Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 32

The 2018 Buzzword: "GDPR", and how it practically affects corporations in the EU and the US

Nikolaos Theodorakis

2018

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology-related and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Nikolaos Theodorakis is a Lecturer and Fellow at the University of Oxford and a senior associate with Alston & Bird LLP, focusing on issues of privacy and data protection, technology, international trade law and competition law.
Nikolaos completed his Ph.D. at the University of Cambridge, where he focused on issues of Corporate Compliance, Liability and Regulation. He also holds degrees from the University of Athens (LL.B.), University of Cambridge (M.Phil.), University of Oxford (PGC), London School of Economics (B.Sc.) and University College London (LL.M.).
Prior to joining Oxford, Nikolaos taught and conducted research at the University of Cambridge, Harvard Law School, and Columbia Law School. Nikolaos has further worked for the U.S. Committee on Capital Markets Regulation, the Legislative Committee at the U.S. Congress and the Library of Congress, and the UK Sentencing Council. Nikolaos has received fellowships and awards from the ESRC, the British Academy, the Greek Parliament, the Greek State Scholarships Foundation, the EU Bursaries and the Corfield foundation, among others. He has published papers on various topics and presented extensively in conferences and symposia.
Nikolaos's recent engagements include serving as a UN international consultant and legal trainer, an OECD expert, an EU Commission international expert, and a Transparency International country assessor. In the past he has also assumed research and teaching fellowships with Harvard University, the Institute of Advanced Legal Studies at the University of London, the British Institute of International and Comparative Law, and the Max Planck Institute of Foreign and International Criminal law.

General Note about the Content

The opinions expressed in this paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This TTLF Working Paper should be cited as:
Nikolaos Theodorakis, The 2018 Buzzword: "GDPR", and how it practically affects corporations in the EU and the US, Stanford-Vienna TTLF Working Paper No. 32, http://ttlf.stanford.edu.

Copyright

Abstract

The EU General Data Protection Regulation (GDPR) was adopted in 2016, and will formally enter into force on 25 May 2018. It is the biggest change in data protection legislation that has been introduced in the past 20 years. It aims to better regulate the fields of privacy and data protection and at the same time catch up with significant technological developments that have occurred over the past decades. Corporations both in the EU and the US, given GDPR's extraterritorial reach, are working towards compliance. Besides, administrative sanctions can reach up to reach up to 4% of their global revenue, or $24m (€20m), whichever is higher.

This paper will briefly discuss the current status quo of data protection rules in the EU and the US and will then attempt to decipher certain key elements of the GDPR. It will discuss (i) the data subjects' rights and, in particular, the right to data portability, (ii) the concept of the Data Protection Officer (DPO), (iii) the notion of accountability, using Binding Corporate Rules (BCRs) as an example, (iv) the lead supervisory authority, and (v) specific processing challenges for employers like data processing at work.

Keywords: GDPR; General Data Protection Regulation; EU data protection; privacy; technology

Table of Contents

1. Introduction

The EU General Data Protection Regulation (GDPR) was adopted in 2016, and will formally enter into force on 25 May 2018. It is the biggest change in data protection legislation that has been introduced in the past 20 years. It aims to catch up with recent developments and at the same time to provide a regulatory landscape for upcoming technological development. In doing so, GDPR introduces several novel features that no other privacy related regulation contains. In the same fashion, it signals to corporations on both sides of the Atlantic that compliance is the only option since fines can reach up to 4% of their global revenue, or $24m (€20m), whichever is higher.

In preparation of the enforcement of the GDPR, several corporations are puzzled regarding specific requirements, and how they will be implemented in practice. Since the GDPR has an extraterritorial reach, it does not only apply to EU businesses, but also to any business worldwide that either processes EU personal data, or envisions to offer goods or services to EU residents.[1] Understandably, the wide applicability of the GDPR, and the vagueness as to how certain principles will be interpreted, is puzzling companies in the EU and the US.[2]

