Exporting the Policy - International Data Transfer and the Role of Binding Corporate Rules for Ensuring Adequate Safeguards[1]

Bianka Maksó

Phd student, Deák Ferenc Doctoral School of Law, University of Miskolc, Hungary

Personal data plays a key role in our digital age. The legislator is working on making the data controller interested in protecting personal data by self-regulation, so Binding Corporate Rules were enacted as the latest legal institution for ensuring adequate safeguards in case of international data transfers. In this study after a brief description of the strategic value of personal data the author makes an attempt to introduce BCR and their legal background within the rules of international data transfer in order to give an introduction on how EU data protection policy can affect data controllers in third countries.

Keywords: Binding Corporate Rules, international data transfer, adequate level of protection, personal data protection, GDPR, adequate safeguards

1. Introduction

Personal data have economic and strategic value not only for the data controller, but also for the data subject, undoubtedly. In our digital age, applying data protection measures is not a prestige of the data controller, but an obligatory legal requirement and an essential interest of the data subject. This factor is of high importance mostly in cases of data transfers to third countries where the adequate level of protection of personal data must be ensured. As the addressees of the regulation of data protection requirements have been differentiated in the last decade and enterprises have carried (some of) the highest risks of data breaches, the tendency of both EU and domestic legislation is to give priority to self-regulation[2] to enable data controllers to create rules and processes themselves for compliance, for ensuring the rights for personal data protection and for efficient maintenance at the same time. In this tendency Binding Corporate Rules (hereinafter: BCR) have a high importance at first glance as the General Data Protection Regulation[3] (hereinafter: GDPR) considers this legal institution one of the most important legal ways for ensuring adequate safeguards in third countries. However, several concerns may be raised and the real advantages have not been experienced so far.

[1] This research was (partially) carried out in the framework of the Center of Excellence of Mechatronics and Logistics at the University of Miskolc.

[2] Szőke G. L. (2015): *Az európai adatvédelmi jog megújítása – Tendenciák és lehetőségek az önszabályozás területén*, HVG-ORAC Lap- és Könyvkiadó Kft, Budapest

[3] Regulation 2016/679 (General Data Protection Regulation) OJ 2016 L 119, 4.5.2016, pp. 1–88.

2. Personal Data from a Different Perspective

Personal data are natural intermediate goods having value for the data subject and the data controller as well. This perspective is determined by Posner[4] providing a pure but picturesque situation in order to prove the statement: at a job interview, people sell themselves as commercial goods. They can hide the disfavoured qualities to get the job and at the same time mislead the employer. In conclusion hiding personal data or with other words exercising the right to information self-determination results in distorting the market and the real competition by default of performance. However, Posner added, that we can only save ourselves from disadvantageous transactions if we are entitled to retain personal information and others are prohibited to seek sensitive data.

Most infringements and data breaches remain latent as the data subject does not raise a claim because of the unlawful activity as he does not even know or eventually does not care about it. This careless behaviour changes immediately when the data subject has suffered financial loss or disadvantage, e.g. price discrimination at a webshop, or if the level of disturbance has exceeded his own tolerance in case of receiving spam mails or phone calls. However, people are ready to provide as much data as they are asked for for the tiniest benefits like using the supermarkets' store loyalty cards providing a clear picture to the company about buying and eating habits. Due to this tendency we can note that conscious information-self determination requires actions and denials taken by the data subject.

Laudon suggested a digital market of personal data[5] where the data subject can earn money by selling his data. In his market, we can have our own account to sell pieces of personal data at a price negotiated with the buyer. We can even hire agents to achieve better price. The biggest benefits are on one hand that the data subject would be able to follow the way of his data and could keep control over its processing, on the other hand, one would get financial profit from transactions. If we think of direct marketing, we can recognize some similarity albeit with the difference that the data subject cannot claim profit earned by selling his data.

In conclusion, personal data as a layer of our privacy has emotional and social, furthermore economic value for the data subject.

