of the personal information remains accountable for compliance with the original privacy framework that applied when and where the data was collected, regardless of the other organizations or countries to which the personal data travels subsequently".[183] This approach seems to provide that the protections of the law of the place from which the data were transferred "attach to" the data and continue to be applicable as they are transferred abroad.[184]

In the past, complaints have been made about the aggressive jurisdictional scope of data protection laws (such as the EU Data Protection Directive) requiring that their standards be applied abroad. To the extent that requirements for transferring personal data abroad based on the accountability principle become more widespread,[185] there is the potential for increased international conflict about the extraterritorial application of data protection law. In addition, if the state can ensure that its law applies beyond its borders, in accordance with international law it cannot directly pursue their rights without the consent of the participating state.[186]

The main reason why accountability approach is better than the territorial approach is that even if data are transferred to an "adequate country", enforcement of data protection violations may prove problematic even there. Further, in practice the EU approach requires a full adequacy assessment of the data protection laws of each country and proves insufficiently productive in achieving global data protection coverage. Key trade partners of the EU like China, Japan, Brazil, India and the US are not considered as providing adequate protection, which inevitably leads to non-compliance in practice accountability approach to data transfers seems to be more flexible in tailoring to the transfers at hand and even facilitates some form of central

[182] Moerel 2011, op.cit., p. 10.
[183] Malcolm Crompton, Christine Cowper, Christopher Jefferis, "The Australian Dodo Case: An insight for Data Protection Regulation'", 26 January 2009, BNA Privacy & Security Law Report 180.
[184] Kuner 2010, op.cit., p. 1.
[185] Kuner 2009, op.cit., p. 3.
[186] Kuner 2009, Ibidem.

enforcement against the data exporter who is often in the country where the data subject is domiciled. [187]

In the Asia-Pacific region, the twenty-one member economies of the Asia-Pacific Economic Cooperation (APEC)[188] group have agreed on a set of nine privacy principles that members may voluntarily implement in their national economies. The APEC. The EU and APEC approaches to regulation of international data transfers are often seen as diametrically opposed. But they are similar in at least one important respect, since both approaches realize the objective of protecting their citizens, residents, and companies from the misuse of their data when they are transferred abroad by having their law 'attach' to the data. As a result the protections of the place from which the data were transferred continue to be applied.

On 27 February 2014, the Article 29 Working Party adopted an opinion on a practical referential mapping the requirements of BCRs and CBPRs.[189] This document was also endorsed by APEC Member Economies on 27 and 28 February 2014.

The document, prepared jointly by APEC officials and the EU Art. 29 Data Protection Working Party, shows that there is considerable overlap between the two systems. Companies cannot achieve mutual recognition of both systems just by taking on-board the suggestions in this document, but it could serve as a basis for double certification.[190] The document serves as an informal pragmatic checklist for organizations, and facilitates the design and adoption of personal data protection policies compliant with each of the systems.

The EU BCR system and the APEC CBPR system are based on a similar approach, namely codes of conduct for international transfers developed by companies and approved a priori by EU Data Protection Authorities (for BCRs) or by

---

[187] Moerel 2011, op.cit., p. 10.

[188] Asia-Pacific Economic Cooperation, APEC Privacy Framework, 2005, accessed 25 June 2016, http://publications.apec.org/publication-detail.php?pub_id=390

[189]Article 29 Data Protection Working Party, "Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents", WP 212, 27 February 2014, accessed 20 April 2016, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf

[190] "EU DPAs and APEC take a step towards mutual recognition of BCR/CBPR", Privacy Law & Business, 10 March 2014, accessed 7 August 2016, https://www.privacylaws.com/Publications/enews/International-E-news/Dates/2014/3/EU-DPAs-and-APEC-take-a-step-towards-mutual-recognition-of-BCRCBPR/

APEC recognized accountability agents (for CBPRs). The WP29 analysed the CBPR system in order to identify their similarities and differences with the BCR system.

However, the Working Party also emphasizes that data protection policies of applicant companies operating in both regions must be approved separately by the relevant institutions in accordance with the applicable approval procedures for each system. The Working Party notes that significant differences exist between the requirements generally imposed by EU DPAs for BCR approval (in particular those deriving from EU data protection laws) and the CBPR program requirements. There also are differences between the respective objectives, scopes and review processes of the BCR and CBPR systems. Therefore, certain BCR and CBPR requirements are not fully compatible.[191]

In terms of scope of the two systems, the Working Party clarifies that CBPR certification is limited to organizations certified within a CBPR-participating Economy, and the scope of a particular organization's CBPR certification will be limited to the entities, subsidiaries and affiliates identified in its application for CBPR certification. Similarly, the scope of a particular organization's BCRs will be limited to those entities, subsidiaries and affiliates identified in its application for BCR approval. An organization that wishes to transfer personal data from EU Member States to recipients located in non-EU countries may submit an application to the relevant national DPA in the EU for approval of its BCR.