This paper will briefly discuss the current *status quo* of data protection rules in the EU and the US and will then attempt to decipher certain key elements of the GDPR. It will discuss (i) the data subjects' rights and, in particular, the right to data portability, (ii) the concept of the Data Protection Officer (DPO), (iii) the notion of accountability, using Binding Corporate Rules (BCRs) as an example, (iv) the lead supervisory authority, and (v) specific processing challenges for employers like data processing at work. More issues of interest, like breach notification, rules for data storage and erasure, and overall update of data governance policies may be addressed in future research.[3]

2. Transatlantic Data Protection Rules

Data Protection rules have been through significant changes in both the EU and the US over the past years. For instance, in the US there is no single, comprehensive federal law regulating the collection and use of personal data. Instead, the US has various state laws and regulations that may sometimes be overlapping. Guidelines and other self-regulatory

[1] Brendan Van Alsenoy, 'Reconciling the (extra)territorial reach of the GDPR with public international law' in Gert Vermeulen and Eva Lievens (eds), *Data Protection and Privacy under Pressure: Transatlantic tensions, EU surveillance, and big data* (Maklu 2017)
[2] Mark Foulsham and Brian Hitchen, *GDPR: Guiding Your Business To Compliance: A practical guide to meeting GDPR regulations* (Independently Published 2017)
[3] Darren Wray, *The Little Book of GDPR: Getting on the Path to Compliance* (Independently Published 2017)

instruments are also considered best practices- they have accountability and enforcement components that are increasingly being used as a tool for enforcement by regulators.[4]

There are certain federal privacy-related laws that regulate the collection and use of personal data in several sectors. For instance, some apply to particular categories like health information (HIPA- Health Insurance Portability and Accountability Act), credit reports (FCRA- Fair Credit Reporting Act) and electronic communications (ECPA- Electronic Communications Privacy Act). In addition, there are wide consumer protection laws that are not privacy laws *per se*, but have been used to prohibit unfair or unlawful processing of personal data.

Few US states recognize an individual's right to privacy, a notable exception being California. The right to privacy is provided both in the California Constitution and in several pieces of legislation. The California Online Privacy Protection Act (OPPA) also provides requirements on operators who collect personal information. Recently, lawmakers have proposed legislation to amend the way online businesses handle user information. For instance "Do Not Track" aims to protect more the individuals' privacy, however there has been no successful legislation that implements it yet.[5]

The EU approach to data protection is quite different, and this discrepancy creates challenges for how the digital market operates across border. The EU mostly bases its privacy legislation on the European Directive on Data Protection, introduced in 1995. A dated piece of legislation nowadays, the Directive will be replaced by the EU General Data Protection Regulation (GDPR, Regulation 2016/679) in May 2018. This will be the most important change in data privacy regulation in twenty years. This Regulation is the EU's response to

[4] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017)
[5] Mark Foulsham and Brian Hitchen, *GDPR: Guiding Your Business To Compliance: A practical guide to meeting GDPR regulations* (Independently Published 2017)

rising users' concerns about their privacy. In a recent EU survey, 72% of Internet users in Europe still worry that they are being asked to provide too much personal data online.[6]

For the purpose of bridging the different privacy approaches between the US and the EU, and to comply with the existing Directive, the U.S. Department of Commerce jointly with the European Commission developed a "safe harbor" framework. This framework recognized the US as an adequate country to transfer data, under certain safeguards. The safe harbor was later invalidated by the European Court of Justice. It was subsequently replaced by the EU-US Privacy Shield Framework, the validity of which is also currently disputed in the EU courts. This debate indicates the different approach that the EU and the US have with respect to personal data, but at the same time their common interest of facilitating data flows for trade purposes.[7]

The GDPR is intended to make citizens masters of their personal data, and to simplify the regulatory environment for international businesses. Personal data may range from a name, to a photo, email address, bank details, or a computer's IP address. The regulation applies to data controllers, data processors, and data subjects who are based in the EU. It provides for harmonization of data protection regulations throughout the EU and includes a strict data protection compliance regime. The regulation does not extend to the processing of personal data for national security activities or law enforcement, however. For this purpose, an EU Directive on Law Enforcement explicitly regulates such processing for national security purposes. [8]

The GDPR implementation is still a question since it requires wide ranging changes of business practices and a new mentality for companies that need to introduce privacy by

[6] *See:* https://ec.europa.eu/commission/sites/beta-political/files/dsm-factsheet_en.pdf
[7] Jef Ausloos, 'Balancing in the GDPR: legitimate interests v. right to object' (2017) https://lirias.kuleuven.be/handle/123456789/586231
[8] Darren Wray, *The Little Book of GDPR: Getting on the Path to Compliance* (Independently Published 2017)

design and by default in their operations. The most interesting aspect is certainly the GDPR's extraterritorial application, since it can apply even to US companies that process EU personal data.