For the data controller, personal data do not have any emotional value but rather possess strong and strategic economic value. In case of a life insurance contract, the more sensitive the personal data is, the more value it has, influencing the details of the further contract. Also, personal data have effects on marketing costs such as the effectiveness of targeted commercials. Applying data protection measures may attract new customers and improve good reputation. In addition, controlling and transferring personal data play significant role in the everyday basic operation of multinational companies like banks, airlines, software providers, internet-based services or any companies with consumer service departments even if operated in third countries.

In conclusion personal data as an economic good is the new gold for the data controller and the trust is the key to make profit out them.[6] To enhance trust data controllers must have transparent privacy policy, respect the principles like purpose limitation, inform the data subject and process data with his

[4] Posner A. R., *The Right of Privacy, Georgia Law Review*, Vol. 12, No. 3, Spring 1978, Georgia.

[5] Laudon, K. C., *Markets and Privacy, Association for Computing Machinery*, *Communications of the ACM*, Sep 1996, Vol 39, No 9, 92-104, ABI/INFORM Global.

[6] Woolley L.A., *In the digital age, data is gold and trust is the key* http://www.fiercecmo.com/special-report/digital-age-data-gold-and-trust-key (20 October 2016).

permission, in case of the likeliness of any infringement an urgent action is needed to take parallel with noticing the affected data subject.

Last but not least, continuous compliance is also a prior obligation which requires serious efforts mainly in third countries at the events data transfers in spite of the fact that the data controller in a third country may not be subject to EU legislation. In the following sections I aim to highlight why and how the EU's data protection policy can be exported outside the EU.

3. Rules of International Data Transfer

The answers for the questions of why and how the EU's data protection policy can be exported outside the EU are given by the rules of international data transfer.

3.1. Why do the Rules of International Data Transfer Export the Policy?

Noticeably the current regulation does not define the expression "transfer to a third country" and although uploading data to a website which constitutes the subsequent transmission of those data to anyone who connects to the internet and seeks access to it from all points of the world, it does not send that information automatically to people who did not intentionally seek access to those pages, this was thus not considered to be data transfer to a third country.[7]

However, the EU has reached harmonized legal background of personal data protection enhancing it to the level of *primary source of law* by the entry into force of the Treaty of Lisbon and by endowing the Charter of Fundamental Rights with legal binding force equivalent to that of the Treaties. As a secondary source Directive 96/45/EC (hereinafter: Directive) was adopted, a major reform of which began in 2012. Today, the GDPR is already at our doorstep and urges the member states for prepare for its application which will commence with 25 May 2018. In addition, this source of law has direct applicability and the member states are prohibited from implementing it by domestic legislation, so the rules will be directly applicable.

In order to *provide a high standard of personal data protection and ensure data subject's rights* in our virtual age in the digitized economy where the flow of personal data is unlimited – and I must admit that it is also essential and necessary for using certain services – irrespective of state borders and jurisdictions, the legislator must create rules which can safeguard rights outside the geographical borders of the EU.

This is of high importance[8] the well-known case of *C-362/14 Schrems v Ireland Data Protection Commissioner* has shown.[9] In this case it was clearly stated that in the USA, companies did not comply with the basic principles of data protection and personal data is processed by authorities in a way incompatible with the rule of purpose limitation. Finally, the so-called Safe Harbour Decision 2000/520, which was adopted by the Commission in relation to US companies providing adequate level of protection, was declared invalid.

[7] C-101/01 – Lindqvist [2003] ECR 2003 I-12971, p. 56, 59, 60, 70.

[8] Data subjects also feel this important. Check the survey: European Commission: Social Eurobarometer 359 Attitudes on Data Protection and Electronic Identity in the European Union, 2011, Bruxelles, available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf (4 November 2016).

[9] C-362/14 – Schrems [2015] (not yet published in the ECR) ECLI:EU:C:2015:650 p. 14.

3.2. How do the rules of international data transfer export the policy?

Both the Directive Article 25 para. 1. and the GDPR Article 44 determine the default rule: transfer may take place only if *the third country ensures an adequate level of protection*.