The Article 29 Working Party welcomes the result of this joint work with APEC Member Economies, which is the first one with the APEC, and is a great example of cooperation. Indeed, "this practical tool sets out global solutions for multi-national organisations wishing to develop personal data protection and privacy policies compliant with both BCR and CBPR systems, and thereby obtain both certifications."[192]

Hewlett-Packard (HP) is the first to win certification of both BCRs and CBPRs. HP VP and Chief Privacy Officer Scott Taylor said: "if you had your CBPR certification, it probably satisfies a third of the BCR. In reverse, the goal is that if you have completed your substantiation from BCR, it should really satisfy 90-plus percent

[191] Article 29 Data Protection Working Party, "Opinion 02/214 on a referential requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents", 27 February 2014, accessed 2 December 2016, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf

[192] Ibidem.

of the CBPR. Because we started in Europe, it really made the CBPR process relatively simple. Either way, there's a benefit to organizations no matter where they start. The good news is there will be a body of work you won't lose, and you can leverage it in achieving the other."[193]

However, regulators and legislators are understandably most concerned with protecting the data of their own citizens and residents rather than the data of persons in another country. The accountability principle will have to co-exist with the territoriality principle with respect to the processing of personal data on the Internet, since states show no signs of allowing data controllers and data processors to use accountability (or some other manifestation of the personality principle) to escape from the obligation to comply with the national law applicable to them.[194]

This approach also seems to provide expansive room to keep the benefits of an adequacy approach (which stimulates third countries to adopt adequate data protection laws) while also providing for more flexible organisational measures, which may mitigate the downsides of the adequacy system.[195] But reliance by both the EU and APEC on the adequacy principle is perhaps an encouraging sign that the two approaches have more in common than is often assumed, and that accommodation between their approaches to international data transfers may someday be possible.[196]

Daniel Solove confirms that it is highly unlikely that any time soon there will be enacted a global treaty or binding legal instrument. However, at the same time, there has been a growing need for greater coordination between the different national and regional approaches to data privacy. We cannot expect that countries will give up their own national privacy frameworks, that much can be achieved through international cooperation, private-sector mechanisms, and technological solutions.[197]

In a world where nearly everything seems to be connected through the boundless Internet and global companies, we still have laws requiring that data should be held within specific territories or regions. BCRs are free of this burden.

[193] Carson 2014, op.cit., p. 25.
[194] Kuner 2009, op.cit., p. 4.
[195] Moerel 2011, op.cit., p. 10.
[196] Kuner 2009, op.cit., p. 4.
[197] Daniel Solove, „The future of global privacy: Conflict or harmony?" LinkedIn, 21 April 2014, accessed 10 April 2016, https://www.linkedin.com/pulse/20140421120856-2259773-the-future-of-global-privacy-conflict-or-harmony?_mSplash=1&published=t

Entrepreneurs, for example cloud providers, can create a trusted area to process data.

What supports the BCRs as a global data protection instrument is the so called “Brussels effect” – European data protection solutions adopted by countries all over the world, which makes instruments like BCRs more familiar and local. The biggest dissimilarity to the EU seems to appear in the USA, although latest events show that Americans are not satisfied with their current way of dealing with data; treating their data as a product.

An interesting development is how companies are trying to deal with the lack of at global data transfer instrument and trying to fill this gap by connecting possibilities offered by both BCRs and CBPRs. The Article 29 Working Party noticed the need to fill this gap and adopted an opinion on a practical referential, mapping the requirements of BCRs and CBPRs. This leads to forgetting about national borders and creating a trusted area within the companies, which is more in line with practical reality when it comes to modern data flows.

For the BCRs potential to become a global instrument it creates a few advantages – first of all the leadership of the Article 29 Working Party in involving BCRs and APEC cooperation. Second of all fulfilling BCRs with this mutual effort gives another big advantage which is meeting the requirements of other regional data transfer solutions. Even though it is not fully compatible yet, but the first companies that win both certifications seem to be satisfied and also emphasise that fulfilling BCRs requirements make it easier to acquire other regional data transfer tools.