In any event, the GDPR is changing the way companies process, transfer and otherwise use personal data. The EU-US digital market connection is becoming increasingly challenging, in terms of compliance, because of the regulatory chasm. The new Regulation creates significant opportunity to protect and grow the digital market, yet at the same time compliance efforts might stall progress.

3. Indicative GDPR Issues

Several companies in the EU and the US are concerned with a number of issues in light of the GDPR, namely (i) the data subjects' rights (ii) the concept of the Data Protection Officer (DPO), (iii) the notion of accountability (iv) the lead supervisory authority, and (v) specific processing challenges. The following subsections will discuss these issues in detail.[9]

3.1. Right of Data Portability for data subjects

The GDPR introduces a new right to data subjects regarding data portability. In essence, the data subject can request to receive their personal data in a structured, commonly used format. They can then choose to either keep their data, or transmit them to a new controller. For instance, a data subject can ask his bank to transfer all his data to another bank, in preparation of account immigration. This is a new concept, certainly in the US where privacy laws only recognize the right to access and correction.[10]

[9] Andreas Linder, *European Data Protection Law: General Data Protection Regulation 2016* (CreateSpace 2016)

[10] Article 29 Working Party Opinions and Recommendations, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm, accessed 12 February 2018

Article 20 (1) of the GDPR reads *"[t]he data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the data have been provided […]*" To facilitate the process of granting data portability rights, the Article 29 Working Party (WP29) has issued guidance that discusses the particulars of data portability, the conditions under which the right applies, and how it interact with other GDPR rights.

3.1.1. Elements of Data Portability

There are five key elements that employers should be aware of when granting data portability rights:[11]

- *"Right to receive personal data:"* The right to receive personal data in a structured, commonly used and machine-readable format.

- *"Right to transmit personal data from one data controller to another:"* This permits a data subject to transmit personal data from the controller to another.

- *"Data portability tools:"* Corporations should give the data subject the option between directly downloading his or her data, and having the data controller transfer the data to another data controller.

- *"Controllership:"* The GDPR rights do not oblige the data controller to retain the personal data for longer than required to deliver the service. In other words, there is

[11] Orla Lynskey, 'Aligning data protection rights with competition law remedies? The GDPR right to data portability' (2017) European Law Journal [*in press*] ISSN 1351-5993

no requirement to retain data only for the possibility that an individual may wish to exercise their right in the future.[12]

- *"Data portability vs. other rights of data subjects:"* This means that exercising the right to data portability does not hamper, or otherwise affect, the other rights that the GDPR recognizes. For instance, a data controller cannot delay or refuse another data subject's request just because they are dealing with a data portability request at the same time.

3.1.2. When and How Data Portability Applies

The right to data portability applies when the data controller has received information based on the data subject's consent, or in the context of a contract. Data portability only applies to processing carried out by automated means. Further, compliance with one data subject's right to data portability is not meant to generate any adverse effects on the rights and freedoms of others.

The controller is not required to provide intellectual property or trade secrets; in case the data portability request involves data in files that include such sensitive information, the corporation would need to transfer the personal data in a form that excludes information related to intellectual property or trade secrets. [13]

In terms of practical compliance, companies that are subject to the GDPR are expected to update their privacy notices so that they reflect this new right. When providing for this right, it should be mentioned separately from other rights and it should be clear. Corporations are expected to respond to a request within one month of receipt, or three

[12] Andreas Linder, *European Data Protection Law: General Data Protection Regulation 2016* (CreateSpace 2016)
[13] Orla Lynskey, 'Aligning data protection rights with competition law remedies? The GDPR right to data portability' (2017) European Law Journal [*in press*] ISSN 1351-5993

months for particularly complicated cases; in the latter scenario, they need to promptly inform the data subject of the reasons that cause this delay.