The GDPR's preamble declares (103 and 105) that without the need to obtain any further authorisation, transfer to third country can only take place if an adequate level of data protection is offered. The GDPR applies a differentiation between a third country, a territory or specified sector within a third country, and an international organisation. Adequate level is *a level equivalent to* that ensured within the Union: effective independent data protection supervision is required and cooperation mechanisms with the Member States' data protection authorities is needed, also, the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress. These factors have not been determined in regulation until the above cited Schrems-case, but it is supportable to implement them into a legislative act instead of referring to it only in case-law. The GDPR's preamble also states (104) that for evaluating the adequacy of the Commission takes into account several objective criteria: how a particular third country respects the rule of law; access to justice; international human rights norms and standards; general and sectoral law; specific processing activities and the scope of applicable legal standards. This is a complex development as under the Directive the assessment dealt with circumstances surrounding a data transfer: the nature of the data; the purpose and duration of the proposed processing operation, the country of origin and country of final destination; the rules of law, both general and sectoral and security measures which are complied with in that country. So instead of the former operational perspective, the *GDPR rather puts emphasis on the legal guarantees* offered to the data subject.

According to the rules detailed above, a data controller in a third country shall ensure the same level of protection for personal data as the data controller in the territory of the EU. However, the data controller in the third country is not subject to the EU regulation, and not subject to any member state's or the EU's jurisdiction, yet it shall comply with EU standards of data protection. This phenomenon can be deemed the 'export' of the EU's policy into third countries.

Both the Directive and the GDPR have specified rules on data transfers to third countries and both can be characterized by their extraterritorial effect[10] on data controllers running in third countries. Compliance will be a crucial factor in the future, because the GDRP will raise the administrative fees in case of infringement up to 20000000 euros or 4% of the total worldwide annual turnover of the preceding financial year which also proves the sensitive value of personal data and privacy protection. Also, it must be noted that in many cases compliance is obligatory for the data controller itself as a natural person or legal person, and not for the third country as a whole, although many factors of adequacy, such as the independent supervisory authority or the respect of the rule of law, depend on the third country's constitutional system. In order to cope with this anomaly the GDPR seems to introduce a different perspective: it supports self-regulation which has the ultimate advantage of improving the willingness to comply. It introduces codes of conducts and certification intended to contribute to the proper application of GDPR. In relation to international data transfers GDPR inherited the essential structure of the Directive, but it is extended in the adequacy methods.

[10] Kuner, C. (2015), *Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law*, University of Cambridge Faculty of Law Research Paper No. 49/2015, Cambridge.

In the USA self-regulation started in the early 1990's, but has not earned successful appreciation. Only those self-regulatory actions were able to exist longer which enjoyed governmental involvement. Self-regulation was mostly supported and promoted but not applied. A well-detailed, transparent and adequate self-regulatory method with regular audits and certifications can easily become a burden for its subjects and the need for rephrasing the regulations in effect has already been eliminated.[11]

4. Thoughts on Binding Corporate Rules

4.1. BCR in the GDPR

A transfer of personal data to a third country or an international organisation may take place if the adequacy is ensured by one of the following measures:

- the *Commission has decided* that the third country ensures an adequate level of protection; This kind of legal basis was also applied in the above referred Schrems-case regarding Decision 2000/520 and many other countries have earned such a decision[12];

in the absence of such decision:

- based on *an international agreement* in force between the requesting third country and the Union or a Member State, without prejudice of the rules of GDPR;
- a controller or processor may transfer personal data only if the controller or processor has *provided appropriate safeguards*, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

The appropriate safeguards are the following pursuant to Article 46 of the GDPR:

- a legally binding and enforceable instrument between public authorities or bodies;
- *BCR*;
- standard contractural clauses adopted by the Commission;
- standard contractual clauses adopted by a supervisory authority and approved by the Commission;
- an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards;
- an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards.

