MultiScience - XXXI. microCAD International Multidisciplinary Scientific Conference
University of Miskolc, Hungary, 20-21 April 2017
ISBN 978-963-358-132-2

CONCEPTS AND RULES IN THE GENERAL DATA PROTECTION REGULATION

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

INTRODUCTION

Since 2012 the legal framework of personal data protection has gone through major reform, globally. Resulting from the growing operation of the internal market of the EU, the economic and social integration with the rapidly changing technological developments and globalisation have led to increased needs of cross-border flows of personal data. This progress has brought new challenges and required a strong and more coherent data protection framework in which legal and practical certainty for natural persons, economic operators and public authorities should be enhanced. As the 96/45/EC Directive was failed to prevent from fragmentation in the implementation of data protection rules across the EU and the Safe Harbour decision with regard to the data transfers to the US was also declared invalid by the Court of Justice of the European Union, the level of protection in all Member States and the transfers to third countries can only be provided with equivalent protection if comprehensive and clear rules of enforceable rights and binding obligations are to be directly applied with the opportunity for effective remedy and sanctions imposable on the breaching party. Having these in mind the *REGULATION (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* (hereinafter: GDPR) was adopted in April 2016. This study analyses how the rules of GDPR meet the requirements of the above-noted aims and needs to be well-prepared for its application from 25th May 2018. In addition, an attempt is made to examine how the latest trends of data protection are incorporated in the certain rules of it.

1. STEPS TO PREPARE

However the main principles and concepts of Directive 95/46/EC remain sound, there are new elements and significant enhancements in GDPR which will be directly applicable in all member states. The GDPR emphasises a new governance model of strong DPAs along with increased co-operation of the controllers and processors to turning data protection 'from a paper existence into a reality'.[2]

[1] The author is PhD student in Deák Ferenc Doctoral School of Political Science and Law, University of Miskolc. Contact: jogmakso@uni-miskolc.hu
[2] Wright, David, De Hert, Paul (Eds.): Enforcing Privacy Regulatory, Legal and Technological Approaches, Issues in Privacy and Data Protection, Series Volume 25, Springer International Publishing, 2016. 1-5. pp.

DOI: 10.26649/musci.2017.104

To help the preparation many national data protection authorities (hereinafter: DPA), inter alia the Hungarian[3] and the UK[4] ones, have issued a compilation of 12 steps in order to facilitate in finding which parts of the GDPR will have the greatest impact:

1. Being aware of the changing legal environment;
2. Audit and document the data held by the controller;
3. Reviewing and communicating privacy policy;
4. Checking procedures to ensure the rights of data subjects;
5. Updating procedures and plan how to handle requests;
6. Identify the legal basis for control and process;
7. Reviewing how to seek, obtain and record consent of the data subject;
8. Realizing special protection on children;
9. Reviewing procedures to detect, report and investigate a personal data breach;
10. Implementing Data Protection by Design and Impact Assessments;
11. Data Protection Officer to be appointed and trained;
12. Determining of which DPA's jurisdiction under the controller is.

2. TENDENCIES INCORPORATED

As it is clear from the above listed-steps, the general philosophy of the GDPR is based upon the latest requirements of personal data protection deriving from the *need of strict consciousness* of controllers. GDPR expands its scope of application outside the geographical territory of the EU and introduces obligations with severe sanctions on processors directly[5] so that controllers and processors need easily applicable and clear rules to be able to comply. I must note at this point that *the definition of the activity of the processor is neither incorporated in the Directive, nor in the GDPR*, unlike the Hungarian Act CXII of 2011 on Informational Self-Determination and Freedom of Information. Data subjects need[6] for enforceable rights, also the protection of a high standard and effective opportunity for remedy are supported in the GDPR, but making controllers interested in data protection has got bigger emphasis. To prove this statement let's have a look at Article 83 pursuant to which *administrative fines* up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, can be imposed on the breaching controller or processor in case of intentionally or negligently committed infringement, of the same or linked processing operations.
According to some details stated above *three new tendencies can be recognized easily*: Firstly the supported methods of co- and self-regulation with a strong emphasis on privacy by design and impact assessments in order to prevent from