Another practical difference is that companies must not charge fees for providing personal data unless they can demonstrate that the requests are unfounded or excessive, primarily because of their repetitive character.[14]

3.2. Data Protection Officer Obligations

Under certain circumstances, companies are required to appoint a Data Protection Officer (DPO). This is a novel notion that companies both in the EU and the US will need to carefully consider. Multinationals, particularly in the US, are not very much acquainted with the concept of the DPO, yet this is about to change.[15]

3.2.1. Obligation to Appoint a DPO

GDPR requires companies to appoint a DPO when (1) their "core activities" involve (2) "regular and systematic monitoring" on (3) a "large scale." It also requires them to appoint a DPO when their "core activities" consist of "large scale" processing of sensitive data or criminal convictions. However, even companies that are not required to appoint a DPO may voluntarily appoint one to demonstrate their commitment to accountability.[16]

- "Core activities" are defined, according to WP29, as the operations that are required to achieve the goals of the company. This does not include ancillary functions, or supportive functions (e.g. IT support);

[14] David Flint, 'Storms Ahead for Cloud Service Providers', (2017) 38(3) Business Law Review 125–126
[15] Irene Loizidou Nicolaidou and Constantinos Georgiades, 'The GDPR: New Horizons' in Tatiani-Eleni Synodinou, Philippe Jougleux, Christiana Markou, Thalia Prastitou (eds), *EU Internet Law* (Springer 2017)
[16] Article 29 Working Party Opinions and Recommendations, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm, accessed 12 February 2018

• "Regular and systematic monitoring" includes all forms of tracking and profiling on the internet. Such monitoring can be quite wide and include online behavioral advertising and loyalty programs. includes all forms of tracking and profiling on the internet.

• "Large scale" can either relate to the number of data subjects that are affected by a processing activity, or the volume of the data processed, or the duration of such processing, or the geographical extent of processing.

3.2.2. Requirements for the DPO Position

When structuring the DPO position, companies must take into consideration a number of factors so that they appoint the most suitable person.

DPOs must be personally available to the company's supervisory authority (SA), local EU data subjects, and company employees. Also, the DPO's expertise should be commensurate with the sensitivity, complexity and amount of data a company processes.

A DPO can be either an internal employee or an external firm, depending on the company's preference. However, companies should be careful not to appoint a person that may have a conflict of interest in determining his required tasks. DPOs are particularly important when decisions that have data protection implications are taken, and in data breach incidents.[17]

In any event, the DPO must maintain his independence and cannot be dismissed or penalized for performing his tasks. Further, the company must support him in performing his tasks by, for instance, providing sufficient time, continuing training, and internal resources to

[17] Irene Loizidou Nicolaidou and Constantinos Georgiades, 'The GDPR: New Horizons' in Tatiani-Eleni Synodinou, Philippe Jougleux, Christiana Markou, Thalia Prastitou (eds), *EU Internet Law* (Springer 2017)

allow him fulfill his tasks. The more complex the processing operations are, the more resources need to be invested in the DPO.[18]

DPOs are permitted to consult a SA on any matter they deem appropriate and are bound by confidentiality within the performance of their tasks. WP29 clarifies that DPOs are not personally responsible for non-compliance with the GDPR. It is the corporation who remains liable, however this may be challenged in cases where the corporation can demonstrate that the DPO neglected his obligations.

Taken together, these requirements create a substantial amount of work for companies to accomplish in light of the GDPR. [19]

3.3. Demonstrate Maximum Accountability: Binding Corporate Rules

The GDPR requires companies to demonstrate full accountability, to prove that they have a solid and compliant privacy program in place, and incorporate the principles of privacy "by default" and "by design". This practically means that a corporation needs to embed privacy in its corporate architecture, and enforce it through every company level. Further, companies need to ensure that they have an adequate data transfer mechanism when they transfer, or onward transfer, data outside the EU. The Binding Corporate Rules are, therefore, the golden measure in demonstrating accountability and compliance with the GDPR.[20]

Binding Corporate Rules are an intracompany code of conduct that regulates the principles and rules that apply to the processing and transfer of personal data within a