Standard contractual clauses were constructed by the Commission[13] and experience has shown that they are useful for companies transferring personal data on an occasional basis and transferring a limited amount of personal data. All other means are ways of self-regulation.

[11] Wright D. & De Hert P. (eds.), *Enforcing Privacy: Regulatory, Legal and Technological Approaches Law*, Governance and Technology Series, Volume 25, Springer International Publishing, Switzerland, 2016.

[12] See the full list of the countries: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (5 November 2016).

[13] Between data controllers and data processors: 2010/87/: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) OJ L 39, 12.2.2010, pp. 5–18, Between data controllers: 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (notified under document number C(2001) 1539) OJ L 181, 4.7.2001, p. 19 and 2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction

The EU legislator supports self-regulation as BCR is enacted as a prior method for ensuring adequate safeguards among several other means. In order to enhance transparency and compliance with the GDPR, codes of conducts and certification are strongly encouraged. So it is not surprising that the above cited list of the appropriate safeguards includes the BCR as its second element ahead all other commonly applied methods.

4.2. BCR as a Legal Instrument

BCR mean "policies which are adhered to by a controller or processor established on the territory of a Member State 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, or group of enterprises engaged in a joint economic activity" pursuant to Article 4 paragraph (20) of the GDPR.

BCR are designed for regular transfers of huge sums of personal data. By applying this code of conduct, companies can avoid further administrative procedures and data transfers can be conducted without any other requirement to fulfil.[14] By obeying its rules, compliance of the members of a multinational company is also ensured as the rules of the BCR were authorised by the supervisory authority or even other member states' authorities in advance before its first application. Furthermore, in case of any changes of the legal surrounding or the structure of the applying companies or the nature of the data transfers a revision is compulsory.[15]

Although BCR have binding force on the applicants and the data subjects as third party beneficiaries become entitled to enforcement before the data protection authority and/or the competent court,[16] there have been hot debates whether BCR as unilateral commitments can constitute a right for the data subject to claim for remedy before a court.[17] It has not been experienced either how the data controller in the EU can satisfy the burden of proof in case of infringement committed by the member of the group in a third county.

However, BCR are designed *to reduce administrative costs and burdens*, it seems that authorizing BCR is a long-lasting and costly procedure. According to the ICO, the UK's data protection authority, the procedure may last as long as a year.[18] I must note that in Hungary, following its introduction on 1

of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271) OJ L 385, 29.12.2004, pp. 74–84.

[14] Before the enactment of BCR it was also assumed that it will eliminate further needs of administrative actions to take for international data transfers. STEPHENS, J. (2003): *International communications round table ASBL: ICTR comments on bindign corporate rules***.** Brussels 30 September 2003, an open letter of ICRT to the Article 29 Working Party http://ec.europa.eu/justice/data-protection/article-29/press-material/public-consultation/bcr/2003_bcr/icrt_en.pdf (15 November 2016).

[15] 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*), Adopted on 24 June 2008, B-1049 Brussels, Belgium, Office No LX-46 06/80, point 5. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp153_en.pdf (15 November 2016).

[16] Article 29 Data Protection Working Party: *Working Document Setting up a framework for the structure of Binding Corporate Rules (WP 154),* Adopted on 24 June 2008, Brussels, Belgium, Office No LX-46 06/80. point 18. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp154_en.pdf (15 November 2016).

[17] Article 29 Data Protection Working Party: *Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers (WP 74),* Adopted on 3 June 2003, Brussels, Belgium, Office No C100-6/136, point 1 and 3.3.2. http://www.naih.hu/files/D_bcr_wp074_en.pdf (15 November 2016).

[18] https://ico.org.uk/for-organisations/binding-corporate-rules/ (4 November 2016).

October 2015, over a period of a year more than twenty multinational companies[19] with several members have finished the process of their BCR. The highest costs are incurred regarding legal counsels who facilitate the administrative processes before the national data protection authorities. The costs deriving from the administrative nature of the process differ in each member state, but none can be deemed expensive.[20] As for the procedure it must be evaluated as being a complex one. The draft is required to be submitted and the applicant is obliged to modify it according to the notes and comments of the national data protection authorities as many times as it is needed, otherwise the BCR may not get authorization.

