MultiScience - XXX. microCAD International Multidisciplinary Scientific Conference
University of Miskolc, Hungary, 21-22 April 2016, ISBN 978-963-358-113-1

International data transfer with special attention to the conclusions of the invalidity of US Safe Harbour scheme

dr. Bianka Maksó[1]
Ph.D. student
University of Miskolc, Deák Ferenc Doctoral School of Political Science and Law

INTRODUCTORY IDEAS

"It is to be concluded that Decision 2000/520 is invalid."[2] With this ruling the Court of Justice of the European Union annulled the legal base of adequate level of protection concerning personal data transfers from the EU to the territory of the USA. Among several reasons the most significant one on which this decision is mostly based is that the practise of the USA, i.e. federal agencies were capable of accessing to the personal data which had been transferred to the United States while the Union citizens have no effective rights to be heard, fails to comply with EU laws. The adequate level of protection, which is a prior requirement of international data transfers, is cannot be deemed ensured by the USA as a third country as the Decision of the Commission on 'Safe Harbour Scheme' declared invalid. In this paper I am willing to examine how the Safe Harbour scheme really worked, why was it annulled and what other legal instruments are available to replace it.

REGULATION OF INTERNATIONAL DATA TRANSFER

From a European citizen's point of view

Principles dates back to the 1980's when the OECD published its recommendation[3]on personal data transfer. Principles became statutory regulations which derive from the human right of the protection of privacy and personal data.[4] At an EU level the Treaty of Lisbon gives legal effect to the Charter of Fundamental Rights so that the issue of privacy protection has been enhanced to the level of primary source of law in 2010. Furthermore the Article 16 of Treaty on the Functioning of the European Union declares the right to the protection of personal data concerning them.
The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter: Directive) was enacted at EU level which is the main legal source of general[5]data protection. As its preambles declares the expansion of international trade is important but the protection of individuals guaranteed in the Community by the Directive does not stand in the way of transfers of personal data to third countries. However every data controller shall respect the data subjects' fundamental rights and freedoms, especially the right to privacy, so transfers to a third country which does not ensure an adequate level of protection shall be prohibited. As the largest economies in third countries "are lacking the comprehensive law […] supervisory and enforcement mechanisms"[6]in the field of data protection then the EU legislator shall take actions

DOI: 10.26649/musci.2016.129

to protect EU citizens. Especially in the field of international data transfer some experts consider EU legislation an extraterritorial jurisdictional regime, [7] not in the scope of the Directive but in effect of its rules.
Article 25 of the Directive declare default rules: transfer may take place only if the third country in question ensures an adequate level of protection. The Court of the EU in the so called Lindquist – case (C-101/1.) ruled that there is not an exact concept of international data transfer. Conceptual characteristics has been added by the Curia in the judgement of C-362/14 in points 73 and 74. according to which a third country cannot be required to ensure a level of protection identical to that the EU legal order but the 'level of protection [...]is essentially'. The means may differ but have to prove effectiveness e.g. existence of independent supervisory entity, judicial way of enforcement and compensation, enforceable rights of the data subject. Article 26 states derogations for cases in which the third country does not provide adequate level but personal data still can be transferred. Ways of ensuring adequate level is using contractual clauses[8] created by the Commission. Pursuant to the Article 25. para (6) the Commission as a result of a comitology procedure can find that a third country[9] ensures the adequate level of protection as did so in connection with the USA by the 2000/520/EC Commission Decision on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.[10]