[18] Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR' (2017) Harvard Journal of Law & Technology [*in press*]
[19] Darren Wray, *The Little Book of GDPR: Getting on the Path to Compliance* (Independently Published 2017)
[20] Runshan Hu, Sophie Stalla-Bourdillon, Mu Yang, Valeria Schiavo, and Vladimiro Sassone, 'Bridging Policy, Regulation, and Practice? A Techno-Legal Analysis of Three Types of Data in the GDPR' in Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth and Paul De Hert (eds), *Data Protection and Privacy: The Age of Intelligent Machines* (Hart Publishing 2017)

company group, including cross-border. BCRs were established through the standard practice of data protection authorities (DPAs) and the guidance of the Article 29 Working Party (WP29). The upcoming General Data Protection Regulation explicitly recognizes BCRs,[21] both for controllers (BCR-C) and processors (BCR-P). It also extends the scope of application not only to a corporate group but also to a group of enterprises engaged in a joint economic activity,[22] for instance joint ventures.[23]

After WP29 endorsed BCR-C as a useful mechanism for data transfers of complex international structures in 2003, several companies adopted them. Instead of having to justify international transfers on an individual basis, and concluding model contracts with numerous parties, BCRs allow a single set of transfer rules for the entire company group. In today's interconnected world, it is increasingly important to easily transfer data wherever needed, and BCRs offer the flexibility required for such elaborate transfers.

A framework for BCR-Ps was introduced much later, in 2012, and their further inclusion in the GDPR was fiercely debated. In endorsing their inclusion, WP29 praised the merits of BCR-P as an optimal solution for international data transfers. At the same time, WP29 held that BCR-P provides more transparency and accountability requirements beyond those provided in model clauses or other transfer mechanisms (e.g., the current Privacy Shield).

To date, 88 companies have had their BCR procedures concluded, 10 of them pertinent to BCR-Ps. This number is expected to rapidly increase in light of the GDPR and the several benefits associated with BCR:

---

[21] Regulation (EU) 2016/679 of the European Parliament, the Council of the European Union and the European Commission (GDPR) [2016] art 47

[22] Regulation (EU) 2016/679 of the European Parliament, the Council of the European Union and the European Commission (GDPR) [2016] recital 110

[23] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017)

3.3.1. Increased Flexibility

BCRs will become more flexible under the GDPR. Under the current regime, countries have to first approve their BCRs in all relevant countries through mutual recognition or a cooperation procedure.[24] They still need to obtain national DPA authorizations in certain countries to allow for the transfer of personal data under the BCRs. These transfer permits only allow specific transfers, and any time a company wants to expand or alter its transfers, a new notification and permitting procedure is required. Making things more complicated, BCRs are not recognized in Portugal as a valid legal basis to transfer personal data outside of the European Economic Area (EEA).[25]

The GDPR does not contain DPA notification and authorization requirements for data transfers. National authorizations of BCRs will be abolished, which will significantly reduce the time required to introduce a BCR and will increase flexibility altogether. Because of the direct applicability of the GDPR in all EU member states, any remaining inconsistencies (e.g., Portugal) will be automatically ironed out. As a result, processors will likely increasingly rely on BCR-Ps to justify transfers outside the EEA since they will be able to engage in practically unlimited data transfers within their company groups.

3.3.2. Demonstrate Accountability

Under the GDPR, the data transfer rules are also directly applicable to processors. Processors should, therefore, no longer be dependent on data transfer mechanisms put in

[24] Pieter Wolters, 'The security of personal data under the GDPR: a harmonized duty or a shared responsibility?' (2017) 7(3) International Data Privacy Law 165–178

[25] Runshan Hu, Sophie Stalla-Bourdillon, Mu Yang, Valeria Schiavo, and Vladimiro Sassone, 'Bridging Policy, Regulation, and Practice? A Techno-Legal Analysis of Three Types of Data in the GDPR' in Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth and Paul De Hert (eds), *Data Protection and Privacy: The Age of Intelligent Machines* (Hart Publishing 2017)

place by controllers, but rather have their own tools available to comply with these requirements. Besides, WP29 has indicated that a BCR is an organizational accountability tool that has many merits beyond contractual solutions such as the EC model clauses.[26]