[3] NAIH: Felkészülés az Adatvédelmi Rendelet alkalmazására 12 lépésben http://naih.hu/felkeszueles-az-adatvedelmi-rendelet-alkalmazasara.html [2017.02.06.]
[4] ICO: Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf [2017.02.06.]
[5] Hazel Grant, Amy Lambert, Kate Pickering: Data Protection Day—data processors and the GDPR http://www.fieldfisher.com/publications/2016/02/data-protection-day-data-processors-and-the-gdpr#sthash.pbVmLTrz.dpbs [2017.02.04.]
[6] According to the latest survey of Eurostat (2015) 89% of the participants believed that the protection of personal data should not be limited by state borders and have the same level of protection over their personal information, regardless of the country in which the process of their data is based. http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf

incidents in advance and generally encourage consciousness of controllers, processors and data subjects - instead of listing rights for the data subject which are unable to remedy the breach after its occurrence -. Secondly regulating data flows towards third countries and thirdly the more effective cooperation of DPAs with each other and with the private sector controllers and processors can be realised by examining the certain sections.

2.1. Supported methods for increased consciousness

2.1.1. About the methods

The success of regulations depends on the nature of the rules, the efficiency of implementation and the willingness to obey. As loopholes can occur and legal regulation can be difficult to apply which come to light in practice both data subjects and data controllers need subsidiary solutions. *Co- and self-regulation* can serve as a complement to legislation but cannot substitute it. [7] These rules are flexible enough to quickly adapt to changing technological, economic, structural changes and incorporate new technologies. To strengthen trust between organizations and their consumers it is a good way to state obligations themselves by increasing the will of obedience. Co-regulation means the joint administration of the regulation by industry and government. Self-regulation is a regulatory process during which organizations which represent an industrial sector set and enforce rules or rather standards relating to the conduct of companies in the certain field. The distinction between the two types may blur in practice. In this aspect, the *Binding Corporate Rules represents a mixed type* of regulation as it is created and applied by a certain group of undertakings and authorized by the national DPA.
Privacy by design means that the controller should adopt internal policies and implement measures to be taken into account the right to data protection when developing or designing products and services.
The support of these methods can be discovered in certain rules of GDPR.

2.1.2. Pursuant to the GDPR

Article 25 states that the controller shall implement appropriate technical and organisational measures to integrate the necessary safeguards into the processing. The GDPR set as a default rule in Article 37 the designation of the *data protection officer*. Public authorities, controllers or processors, dealing with processing operations which require regular and systematic monitoring on a large scale and which require special categories of personal data and data relating to criminal convictions and offences, shall appoint such a person on the basis of professional qualities, expert knowledge and practices. The officer may be a member of the controller or processor, or can fulfil the tasks on the basis of a service contract, but does not receive any instructions so functions as an internal supervisory entity to inform, advise and monitor compliance.

---

[7] For a detailed explanation see: Daniel Castro: Benefits and Limitations of Industry Self-Regulation for Online Behavioural Advertising, ITIF, 2011 pp. 1-3 http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf [2017.01.05.]

The EU legislator in Section 5 gives special priority for *Codes of conduct and certification*. In contrast, the Directive only situates them as a sector-specific method to facilitate the application of the Directive. These codes can be defined as self-regulation as the rules, prepared by associations and other bodies representing categories of controllers or processors, are taking account of the characteristics of the processing carried out in the certain sector. Without prejudice to the tasks and powers of supervisory authorities, mechanisms shall be created which enable the body with an appropriate level of expertise in relation to the subject-matter to carry out the mandatory monitoring of compliance with the provisions of the codes.
Pursuant to Article 42 GDPR encourages the establishment of data protection certification mechanisms with validated evaluation procedure[8] and data protection *seals and marks*, for the purpose of demonstrating compliance, although seals mean recent compliance with the inherent need for periodic supervision. For instance, during 2016 the UK's Information Commissioners Office established the Privacy Seals[9] which is a symbol of quality and high standard of data protection. ICO will approve third parties to deliver ICO privacy seal schemes. Schemes focusing on different sectors. Potential scheme operators must be accredited by the national accreditation service. Once ICO endorsed, the scheme operators will be responsible for the day to day running of the scheme. Organisations wishing to apply for an ICO privacy seal will then have to make an application to a scheme operator. Then if the organisation shows that they meet the operator's assessment criteria, it will be awarded an ICO privacy seal. Once awarded, the organisation can use the seal externally to show the application of best practice. In addition, the CNIL in France and DPA from Schleswig-Holstein has also established voluntary privacy seals but the first pioneer was Japan.[10]