To a Safe Harbour through a windy ocean

Since the adoption of the Directive data transfer between the EU and USA has raised hot debates and the latest news have widened the gap. The US data protection legal system differs significantly from the EU system.
The concerns root in deeper social and legal differences[11] of privacy which is really far from globally accepted concept. Privacy is undoubtedly based on the well-known Warren-Brandeis interpretation in the fundamentally dissimilar regimes there are several differences. In the EU comprehensive laws regulates data protection both general and sectorial while in the USA rather sectorial or ad hoc rules are in effect and self- and co- regulation is well-accepted. The constitutional base of data protection in the EU is a fundamental right of a dynamic and evolving Constitution. In the USA privacy exists in three values: i) personal autonomy[12] ii) right to be let alone iii) right to information privacy while the idea of the living Constitution is disfavoured. The privacy in the USA is deriving from property and contract, alienated from the individual while in the EU personal data is part of the identity.[13] The supervisory authority in the EU has comprehensive investigation powers and can fine sanctions. In the USA supervision is varied in models and its applicable legal means vary according to the sector nature. Sectorial regulation has appeared in the fields of banking data, children online activities, direct marketing etc. although some experts deem it particular i.e. not integral but partial, rather than sectorial.[14]
The US federal powers in data protection can occur only in the area of consumer protection. The federal Privacy Act (1974) cannot be applicable for business organisations and it includes much softer rules and the Directive and standards.

There has been a strong tradition that business organisations prefer self-regulation instead of state intervention.[15] But latent infringements and the high risk if impossibility on control over data controllers have not strengthen this attitude. However, the same tendency, i.e. the data subject's weakening role in exercising rights, has arising in the EU as well. This supports the efforts to oblige the data controller to ensure protection and encourage providing adequate protection by self-regulation instead of providing rarely exercisable rights for the data subject.[16]
In order to the transfer of personal data to the USA would not be prohibited the *US Department of Commerce and the EU reached an agreement* which resulted in the Safe Harbour scheme determined by the 2000/520/EC Commission Decision (hereinafter: Safe Harbour Decision). By this legal instrument the EU recognized that the companies operating in the territory of the USA that want to "avail themselves of the proposed "safe harbour" will have to *certify that they will protect the information they collect* in accordance with prescribed guidelines."[17]The "safe harbour" created by the Principles and the FAQs issued by the US Department of Commerce on 21 July 2000. Self-certification is voluntary.
Pursuant to Annex I the following principles shall be respected:

- notice: informing individuals about the data control in details with special attention to purposes, limitations, about third persons able to get to know the collected data, ways of rights enforcement
- choice of op out
- onward transfer in case the third party acknowledge the principles
- security
- data integrity: information shall be relevant to the purpose
- access of individuals
- enforce: affordable independent recourse mechanisms; follow up procedures of compliance and obligation of remedy issues

FAQs which have also binding force on the certifying organisations contains certain problematic issues which shall be handled during application e.g. the non-existence of second liability, the events of the use of sensitive data without explicit consent, the issue of self-certification, verification in follow up procedures, the matters of individual's access, issued of data transfers concerning employee's data.
Two conjunctive requirements were stated:[18]the organisation receiving the personal data has unambiguously and publicly disclosed its commitment on compliance with the Principles implemented in accordance with the FAQs *and* the statutory powers of a government body in the United States listed in Annex VII can be applicable on them i.e. certain state agencies are empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in case of non-compliance. Organisations shall be subject to the jurisdiction of the Federal Trade Commission. Decisions to qualify for the safe harbour are voluntary, and qualification can be received in different ways.[19] More than 5500 firms has volunteered to comply with the rules[20] e.g. Apple Inc., Hewlett Packard Enterprise Company and its U.S. subsidiaries, Facebook Inc. Federal Trade Commission (hereinafter: FTC) was responsible for the handling of obligatory tasks deriving from the Safe Harbour Decision such as prohibiting the certain action, filing a complaint in a federal

district court in case any violation and dealt with individuals' complaints, taking notifications to the Department each time.
However the declarative and voluntary nature of the scheme indicated concerns about its execution and its real transparency. Debates reflected that US state agencies had access and processed personal data in a way which did comply with the original legal ground and purposes of collection. Furthermore companies also failed to comply the certified principles.[21]

ACCORDING TO THE JUDGEMENT

The previous sections of this paper can be considered an interesting part of legal history as the Curia by the judgement of C-362/14 in point 106. got to the conclusion that the Safe Harbour Decision is invalid. However the decision is based on pure procedural issues rather than substantive ones.