For intragroup transfers, BCRs not only provide a good basis for transfers but also help demonstrate broader compliance with the GDPR, for instance the principles of accountability,[27] lawfulness of processing,[28] general processing requirements,[29] and security of processing.[30]

3.3.3. Meet the By-Default and By-Design Requirement and Avoid High Fines

GDPR refers to the requirement of ensuring data protection by design and by default.[31] Therefore, companies should introduce appropriate technical and organizational measures so that all the data protection principles are met. This is a relatively wide concept, and high GDPR fines leave no room for experimentation.[32]

To this end, the GDPR provides that an approved certification mechanism, like a BCR, may be used as an element to demonstrate compliance with the by-design and by-default requirements. This tangible uplift in compliance may save companies substantial amounts of money.

---

[26] Pieter Wolters, 'The security of personal data under the GDPR: a harmonized duty or a shared responsibility?' (2017) 7(3) International Data Privacy Law 165–178
[27] Regulation (EU) 2016/679 of the European Parliament, the Council of the European Union and the European Commission (GDPR) [2016] art 5
[28] Regulation (EU) 2016/679 of the European Parliament, the Council of the European Union and the European Commission (GDPR) [2016] art 6
[29] Regulation (EU) 2016/679 of the European Parliament, the Council of the European Union and the European Commission (GDPR) [2016] art 28
[30] Regulation (EU) 2016/679 of the European Parliament, the Council of the European Union and the European Commission (GDPR) [2016] art 32
[31] Regulation (EU) 2016/679 of the European Parliament, the Council of the European Union and the European Commission (GDPR) [2016] art 25
[32] Article 29 Working Party Opinions and Recommendations, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm, accessed 12 February 2018

3.3.4. Reduce a Company's Operational Cost and Administrative Burden

A BCR can also reduce a company's overall operational cost. While a processor, a company may be required to make several cross-border transfers across the globe. If it opts for Model Clauses, for example, the overall cost of the process will be higher, and the administrative burden of dealing with several different schemes particularly heavy. The cost of a BCR is significant in the beginning, yet once in place, less time and money is required for daily company operations.

3.3.5. Enhance Customer Confidence

A BCR is a very detailed code of conduct that exposes a company's policies and procedures to regulators and the public. Once enforced, a BCR signals to customers that the company takes its data protection duties very seriously and that their data is in safe hands. Processors may operate in various sensitive industries (e.g., financial services, telecoms, technology) where reputation is extremely important and may have a significant impact on a company's viability and profitability. BCRs communicate a transparent, robust, and holistic data protection approach.

3.3.6. Future Procedural Flexibility

The GDPR gives leeway to the European Commission, upon consultation with the newly introduced European Data Protection Board (EDPB), to create procedural rules in the future to better facilitate the approval process. Since the European Commission may specify the format and procedures for BCRs, it is likely we will experience model BCR approval procedures, which may streamline the BCR approval process even further.

3.4. The Lead Supervisory Authority

GDPR offers the benefit that one supervisory authority (the Lead SA) can deal with any issues that relate to cross-border processing activities or activities that involve citizens of more than one EU country. This "One Stop Mechanism" as the GDPR calls it only applies where a processor or controller carries out cross-border processing of personal data, as opposed to merely local data processing.[33]

For instance, processing that takes place in the context of the activities of establishments in more than one Member State, e.g. France and Germany, or processing that takes place in one Member State but it substantially affects or is likely to affect individuals in more than one Member State. In determining this substantial affect, companies should determine whether the processing has or may have the following impact on individuals:

- cause them damage, loss or distress;
- limit their rights and opportunities;
- affect their health, well-being or peace of mind;
- affect their financial or economic status or circumstances;
- leave them open to discrimination or unfair treatment;
- involve the analysis of special categories of data or children's data;
- cause them to change their behavior in a significant way;
- create unlikely, unanticipated or unwanted consequences for them;
- create embarrassment or other negative outcomes including reputational damage, or;

[33] Mark Foulsham and Brian Hitchen, *GDPR: Guiding Your Business To Compliance: A practical guide to meeting GDPR regulations* (Independently Published 2017)