In the 21st Century it is not enough to place inspectors at our ports of entry to monitor the flow of data, goods and people. Border security can no longer be just a coastline or a line on the ground between two nations. We must also have a “virtual border” that operates far beyond the land of border.[198]

[198] Poullet 2007, op.cit., p. 41.

6. Conclusions

In the context of the knowledge and data acquired during the research, it occurs that there is not much chance to reach in the near future a global consensus on cross-border data protection. Moreover countries are losing control over data transfers, as national borders cannot stop the flow anymore. At present, if personal data can be transmitted instantaneously to multiple locations anyplace in the world, its location becomes ambiguous.[199] If that is the situation, regulations which attempt to protect the data privacy of Europeans, or anyone else for that matter, must also ignore "location" as a constraint if they are to be effective.[200]

The Schrems case illustrates that any distinction between extraterritorial and territorial jurisdiction has become meaningless in the context of regulation of international data transfers. The judgment provided the opportunity for the EU to revise its approach to reaching adequacy determinations, and to consider what mechanisms could actually lead to data protection in the real world of international data transfers. By determining the standard that third countries must meet to be declared "adequate" in the eyes of the EU, the CJEU has effectively set the global data protection bar at a high level.[201] Many third countries will revise their data protection law and practice in an attempt to meet this standard. On the other hand, adequacy norms might be too troublesome to implement by the whole world, but flexible BCRs seem like a reasonable solution.

The establishment of BCRs was caused by the need of corporations to make data flows less formalised, more flexible and to make one standard, no matter where the corporate group is situated. It seems that as more and more data moves online, is stored in the cloud, and gets transmitted all around the world the more governments become determined to introduce territorial restrictions limiting the movement of data.

The BCRs structure shows its big advantage, i.e. the flexible nature that can easily be adjusted to the market demands. The Article 29 Working Party issued papers based on the current situation and market demands. The application procedure is getting easier and faster thanks to the co-operation procedure and

[199] Colin Bennett, "Convergence revisited: toward a global policy for the protection of personal data?" Technology and Privacy: The New Landscapte, Cambridge: The MIT Press, 1997.
[200] Kobrin 2002, op.cit., p. 31.
[201] Kuner 2016, op.cit., p. 21.

mutual recognition, which will soon be replaced by the new consistency mechanism formalizing the cooperation of DPAs. The BCRs regulation and upcoming changes demonstrate that the EU wants to keep its strict data protection policy, however noticing global market struggles and needs tries to make it more adjustable.

Other possible advantages confirm that BCRs could become a global instrument. By using BCRs as an international data transfer instrument entrepreneurs, for example cloud providers, can create a trusted area to process data and not bother about the national borders. Harmonisation of the EU law, a high standard of data protection, tailor-made solutions, the possibility of regulating companies' compliance issues, gradually simplifying the procedure to establish BCRs indicates that the EU really wishes to expand this solution worldwide.

Disadvantages are being improved, the myth of the complicated procedure is still functioning but thanks to taken steps of informing and issuing opinions by the Article 29 Working Party this is changing. Moreover the liability regime is no more severe than in other data transfer tools that meet EU requirements.

The analysis of alternatives for BCRs shows that either they contain too many rigid and unworkable provisions that any commercial organisation would be very reluctant to accept them – and, once the business reaches any sort of global scale of data flows, regular signing rapidly changing numerous model clauses becomes very unattractive; or remains a solution only for transfers of data from Europe and Switzerland to the US and the substitute (Safe Harbour Principles). According to the Article 29 Working Party's latest opinion, the current version of the Privacy Shield will not provide adequate protection for personal data transferred to the US. It seems unrealistic that EU companies will suddenly pull the plug and stop transferring their data to the US. There is also the added complication of the newly approved EU General Data Protection Regulation. Therefore, if the goal is to achieve compliance with the GDPR, the Privacy Shield alone will not be sufficient. For companies who are keen to use EU data protection law as a global compliance standard within their organisation, Binding Corporate Rules may be a better option as these, which already exist cover many of the GDPR requirements

One cannot force countries to implement a voluntary agreement, although some kind of compulsion appears when companies want to arrange businesses with the EU. What supports the BCRs as a global data protection instrument is the so called "Brussels effect" – meaning that European data protection solutions are being

adopted by countries all over the world, which makes instruments like BCRs more familiar and local.