Facts of the case

An Austrian national residing in Austria made a complaint to the Commissioner in which he asked the Commissioner to prohibit Facebook Ireland from transferring his personal data to the United States because the law and practice in force in there did not ensure adequate protection against the surveillance activities. The Commissioner concluded that he was not required to investigate the complaint so he rejected it as unfounded. He added that there was no evidence that the relevant personal data had been accessed by the NSA. The basic statement of the decision is that "the adequacy of data protection in the United States had to be determined in accordance with Decision 2000/520 and the Commission had found in that decision that the United States ensured an adequate level of protection".[22] As the Irish laws prohibit the transfer in case that the third country does not provide adequate level of protection and according to the High Court which decided in this case a second instance forum also declared that surveillance can only occur if it is verified by objective reasons, have legitimate purpose and there are suitable guaranties. Even though the validity of the Safe Harbour Decision was not formally contested, the question was whether the Commissioner was bound by the Safe Harbour Decision that the United States ensures an adequate level of protection or the Commissioner can take other findings on his own investigation.

The preliminary ruling and the conclusions

Basic statement of the Curia that the Directive shall be interpreted in the light of the fundamental rights guaranteed by the Charter. According to the merit of the judgement the national supervisory authorities have a wide range of powers, but they do not have powers in respect of processing of such data carried out in a third country. Nevertheless the operation of transfers to third countries itself shall be considered to be processing of personal data so the member stated pursuant to Article 25 and 26 of the Directive are entitled to take control over them. Conclusively in point 52. of the Judgement:

> *'Thus, until such time as the Commission decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, admittedly cannot adopt measures contrary to that decision […]'*

However it also states in point 57. and 66. that the national supervisory authorities upon any request must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the directive. In cases similar to this one the national supervisory authority's task to examine the claim with all due diligence regardless of the decision made by the Commission in the subject of a third country about its adequate level of protection. The judgement highlights that the Safe Harbour Decision has not binding force on state agencies in line with that national security, public interest, or law enforcement requirements' have primacy over the safe harbour principles at all. Additional comment of the Curia is that there is no effective judicial protection against these kind of measures. According to the referred communications the Commission came to the conclusion that the principles of proportionality and the purpose of national security did not based the accessions, while there were no effective judicial or administrational means of redress. Furthermore in Safe Harbour Decision it is not declared that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law. The court did not examined the content of the principles but annulled the whole Decision as its articles failed to comply with the Directive and the Commission exceeded its powers by accepting it.

REPLACE WITH BCR

Conceptual determination

The legal recognition of Binding Corporate Rules (hereinafter: BCR) has gone through a long development process until it became a familiar[23] legal instrument for multinational companies. Its first appearance dates back until 2003 and since then further soft-law-type legal sources and national statutory regulations provides conceptual and procedural instruction about BCR. The Article 29 Working Group[24] published several working papers, significantly in 2005 and in 2007[25], on the applicability, the function, the authorizing procedures, a code of practise of BCRs and checklist for companies to follow during drafting one to verify compliance to serve as a soft law legal source for the private sector and the authorizing state organs as well. A standard application form has also been published to support the mutual recognition system in order to maintain a harmonised practise among authorities of the member states.

Its more than dozen-year-long history now seems to have a sudden rising as the draft of the General Data Protection Regulation[26] declares it in Article 42. para (2) a particular and prior mean of providing the adequate level of protection just besides the Commission's Decision enacted in Article 41. In the legal text Article 4. point 17. defines that BCR '*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.' BCR includes essential principles and enforceable rights as internal rules of a multination group of companies to ensure appropriate safeguards as global policy for transfers of personal data within the company's affiliates running in third countries which do not provide an adequate level of protection. [27] Safeguards can be structured to be the most suitable for the company's needs.

Reasons for replacing

BCR is an alternative of signing standard contractual clauses each time it needs to transfer data once it was approved under the EU cooperation procedure by national data protection authorities. But can it replace the Safe Harbour Decision as well?