- involve the processing of a "wide range" of personal data.[34]

If a company has one EU establishment, this should be considered its main establishment. If it has several establishments in the EU, the main establishment is its EU headquarters.[35] If, on the other hand, a company has several establishments in the EU that make important decisions, the Lead SA is the SA for the particular cross-border processing activities that are managed by the establishment within its jurisdiction.[36]

However, not every case is as straightforward. There are instances which are called "borderline', where an organization does not have a central administration in the EU, or where its EU establishments do not make decisions that relate to cross-border processing. In these cases that are not straight-cut, companies are still advised to designate an establishment that has the authority to implement such decisions, and which can assume liability in case of an incident. That said, the designation of a Lead SA is not absolute since another SA may claim authority, or may wish to dispute the designation of another SA. This means that a company must document each steps towards designating an SA, and that it ultimately bears the burden of proving its designation.

If a company is not established in the EU, it cannot benefit from the One Stop Shop mechanism, which has significant benefits since it leads to reduced bureaucracy. In such cases, companies must deal with the various local SAs in the countries where they are active, through the local EU representative.

[34] Regulation (EU) 2016/679 of the European Parliament, the Council of the European Union and the European Commission (GDPR) [2016] art 33 and art 34
[35] Christopher Kuner, Dan Jerker, B Svantesson, Fred Cate, Orla Lynskey, Christopher Millard, Nora Ni Loideain, 'The GDPR as a chance to break down borders' (2017) 7(4) International Data Privacy Law 231–232
[36] Article 29 Working Party Opinions and Recommendations, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm, accessed 12 February 2018

3.5. Data Processing at Work: New Challenges towards Compliance

Corporations that wish to comply with the GDPR must also be careful about data processing at work. Technology allows significant monitoring of employees in both their workplace, and outside of it. For this purpose, the Article 29 Working Party recently issued an opinion that discusses the processing of employee personal information. WP29 focuses on the use of new technologies by employers and assesses requirements in light of the upcoming General Data Protection Regulation.[37]

3.5.1. Consent and legal bases to process personal information

The WP29 has historically asserted that employees' consent should not be a legal basis for processing employees' personal information. The power imbalance between employer and employee leads to an uneven situation where consent is not freely given. Even if consent were to be considered valid, it must be specific and proactive, and the employee can withdraw it at any point.[38]

Corporations preparing for the GDPR should not therefore treat consent as a legal basis for processing, at least in most cases. Instead, the majority of the processing should be based in the context of performance of a contract (e.g. salary payments), legal obligations (e.g. fraud prevention) or legitimate interest.

3.5.2. Employee monitoring

The Opinion extensively discusses monitoring of employees' behavior. Several technologies allow employee monitoring, such as GPS-tracking of smartphones, monitoring

[37] Article 29 Working Party Opinions and Recommendations, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm, accessed 12 February 2018

[38] Christopher Kuner, Dan Jerker, B Svantesson, Fred Cate, Orla Lynskey, Christopher Millard, Nora Ni Loideain, 'The GDPR as a chance to break down borders' (2017) 7(4) International Data Privacy Law 231–232

IT usage, Data Loss Prevention (DLP) tools, eDiscovery, Bring-Your-Own Device (BYOD) and the use of CCTV.[39]

Employers should adopt a monitoring policy explaining monitoring details such as time and location. Employers should provide notices stipulating the purposes of monitoring and possibilities for employees to prevent their data captured by monitoring technologies. The WP29 also recommends involving a representative sample of employees in the creation and evaluation of such policies and notices.

3.5.3. Main types of employee monitoring

IT usage monitoring

IT usage monitoring can generate large data amounts. Data analysis and cross matching techniques create the risk of incompatible further processing. The WP29 warns that the risk is not limited to the analysis of the contents of employee communications, but even to wider communications.

To mitigate risk, prevention through technical means should be prioritized over detection. For instance, if prohibited use of communication services can be prevented by blocking certain websites, then blocking should be the preferred option.