2.1.3. In the US

Although self-regulation in the EU has been promoted lately, in the US without few exceptions projects generally did not last long nor gained big success. Industry-supported self-regulations were created and maintained without enough transparency, covered only a fraction of an industry or a sub-group, operating organisations were short-lived with limited scope, although they were highly promoted.[11] Other self-regulatory frameworks with government involvement existed longer. Safe Harbour Decision on the data transfers from the EU to the USA was only declared invalid in October 2015 after its approval by the EU Commission in 2000. The biggest comments on its running were the low rate of compliance and the lack of supervision. In addition, the Curia[12] added that without administrative or judicial means of redress and a legislation that compromising the essence of the fundamental right to respect for private life the adequate level of protection cannot be deemed ensured.

---

[8] Kirsten Bock: Data Protection Certifi cation: Decorative or Effective Instrument? Audit and Seals as a Way to Enforce Privacy In Wright, David, De Hert, Paul (Eds.): *Enforcing Privacy Regulatory*, Legal and Technological Approaches, Issues in Privacy and Data Protection, Series Volume 25, Springer International Publishing, 2016
[9] https://ico.org.uk/for-organisations/improve-your-practices/privacy-seals/ [2017.01.05.]
[10] Bock 2016 pp. 335.
[11] Robert Gellman, Pam Dixon: Failures of Privacy Self-Regulation in the United States In Wright, David, De Hert, Paul (Eds.): *Enforcing Privacy Regulatory*, Legal and Technological Approaches, Issues in Privacy and Data Protection, Series Volume 25, Springer International Publishing, 2016.
[12] http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf [2017.02.05]

Its ancestor, the Privacy Shield is also a voluntary framework to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements.[13] If an eligible private sector entity makes the commitment to comply with the Shield's requirements, it will become enforceable under U.S. law or such organizations can commit to cooperate with European DPAs. Participating organizations are deemed to provide adequate protection which is a key requirement for data transfers outside of the EU under the Directive and the GDPR as well. Referring that the Privacy Shield has just started operation, real advantages will be seen in the future. So far in a half-year-long period 1666 organisations have joined,[14] in contrast Safe Harbour counted more than 5000 companies[15] in fifteen years.
Several attempts of self-regulation with the participation of government, industry, academia and civil society were succeeded but not in long term without a wide focus. *These efforts were rather promoted than really applied* because the standard of obedience was poor and there was not a proper supervisory mechanism.

3. DATA FLOWS TOWARDS THIRD COUNTRIES WITH CO-REGULATION

There is growing number of data transfers as a result of to the intensifying transatlantic and other relations to third countries, mainly in the digitalized economy. However EU data protection legislation is considered to be an extraterritorial jurisdictional regime[16] in practise and DPAs should exercise jurisdiction on data controllers operating in third countries,[17] the existence of adequate protection and effective remedy highly depends on the cooperation of the DPA – if there is one – in the third country. To avoid this risk EU legislator makes attempts to ensure protection with applying methods to make the data controller involved.
As the Directive does, the GDPR also applies the approach to *export its principles and policies into the operation of the data controllers in third countries*. Article 44 declares that any transfer shall take place only if the conditions laid down in GDPR are complied with by the controller and processor in the third country. The key condition is the existence of adequacy of the level of protection which is assessed by certain elements listed in Article 45 para. 2. The required result of this assessment was defined in Case C-362/14[18] point 74 according to which the means to which that third country has recourse may differ from those employed within the EU but those means must nevertheless prove, in practice, effective essentially equivalent. Besides the solution of transfers on the basis of an adequacy decision made by the Commission data controllers can transfer data if appropriate safeguards are provided and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Appropriate safeguards are listed in Article 46 para. 2. As a proof of co-regulatory approach, three out of the six solutions are a kind of self- or co-regulatory methods like the binding corporate rules and the approved certification mechanism in Article 40 and Article 42.