BCRs may be a convenient, already existing, solution to globally coordinate corporate standards of processing data. BCRs are gaining in importance, thanks to a new regulation the number of those documents will continue to increase. A lot of companies chose BCRs as a permanent solution for international data transfers and this trend is expected to stay. Currently, because of easier procedure and better cooperation among EU DPAs, BCRs can be used not only by large corporations, but also by many medium-sized companies. The BCRs approval process runs more smoothly and faster. BCRs for data processors have opened up the instrument for a large number of new companies to benefit, including the various service providers and members of the outsourcing industry.

The EU claims the right to judge the appropriateness of the data protection regulation of other countries and it has, as shown in the thesis, actual influence on the rest of the world's international corporations. If they wish to operate in Europe, they must adapt to European standards, which is easier by adopting BCRs than any other tool.

Companies understand that BCRs are a great way to move away from outdated and bureaucratic practices. They help strengthen accountability and promote compliance. Cooperation with the other compliance instruments is increasing. Interesting occurrence is how companies are trying to deal with the lack of a global instrument and are filling the gap by connecting possibilities offered by both BCRs and CBPRs. The Article 29 Working Party and its APEC counterparts are working together closely to provide practical tools to multinational organizations that do business both in Europe and the Asia-Pacific region and look for global solutions for their data transfers.

If an organisation had its CBPR certification, it satisfies a third of the BCRs. In reverse, completing substantiation of BCRs satisfies more than 90 percent of the CBPRs. The Article 29 Working Party among others stated that, if the rules comply with Directive 95/46/EC, as well as with the national data protection legislation, Binding Corporate Rules might become for corporate groups a truly global privacy policy.[202]

[202] WP 74, op.cit., p. 4.

Lastly, companies with BCRs have a competitive advantage. As data protection becomes increasingly important in today's data-driven business world, BCRs can help strengthen customer trust and inspire favourable perceptions of a company. Therefore, by incorporating a comprehensive and effective data protection program, companies with BCRs have a competitive advantage in the global marketplace.

However, even having Binding Corporate Rules approved by DPAs cannot restrain data access by foreign intelligence services. At a legal level, such third country agencies are not constrained by EU law, and at a practical level their capabilities are not in any way hindered by such procedural mechanisms. Kuner claims that EU data protection law is partially based on legal fictions.[203] There is uncertainty that the points upon which the Court relied to invalidate the Safe Harbour can be applied to other legal mechanisms for data transfers under the Directive as well. The judgment therefore reveals the internal contradictions in the regulation of the transmission of data in accordance with EU law, and also shows how one-sided application of EU law cannot in practice provide effective protection. The biggest conflict arose between the US and the EU. The EU wants the US to adopt a data protection framework and change their law. The US wants the EU to facilitate the transfer of personal data abroad to further economic development. At the moment it is unrealistic to imagine that there could be a single, overarching "solution". Nevertheless, the influence of European data protection law is quite a strong premise for BCRs to be accepted globally.

In the absence of trust to the Privacy Shield, inefficient SCCs to the amount of data transfers and uncertainty to the laws – BCRs for years are gaining trust and new participants. For any large multinational organisation, there really remains only one solution: Binding Corporate Rules as a more solid data transfer solution but also as a global privacy compliance framework that will enable them to better comply with the upcoming data protection regulation. The BCR is really the glue, putting together all the different modules necessary for a company ensuring compatibility of data protection with business activities, the ethics and law.

[203] Kuner 2016, op.cit., p. 21.

Bibliography

(n.d.). Retrieved May 15, 2016, from Der Hessische Datenschutzbeauftragte: https://www.datenschutz.hessen.de/ft-europa.htm#entry4521

(n.d.). Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf

"EU DPAs and APEC take a step towards mutual recognition of BCR/CBPR". (2014, March 10). Retrieved August 7, 2016, from Privacy Law & Business: https://www.privacylaws.com/Publications/enews/International-E-news/Dates/2014/3/EU-DPAs-and-APEC-take-a-step-towards-mutual-recognition-of-BCRCBPR/

"Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries". (n.d.). Retrieved March 15, 2016, from http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

"Procedure". (n.d.). Retrieved from European Commission: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/procedure/index_en.htm

"The historical growth of data: why we need a faster transfer solution for large data sets". (n.d.). Retrieved July 12, 2016, from SIGNIANT: http://www.signiant.com/articles/file-transfer/the-historical-growth-of-data-why-we-need-a-faster-transfer-solution-for-large-data-sets/

"What is mutual recognition?". (n.d.). Retrieved April 20, 2016, from European Commission: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/mutual_recognition/index_en.htm