In cases of internet traffic monitoring, the WP29 believes that employers should provide an alternative for unmonitored access for employees, such as a free Wi-Fi network or specific devices where employees can access the internet for personal use

[39] Frederik Zuiderveen Borgesius, Sanne Kruikemeier, Sophie Boerman and Natali Helberger, 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation' (2017) 3(3) European Data Protection Law Review 353- 368

Data Loss Prevention (DLP)

The use of Data Loss Prevention tools, which monitor outgoing communication to prevent data or confidentiality breaches, are permitted. However, unnecessary processing of personal information must be avoided through a number of ways (e.g. by delivering a warning message before the e-mail is sent to give the sender the option to cancel it). Further, the employer should implement and communicate a specific acceptable use policy for DLP.

Cloud Services

When an employer requires employees to use cloud services in the context of their work, they must also designate private cloud folders (e.g. a cloud folder named "Private") to which the employer may not gain access unless under exceptional circumstances.[40]

Bring Your Own Device (BYOD) policies

Employers must avoid monitoring private information in BYOD devices. At the same time they need to protect their business and personal information. This can only be done if there are adequate means to distinguish between privacy and business uses of the BYOD device. As a result, they must have methods in place to ensure that the employee's own data on the device is securely transferred.

Wearable devices

[40] Article 29 Working Party Opinions and Recommendations, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm, accessed 12 February 2018

As for wearable devices, the Opinion reiterates that the employer cannot use the employees' consent as a basis for processing this information due to their sensitive nature (e.g. health data). It would be generally prohibited for employers to receive any sensitive personal information in the context of wearable devices (e.g. employees' sleeping and exercise patterns).

Geo-location monitoring

The deployment of vehicle telematics to collect geo-location data is permitted for a number of purposes (e.g. efficiency of service delivery, safety of employees). However, the employer should first assess whether the processing for these purposes is necessary and whether the implementation satisfies the principles of proportionality and subsidiarity. In any event, the employee should be aware of such monitoring and should have the option to temporarily deactivate this option, for instance when he/she drives to attend to a personal matter.[41]

Recruitment and in-employment screening

The employer is not by default allowed to process publicly available information from the social media profile of a job applicant. To process such information the employer should evaluate:

- Whether there is a legal ground that justifies processing (e.g. legitimate interest)
- Whether this is a private or a business social media account

[41] Article 29 Working Party Opinions and Recommendations, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm, accessed 12 February 2018

- Whether the processing is necessary and relevant to the performance of a task (e.g. to assess the qualifications of a candidate).

In any event, such personal information should be deleted if the candidacy does not move forward, and the individual must be informed of the processing before the start of the recruitment process.

While in employment, screening of employees' social media profiles should not occur on a generalized basis and employers should not require employees to use a corporate social media profile.

3.5.4. Data Protection Impact Assessment- a Useful Ally

WP29 suggests that the employer should consider running a Data Protection Impact Assessment and take measures to minimize impact on employees' privacy and secrecy of communications.

WP29 refers to a DPIA as good practice when employers wish to roll out monitoring technology, automated decision making, and profiling that involves employees. The Opinion also mentions that employers should conduct a DPIA to introduce Mobile Device Management (MDM) that allows them to locate devices remotely.[42]

4. Conclusion

This paper has tried to demonstrate that compliance with the GDPR is not an easy task, even when companies wish to be fully compliant. There are many factors that they need

[42] Article 29 Working Party Opinions and Recommendations, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm, accessed 12 February 2018

to take into consideration, including the size of the company, their processing activities, their vendor management, their information security measures, and their corporate governance policies. In other words, every company that finds itself subject to the GDPR, in both sides of the Atlantic ocean, should have a clear plan on how to achieve, and be able to demonstrate, compliance.

It is of course unknown how rigorously will the GDPR be enforced. However, EU regulators signal that they will be rather fierce. Countries that are in the process of implementing the GDPR, like the UK that introduced the Data Protection Bill, have even suggested criminalizing certain data related violations (e.g. the attempt to re-identify anonymous data). The next years will also be revealing as to whether a new type of EU litigation that pertains to privacy matters will emerge. Supervisory Authorities in certain EU Member States are already planning to set up special courts that will deal with privacy concerns. The future will tell how things will evolve in this emerging and constantly growing field.