---

[13] https://www.privacyshield.gov/Program-Overview [2017.02.05]
[14] https://www.privacyshield.gov/list [2017.02.05]
[15] https://safeharbor.export.gov/list.aspx [2017.01.10.]
[16] 7KUNER, Christopher: Extraterritoriality and Regulation of International Data Transferring EU Data Protection Law, University of Cambridge Faculty of Law Research Paper No. 49/2015, Cambridge, 2015
[17] Refferring to Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner national DPAs must be able to examine, with complete independence, whether the transfer of a person's data to a third country complies with the EU legislative requirements.
[18] ECLI:EU:C:2015:650

One of the biggest advantages of these methods is the flexibility as they can be tailored in a way that the data controller needs, structure and practise require. After their approval, they can be applied without requiring any further specific authorisation from a supervisory authority. As the GDPR makes a differentiation in relation to the approach of third country transfers among the third country, a territory or one or more specified sectors within that third country, or the international organisation in question, these methods can also be separated on the preference of the certain data controller. Furthermore, GDPR in preamble 37 also declares the definition of a group of undertakings which should cover a controlling undertaking and its controlled undertakings, the interpretation of data controllers or processors running in third countries are also become more obvious.
In conclusion, the data controller in the EU which transfers personal data from the EU towards a third country have to ensure the adequate level of protection in the certain third country. If the third country does not ensure that protection by laws and authorities then the data controller shall do that itself, internally, by applying the above details means of self- or co-regulation like binding corporate rules or approved clauses. Having this in mind the adequate level of protection required by EU law is ensured and the jurisdictions of one or more EU national DPAs are also guaranteed. *Binding Corporate Rules* regulated in Article 47 *has seemed to be the most supported model* for the mixed type of regulation as it involves the strong cooperation of the group of undertakings as data controllers and the relevant national DPAs during its authorization and it ensures compliance and the acceptance of liability for any breaches by the controller or processor established on the territory of the EU, under a jurisdiction of a national DPA. Its rules are binding for the members of the group in third countries ensuring adequate level at the certain data controller. In other words, BCR is adopted at the level of the data controller, the scope of it does not extend to the whole country or the sectors of industry but enjoys stronger obedience.

4. COOPERATION WITH DPAS

The consciousness of data controllers comes with the intensive cooperation with the DPAs. The creation of the best practise of the consistent application of the GDPR requires that each national DPA shall contribute throughout the EU pursuant to Article 51 para. 2. The authorization processes of code of conducts and Binding Corporate Rules are only one element of the increased collaboration in which DPAs in the mutual recognition regime and the lead authority with the data controller must evolve successful cooperation.
Also, there is a binding notification obligation on controllers and processor. According to Article 33 and 34 processors have to notify the controllers and controllers have *to notify the personal data breach to the supervisory authority* - and the data subject as well - without undue delay or a reasoned notification in case of more than a 72-hour-delay.
The data protection officer should be in a position to perform effective communication with the DPA and act as the contact point for the supervisory authority.

In case a data-protection impact assessment indicates that processing operations involve a high risk, *a consultation of the supervisory authority* should take place prior to the start of processing activities. Because of these binding obligations it is a key preparatory element to determine of which DPA's jurisdiction under the controller is.

5. BOTTOM LINES

As GDPR will be directly applicable in the Member States all participants of processing activities need preparation to be aware of the rules which have an unaccustomed approach towards data protection. What is more, it may have a high cost of any breach or omission.
The application of the rules of GDPR will not definitely be easy as it implements new methods which are unusual in this sector among European data controllers as the Directive does not exclude these forms, but rather just positively supports them.[19] However foreign samples of co- and self-regulation are available, they are mostly ended up with little success. Furthermore, there is no judicial case law concerning these supplementary methods like the code of conducts.
Obligations imposed on the data controllers and processors facilitate to prevent from data breaches and the extended jurisdiction of DPAs helps more effective remedy. The general approach puts the emphasis on the full compliance of the data controller rather the need of active participation of the data subject which is a supportable and more effective way of regulation.

[19] Dr. Balázs Rátai, Dr. Tamás Szádeczky, Dr. Gergely László Szőke: Implementing And Audit Of The Codes Of Conduct, DECEMBER, 2012 http://pawproject.eu/en/sites/default/files/page/implementing_and_audit_of_coc.pdf [2017.01.05.]