<table>
<tr><th></th><th>BCR</th><th>Safe Harbour Decision</th></tr>
<tr><td rowspan="4">Legal nature</td><td colspan="2">- voluntary application
- binding force
- works with state cooperation and supervision
- commitment of a private sector organisation to comply with its rules and respect its principles
- ensures adequate level for the company and its affiliates, not in the third country itself</td></tr>
<tr><td>legal mean enacted in private law</td><td>legal mean enacted in public law - Commission Decision</td></tr>
<tr><td>terms and conditions</td><td>self-certification</td></tr>
<tr><td colspan="2">for applicability actions of private organisations' and state actions are/were needed as well</td></tr>
<tr><td rowspan="2">Supervision</td><td>national data protection authorities in relevant member states</td><td>FTC at federal level</td></tr>
<tr><td>start investigation upon request of ex officio</td><td>start investigation only upon request</td></tr>
<tr><td>Actions have to be taken for application</td><td>- making a draft
- having it authorized by DPAs
- reporting to the Commission
- paying fee
- continuous up-dating
- obligation to report any changes
- following the technological developments</td><td>- making commitment to respect principles and FAQs
- having the commitment registered
- reporting to the FTC</td></tr>
</table>

Content	highly detailed and created directly in accordance with the structure of the company and the nature of the transfers	general principles and FAQ for practical issues regardless of the certifying organisations needs or structure
	can provide high level of protection general	results law level of protection

Table 2: Comparison of BCR and Safe Harbour Decision

The aim of both legal tools is to ensure the required 'adequate' level of protection. With regards to the legal nature of the BCR and Safe Harbour Decision it is undoubtedly that both are voluntary and once it is applied it has binding force. It is noticeable that BCR has internal and external binding force as well. As for internal binding force the company may fine sanctions in case of breaching the BCR by the company or its affiliate. As for external binding force data subject may raise claims or even sue the company for infringing his right for data protection. While BCR is a self- (and/or co-)regulating legal mean i.e. a private organisation commitment and its authorization by state authorities, Safe Harbour Decision was a state action which needed a private organisation's commitment on complying. Both ensured the adequate level for a certain company. BCR's biggest advantage is that this legal mean is created by the company as a code of conduct which fits the best for the company. Safe Harbour was a sum of principles and practical 'questions and answers' created by the Decision without a opportunity to be changes by the applying organisations. While Safe Harbour application was supervised by the FCT, BCR is continuously looked after by nation data protection authorities. Although the authorization of the BCR is a much complicated procedure, it results a more developed tool which compliance is checked by several nation authorities according to several national laws. European data protection rules has no counterpart in the USA at a similar general and comprehensive level so that Safe Harbour Decision created a brief and general summary of European legal principles for the USA resulting a lower level of protection. The Safe Harbour Decision and its purpose was well-known globally but BCR can be respected as well if the General Data Protection Regulation will come into effect.

CLOSING IDEAS

'Safe Harbour is expected to continue without dramatic change'[28] - this sentence was written in the mid 2015 but it turned out soon that it was inappropriate. As the USA strongly separate the private and the public sector in data protection matters the EU has strict policy on comprehensive data protection. According to the concept of separation of information powers[29] the concentration of personal data is the biggest danger on privacy. As USA consider personal data as alienated commodity then the renewed idea of a data market[30] in which merchants works to evaluate each piece of data and its owner to conclude contractual purchase of such data cannot be

denied at first sight. In the USA among the latest efforts there are a proposal on consumer privacy bill of rights act,[31] plans to establish a new Federal Privacy Council and create rules on communication privacy.[32]

In conclusion as Safe Harbour Decision was found invalid, organisation running in the USA have to find a solution to comply with laws to transfer personal data from the territory of the EU legally. To achieve legal compliance they have to proof to ensure the adequate level of protection. A possible solution, instead of waiting for a next Commission decision or contracting for each transfers, can be a BCR. Great advantages of it are its flexibility and adaptability and the higher level of protection than it was deriving from the Safe Harbour principles.