The cooperation of the involved national authorities is also a key factor. To avoid difficulties in this part of the process a so-called *mutual recognition procedure* has been established. According to this, once the lead authority considers that a BCR meets the requirements, the other involved authorities shall accept it as sufficient basis for their own national permission.[21]

The most serious drawback of BCR currently is that not all Member States of the EU have implemented this legal institution, although from 2018 onwards it will be *directly applicable* because of the entry into force of the GDPR.[22] So, there will be no need for legislative acts to get the BCR commonly accepted but the *best practises should be shared* among companies and authorities as well to create harmonized legal surrounding and practice.

Harmonization without its legal aspect also may be improved within the company's operational policies, as the member of the multinational company in the third country as a subject of the BCR have to keep rules which are based on the standards and legal obligations and rights enacted in the EU. However, these compulsory rules only ensure protection within the company. BCR generalize the data protection standards but they can *improve the level of obedience*. One of their compulsory contents is a complaint handling procedure which can result in a good way to solve problems within the company. BCR are designed to *be individualized to the applying group of companies*.[23] Its flexibility provides the opportunity to fit into the field and structure of the certain industrial sector of the company. A further disadvantage also comes with structural issues: the sub-processor in the third country who is not a member of the multinational company is not subject to BCR automatically, thus the adequate level cannot be deemed to be ensured in relation to the sub-process; meaning that the abovementioned contractual clauses should once again be used.

5. Conclusion

BCR can contribute to better reputation and serve as a good marketing tool, and can also help to establish better contacts with the national authority. Nevertheless there is not enough empirical evidence yet to declare it the best way of ensuring an adequate level of protection. Until the first examples of best practices will become open to the public or less complaints will be raised because of data breaches, the expectations of BCR are difficult to prove.

[19] http://naih.hu/a-bcr-t-magyarorszagon-alkalmazo-adatkezel-k.html (4 November 2016).

[20] For example, in Hungary the procedural fee is 266000 HUF while in Denmark it is free of charge.

[21] Recently 21 countries are taking part in the mutual recognition process. http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/mutual_recognition/index_en.htm (4 November 2016).

[22] See the details: Article 29 Data Protection Working Party: *National filing requirements for controller BCR ("BCR-C")*, Last update: February 2016, http://ec.europa.eu/justice/data-protection/international-transfers/files/table_nat_admin_req_en.pdf (15 November 2016).

[23] cit. WP 74. point 3.1.

In addition EU data protection policy has been partly already exported to create safe harbours again on the windy ocean. The European Commission on adopted 12 July 2016 the EU-USA Privacy Shield[24] in order to replace the invalidated Safe Harbour Decision to serve as legal basis for data transfers to the USA ensuring the requirement of adequate level of protection. 'Furthermore it brings legal clarity for businesses relying on transatlantic data transfers.'[25] US companies must first sign up to the framework with the US Department of Commerce and must apply a privacy policy which includes safeguards for the data subject to ensure the standard of the EU's protection level enforceable under US law. These safeguards are similar, but not the same guarantees as in the EU, such as rights for the data subjects, providing free and accessible dispute resolution before authorities and arbitration at the request of the individual, maintaining data integrity and purpose limitation, obligatory rules for sub-processors and finally having transparent data protection measures and actions.[26]

Undoubtedly it is high time for establishing an efficient method of personal data protection in third countries also as more and more modern challenges like Web2 solutions, drones and world-wide economic relations creates challenges to face. And data controllers have a rushing and growing need for personal data, as it is the gold of the new age.

[24] European Commission - Directorate-General for Justice and Consumers: *Guide to the EU-U.S. Privacy Schield*, European Union, Beglium, 2016.

[25] http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm (5 November 2016).

[26] https://www.privacyshield.gov/Key-New-Requirements (5 November 2016).