“Model Contracts for the transfer of personal data to third countries”. (n.d.). Retrieved June 20, 2016, from European Commission: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

“Opinion 02/214 on a referential requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents”. (2014, February 27). Retrieved December 2, 2016, from Article 29 Data Protection Working Party: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf

“Overview on Binding Corporate Rues". (n.d.). Retrieved June 19, 2016, from European Commission: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm

“Restoring trust in transatlantic data flows through strong safeguards: European EU-U.S. Privacy Shield”. (2016, February 29). Retrieved June 17, 2016, from European Commission: http://europa.eu/rapid/press-release_IP-16-433_en.htm

Andrew Shindler, Z. F. (2016, July 19). *King & Wood Mallesons*. Retrieved July 27, 2016, from http://www.kwm.com/en/uk/knowledge/insights/eu-us-privacy-shield-an-end-to-uncertainty-20160719

Article 29 - Data Protection Workin Party. (2008, June 24). Retrieved March 15, 2016, from Working Dokument setting up a framework for the structure of Binding Corporate Rules, WP 154: 2016 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp154_en.pdf

Article 29 - Data Protection Working Party. (1998, July 24). Retrieved March 15, 2016, from "Transfers of Personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive", WP 12: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf

Article 29 - Data Protection Working Party. (2003, June 3). Retrieved March 15, 2016, from Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfer" WP 74: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf

Article 29 - Data Protection Working Party. (2005, April 14). Retrieved March 15, 2016, from "Working document setting forth a cooperation procedure for issuing common opinions on adequate safeguards resulting from Binding Corproate Rules" WP 107: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp107_en.pdf

Article 29 - Data Protection Working Party. (2007, January 10). Retrieved March 16, 2016, from "Recommendation 7/2007 on the standard application for approval of Binding Corporate Rules for the transferof personal data" WP 133: ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp133_en.doc

Article 29 - Data Protection Working Party. (2008, June 24). Retrieved April 20, 2016, from "Working document setting up a table with the elements and principles to be found in Binding Corporate Rules" WP 153: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp153_en.pdf

Article 29 - Data Protection Working Party. (2008, June 24). Retrieved April 20, 2016, from "Working documetn setting up a framework for the strucuture of Binding Corporate Rules" WP 154: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp154_en.pdf

Article 29 - Data Protection Working Party. (2008, June 24). Retrieved March 15, 2016, from "Working document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules" WP 155: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp155_rev04_en.pdf

Article 29 - Data Protection Working Party. (2012, June 6). Retrieved March 15, 2016, from "Working document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 195: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf
Article 29 - Data Protection Working Party. (2012, June 6). Retrieved April 20, 2016, from "Working document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules" WP 195: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf
Article 29 Data Protection Working Party. (2014, February 27). Retrieved April 20, 2016, from "Opinion 02/2014 on a referential for requirements for Binding Corporaate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents": http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf
Article 29 Data Protection Working Party. (2016, April 13). Retrieved July 25, 2016, from "Opnion 01/2016 on the EU - US Privacy Shield draft adequacy desicion": http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf
Article 29 Data Protection Working Party. (2016, April 13). Retrieved December 2, 2016, from "Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision": http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf
Article 29 Working Party statement on the desicion of the European Commission on the EU-US Privacy Shield. (n.d.). Retrieved August 5, 2016, from http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf
Article29 - Data Protection Working Party. (2013, April 19). Retrieved April 20, 2016, from "Explanatory document on the Processor Binding Corporate Rules" WP 204: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp204_en.pdf
Asia-Pacific Economic Cooperation, APEC Privacy Framework. (2005). Retrieved June 25, 2016, from http://publications.apec.org/publication-detail.php?pub_id=390
Asia-Pasific Economic Cooperation. (n.d.). Retrieved July 27, 2016, from http://www.apec.org/about-us/about-apec.aspx
Bennett, C. (1997). "Convergence revisited: toward a global policy for the protection of personal data?". *Technology and Privacy: The New Landscapte, Cambridge: The MIT Press*
.

Biedermann, T. (2016, Februrary 15). *"The end of a safe harbour: The Schrems decision calls for stricter standards for protection of personal data transferred to the US".* Retrieved April 20, 2016, from Columbia Journal of European Law: http://cjel.law.columbia.edu/preliminary-reference/2016/the-end-of-a-safe-harbor-the-schrems-decision-calls-for-stricter-standards-for-protection-of-personal-data-transferred-to-the-us/

Blume, P. (2000). *"Transborder data flow: is there a solution in sight?".* 8 Int'l J L and Info Technology.