---

[1] The author is a Ph.D. student in Deák Ferenc Doctoral School of Political Science and Law, University of Miskolc. Contact: jogmakso@uni-miskolc.hu. This research was (partially) carried out in the framework of the Center of Excellence of Mechatronics and Logistics at the University of Miskolc.

[2] C-362/14. Judgment of the Court (Grand Chamber) of 6 October 2015., Maximillian Schrems v Data Protection Commissioner, point 106., Reports of Cases: not yet published.

[3]http://www.oecd.org/sti/ieconomy/15590228.pdf [last date of download: 2/1/2016]

[4]OHCR and ECHR declare the protection of privacy, ICCPR prohibits the unlawful interference with his privacy.Furthermore many European constitutions state the right for privacy or the protection if personal data.

[5] General in this sense refers to the distinction between sectorial regulation and general rules of data protection.

[6] KAMARINOU, Dimitra: International transfer of personal data and compliance under Directive 95/46/EC, the dratft Regulation and the international community, *Communications Law*, vol. 18, no. 3, 2013

[7]KUNER, Christopher: *Extraterritoriality and Regulation of International Data Transfersin EU Data Protection Law*, University of Cambridge Faculty of Law Research Paper No. 49/2015, Cambridge, 2015

[8]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) (Text with EEA relevance) OJ L 39, 12.2.2010, p. 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 (Text with EEA relevance) (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 of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271)Text with EEA relevance OJ L 385, 29.12.*2004*, p. 74–84

[9]The list of states deemed to ensure the adequate level: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm e.g. AD, AR, CA, FO, GG, IL. Before the accession Hungary was also the member of this list.

[10]Official Journal L 215 , 25/08/2000 P. 0007 - 0047

[11] R. J. PELTZ-STEELE: The pond betwixt: differences in the US-EU data protection /Safe Harbour Negotiation, *Journal of Internetlaw*, vol. 19. no. 1., 2015 July, pp. 15-30.

[12]It is closes to the European concept of dignity.

[13] R. J. PELTZ-STEELE 2015, pp. 25.

[14]SZŐKE, Gergely László: *Az európai adatvédelmi jog megújítása – Tendenciák és lehetőségek az önszabályozás területén*, HVG-ORAC Lap- és Könyvkiadó Kft, Budapest, 2015 and SZIGETI Tamás: Az információs hatalom korlátozása tengeren innen és túl, Infokommunikációs jog 4. szám. pp. 159 – 165.

[15] SZŐKE 2015, pp. 52-54.

[16] SZŐKE 2015, pp. 92-115.

[17]Safe Harbour Decision Annex III

[18]Safe Harbour Decision Article 1 para. 2

[19]Safe Harbour Decision Annex I

[20]https://safeharbor.export.gov/list.aspx [16/2/2016]

[21] Communication COM(2013) 846 final, Communication COM(2013) 847 final

[22]C-362/14 point 29.

[23]BCRs has not been well-recognized as European national jurisdictions did not know this legal mean but more and more companies has applied one parallel with its enactment e.g. ABN Amro Bank, Deutche Telekom, Hermés, Michelin, Sanofi Aventis ... etc. Check the growing list of the companies: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm [18/2/2016]

[24] An independent advisory body of the Commission. Every mem ber state delegate a representative, the Hungarian member is Dr. Attila Péterfalvi, the president of the national data protection Authority (NAIH).

[25] See: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2003_en.htm

[26] http://register.consilium.europa.eu/doc/srv?f=ST+5853+2012+INIT&l=en [18/2/2016]

[27] http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm [18/2/2016]

[28] R. J. PELTZ-STEELE 2015, pp. 21.

[29] László Sólyom introduced this concept into the Hungarian literature upon German sample. in the journal of *Valóság* in 1988. Sept.

[30] LAUDON, Kenneth C.: Market and Privacy, Working Paper Series, STERN IS-93-21, Centre for Digital Economy Research, 1993

[31] For details see: R. J. PELTZ-STEELE 2015, pp. 19.

[32] https://epic.org/privacy/white_house_consumer_privacy_.html [18/2/2016]