Boris Segalis, M. E. (2015, October 5). *"Day-after-Safe Harbor action plan: Anticipating ECJ Screms decision".* Retrieved June 20, 2016, from Data Protection Report: http://www.dataprotectionreport.com/2015/10/day-after-safe-harbor-action-plan-anticipating-ecj-schrems-decision/

Bradford, A. (2013). "The Brussels Effect". *107 Northwestern University Law Review 1* .

Carson, A. (2014, November 25). *"Hewlett-Packard first to win certification for BCRs, CBPRs".* Retrieved June 21, 2016, from The International Association of Privacy Professionals: Angelique Carson, "Hewlett-Packard first to win certification for BCRs, CBPRs", The International Association of Privacy Professionals, 25 November https://iapp.org/news/a/hewlett-packard-first-to-win-certification-for-bcrs-cbprs/

Christoph Zieger, D. A. (2015, October 26). *"German Data Protection Authorities suspend BCR approvals, question Model Clause transfers".* Retrieved May 15, 2016, from Data Protection Report: http://www.dataprotectionreport.com/2015/10/german-data-protection-authorities-suspend-bcr-approvals-question-model-clause-transfers/

Christopher Kuner, C. R. (2004, October 28). "ICC report on Binding Corporate Rules for international transfers of personal data". *International Chamber of Commerce* .

COE. (n.d.). Retrieved July 27, 2016, from https://www.coe.int/en/web/conventions/about-treaties

Colin Bennet, C. R. (2003). *"The governance of privacy: policy instruments in global perspective".* MIT Press.

(5 February 2010). *Commission Decision (EC) 2010/87/EU on standard contractual clauses for the transfer of personal data to processors.*

Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7-47 (EC), (Safe Harbour). (n.d.). Retrieved June 16, 2016, from http://export.gov/safeharbor/

Commission of the European Communities. (2006, January 20). Retrieved December 2, 2016, from "Commission Staff Working Document on the implementation of the Commission decision on standard contractual clauses for the transfer of personal data to third countries (2001/497/EC)": http://ec.europa.eu/justice/data-protection/international-transfers/files/sec_2006_95_en.pdf

Communication from the Commission to the European Parliament and the Council on the transfer of personal data from the EU to the United States of America under Directive 95/46/EC following Judgment by the Court of Justice in case C-362/14 (Schrems). (2015, November 6). Retrieved May 15, 2016, from http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf

Cross Border Privacy Rules System. (n.d.). Retrieved July 27, 2016, from http://www.cbprs.org/

David Bender, L. P. (2006). *"Binding corporate rules for cross-border data transfer".* Rutgers Journal of law and Urban Policy.

Directive 95/46/EC 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. (1995, October 24). Retrieved November 29, 2015, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

European Commission. (n.d.). Retrieved from Opinions and Recommendations: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

European Commission. (n.d.). Retrieved August 7, 2016, from Cloud Computing Contracts: , http://ec.europa.eu/justice/contract/cloud-computing/index_en.htm

European Commission. (n.d.). Retrieved July 27, 2016, from Opinions and Recommendations: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

European Commission Press Release. (2016, July 12). Retrieved December 2, 2016, from "European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows": http://europa.eu/rapid/press-release_IP-16-2461_en.htm

European Parliament resolution of 12 March 2014 on the U.S. NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs. (2014, March 12). Retrieved June 22, 2016, from http://bit.ly/1LwfNve

Goldring, J. (1998). *Globalisation, national sovereignty and the harmonisation of laws.* Uniform Law Review.

Goode, R. (1991). *"Reflections on the harmonisation of Commercial Law".* Uniform Law Review.

Greenleaf, G. (2012). *"The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108".* Retrieved August 7, 2016, from Internationa Data Privacy Law: http://www.coe.int/t/dghl/standardsetting/DataProtection/Global_standard/GG_European_standards2010.pdf

Greg Wallace, J. P. (2013, December 19). *"Target: 40 million credit cards compromised".* Retrieved December 2, 2016, from CNN: http://money.cnn.com/2013/12/18/news/companies/target-credit-card/

Gunelius, S. (2014, July 12). *"The data explosion in 2014 minute by minute - infographic".* Retrieved July 12, 2016, from ACI: http://aci.info/2014/07/12/the-data-explosion-in-2014-minute-by-minute-infographic/

Joel R. Reidenberg, T. H. (2013, March 10). *"Should the U.S. Adopt European - Style Data - Privacy Protections?".* Retrieved December 2, 2016, from The Wall Street Journall: http://www.wsj.com/articles/SB10001424127887324338604578328393797127094

Kobrin, S. J. (2002, November). "The Trans-Atlantic data privacy dispute, territorial jurisdiction and global governance". *The Wharton School* .

Kong, L. (2010, March 23). *"Data protection and transborder data flow in the European and global context".* Retrieved March 23, 2016, from European Journal of International law: https://ejil.oxfordjournals.org/content/21/2/441.full

Kuner, C. (2016). *"Reality and illusion in EU data transfer regulation post Schrems" .* University of Cambridge.

Kuner, C. (28, January 2013). *"The global data privacy power struggle"*. Retrieved June 19, 2016, from OUPblog: http://blog.oup.com/2013/01/global-data-privacy-power-struggle/

Kuner, C. (2009, January 24). "An international legal framework for data protection: Issues and prospects". *Computer Law & Security Review* .

Kuner, C. (2010, October). "Regulation of transborder data flows under data protection and privacy law: past, present, and future". *TILT* .

Kuner, C. (2012, February 6). "the European Commission's proposed Data Protection Regulation: A Copernican revolution in European Data Protection Law". *Bloomberg* .

Kuner, C. (2009). „Global data transfer on the Internet: Lessons from the Ancient World". *SSM* .

Lee Rainie, S. M. (2016, February 19). *"Americans feel the tensions between privacy and security concerns".* Retrieved December 2, 2016, from Pew Research Center: http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/

Lee, P. (2014, March 5). *"How do EU and US privacy regimes compare?".* Retrieved December 2, 2016, from Field Fisher: http://privacylawblog.fieldfisher.com/2014/how-do-eu-and-us-privacy-regimes-compare/

Maj, M. (2011, May 24). *"GIODO: Przetwarzanie danych osobowych w chmurach jest dopuszczalne, ale...".* Retrieved September 18, 2015, from Dziennik Internautów: http://di.com.pl/giodo-przetwarzanie-danych-osobowych-w-chmurach-jest-dopuszczalne-ale-38127

Malcolm Crompton, C. C. (2009, January 26). “The Australian Dodo Case: An insight for Data Protection Regulation". *BNA Privacy & Security Law Report 180* .
Mark Young, M. K. (2016, February 18). *“EU DPA enforcement guidance post – Schrems”.* Retrieved May 15, 2016, from Inside Privacy: https://www.insideprivacy.com/international/european-union/eu-dpa-enforcement-guidance-post-schrems/
Maximilian Schrems v. Data Protection Commissioner, C - 362/14 (October 6, 2015).
Miriam Wugmeister, K. R. (2007). *"Global solution for cross-border data transfers: making the case for Corporate Privacy Rules".* Morrison & Foerster LLP.
Moerel, L. (2016). "An assessment of the impact of the Schrems judgement on the data transfer grounds available under EU data protection law for data transfers to the U.S.”. *Morrison, Foerster* .
Moerel, L. (2011). *"Binding corporate rules: Fixing the regulatory patchwork of data protection".* Tilburg University.
Munur, M. (2011, December 23). *“Binding Corporate Rules and the proposed EU Data Protection Regulation”.* Retrieved June 23, 2016, from Tsibouris Privacy + Technology Blog: http://blog.tsibouris.com/2011/12/binding-corporate-rules-and-proposed-eu.html
Myriam Gufflet, A. P. (2015, February 3). *“Why do we need Binding Corporate Rules? A look to the future".* Retrieved June 20, 2016, from Bloomberg BNA: https://www.wsgr.com/eudataregulation/pdf/pateraki-0315.pdf
OECD. (n.d.). Retrieved July 27, 2016, from https://www.oecd.org/about/
OECD. (2006). *"Report on the cross-border enforcement of Privacy Laws".* Retrieved July 12, 2016, from www.oecd.org/dataoecd/17/43/37558845.pdf.
Opiela, A. P. (n.d.). *"Wiążące reguły korporacyjne (BCR) jako element efektywnej polityki compliance".* Retrieved August 7, 2016, from Domański Zakrzewski Palinka: https://www.dzp.pl/files/Publikacje/Prawne_aspekty_us%C5%82ug_chmurowych_2015.pdf
Parker, C. (2007). *"Meta-regulation: Legal accountability for corporate social responsibility".* Cambridge University Press.
Pateraki, A. (2016, March). *“EU regulation Binding Corporate Rules under the GDPR – what will change?”.* Retrieved June 18, 2016, from Bloomerg BNA: 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
Paul Craig, G. d. (2011). *“EU Law: Text, Cases, and Materials”.* Oxford University Press.
Peterson, A. (2014, May 21). *"eBay asks 145 million users to change passwords after data breach”.* Retrieved December 2, 2016, from The Washington Post:

https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/?utm_term=.e3f66b4558e5
Philip Rees, D. H. (2007). “Transfers of personal data and Binding Corporate Rules. Binding Corporate Rules: a simpler clearer vision?”. *Computer Law & Security Report* .
Poullet, Y. (2007, March 21). “Transborder data flows and extraterritoriality: The European position”.
Privacy Shield. (n.d.). Retrieved Deember 2, 2016, from https://iapp.org/media/pdf/resource_center/eu_us_privacy_shield_full_text.pdf.pdf
Proprosal for a Regulationof the European Parliamant and the Council. (2012, January 25). Retrieved July 15, 2016, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN
Proust, O. (2016, July 16). *"EU-US Privacy Shield comes into force".* Retrieved August 5, 2016, from Privacy Law Blog: http://privacylawblog.fieldfisher.com/2016/eu-us-privacy-shield-comes-into-force/
Reform of EU data protection rules. (n.d.). Retrieved July 11, 2016, from European Commission : http://ec.europa.eu/justice/data-protection/reform/index_en.htm
Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). (2016, April 27). Retrieved May 15, 2016, from http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
Renee Berry, M. R. (May 2012). *Renee Be“Policy challenges of cross-border cloud computing”.* Journal of International Commerce and Economics.
Rohan Massey, H. E. (2012, June 19). *“Binding corporate rules as a global solution for data transfer”.* Retrieved June 19, 2016, from Lexology: http://www.lexology.com/library/detail.aspx?g=353eff70-2fd3-4c7e-a8ab-571893b4b6a1
Sheftalovich, Z. (2016, Februrary 13). *"The phone call that saved Safe Harbour".* Retrieved August 5, 2016, from Politico: http://www.politico.eu/article/the-phone-call-that-saved-safe-harbor-john-kerry-frans-timmermans
Solove, D. (21, April 2014). *„The future of global privacy: Conflict or harmony?” .* Retrieved April 10, 2016, from LinkedIn: https://www.linkedin.com/pulse/20140421120856-2259773-the-future-of-global-privacy-conflict-or-harmony?_mSplash=1&published=t
Somers, M. (2015, October 28). *"OPM notifies 3.7 million cyber attack victims about data protection services”.* Retrieved December 2, 2016, from Federal News Radio: http://federalnewsradio.com/cybersecurity/2015/10/opm-notifies-3-7-million-cyber-attack-victims-about-data-protection-services/

Sookman, B. (2015, October 12). *"Schrems, what the CJEU decided and why it is a problem for Canadian and other non-EU businesses".* Retrieved May 15, 2016, from Barry Sookman: http://www.barrysookman.com/2015/10/12/schrems-what-the-cjeu-decided-and-why-it-is-a-p

Statement of the Article 29 Working Party. (2015, October 16). Retrieved June 17, 2016, from http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

Statement of the Article 29 Working Party on the presentation by the European Commission of the EU-U.S. Privacy Shield". (2016, February 29). Retrieved June 17, 2016, from http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160229-pressrel_publication_europeancommission_eu-us_privacy_shield.pdf

Steve Coughlan, R. J. (2006, June 23). *"Global reach, local grasp: constructing extraterritorial jurisdiction in the Age of Globalization".* Retrieved June 19, 2016, from Dalhousie Law School: https://dalspace.library.dal.ca/xmlui/bitstream/handle/10222/10268/Coughlan_Currie%20et%20al.%20Extraterritoriality%20EN.pdf?sequence=1&isAllowed=y

The EU General Protection Regulation is finally agreed". (2016). Retrieved May 15, 2016, from Allen & Overy: http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf

Wikariak, S. (2015, October 22). *„Transfer naszych danych do USA trzeba zalegalizować".* Retrieved November 20, 2015, from Gazeta Prawna: http://prawo.gazetaprawna.pl/artykuly/900987,po-orzeczeniu-tsue-transfer-danych-do-legalizacji.html

Yadron, D. (2016, February 17). *"Apple ordered to decrypt iPhone of San Bernanrdino shooter for FBI".* Retrieved June 25, 2016, from The Guardian: https://www.theguardian.com/us-news/2016/feb/17/apple-ordered-to-hack-iphone-of-san-bernardino-shooter-for-fbi