THE NEW ERA OF PERSONAL DATA IN EUROPE: HOW CAN COMPANIES COMPLY?

George- Cristian IOAN
Babeș-Bolyai University
7 Sindicatelor St., 400029, Cluj- Napoca, Romania
georgecristianioan@gmail.com

Abstract. *Enforcing the EU Regulation 679/2016 seems to be a lengthy process, that will change the landscape of the European commerce. Adapting to the Regulation entails several obligations that any data processor must abide by. Respecting these obligations is a challenge that implies several changes to the corporate structure and internal policies and procedures. Protecting personal data is a costly affair and erroneous implementation of procedures, that leads to data leaks, can be harshly sanctioned. Given the large definition of personal data, maintained by the Regulation, it can be assumed that, even if a company does not directly process information of personal nature, it will encounter, at some points in its activity, incidental forms of data processing. For example, even if a firm's lucrative revenue can mainly be attributed to buying and reselling engross, the company will still process user data on its website. There are several steps that any data processor must comply with. These include a preliminary audit for assessing the quality of current data handling procedures. In this sense, data controllers that already had procedures in place to enforce the legal obligations imposed by the Directive 95/46/CE will be in a privileged position. However, market surveys show that very few processors have actually done so. Given that any real implementation of the GDPR is dependent upon a proper preliminary audit, this study will analyze the proper manner in which such an audit must be conducted. Erroneous preliminary assessments will inevitably lead to future violations of the Regulation. Secondly, after the initial assessment, internal procedures for data handling must be put into place. Clear codification is essential in this process. The processor must ensure that all employees that handle personal information of clients and commercial partners are well trained and able to understand exactly what they must do. Moreover, the procedures should not be limited to mere day to day tasks. Crisis scenarios must be addressed, as this can first of all limit the potential damage and ensure that the subjects of data processing are properly informed, in accordance with recital 85 of the GDPR.*

Keywords: *personal; data; European Union; GDPR; DPIA; DPO.*

The nature of the Regulation 679/2016 and the main changes

As of 25th of May 2018, the European Union's new framework of data protection will enter into force. Although data protection is by no means a new concern for the European legislator, even in itself, replacing a Directive, namely Directive 95/46/CE with a Regulation, the General Data Protection Regulation 679/2016 (hereinafter, the GDPR), creates significant changes in the landscape of personal data. As Regulations are mandatory second legislation tools, the provisions of the GDPR are directly applicable to both vertically and horizontally in any member state of the European Union. Thus, any data subject can submit requests to any controller that has access to his data based on the Regulation itself, with no regard to the national legal framework. Moreover, controllers can be held liable for any violations of the Regulation even if its provisions are yet to be adapted in the national law.

Changes of paramount importance are made as far as the substantial regime for processing data is concerned. These include (i) the establishment of obligations to appoint a Data Protection Representative and a Data Protection Officer; (ii) modification of the consent regime; (iii) express codification of the right to be forgotten; (iv) introduction of the obligation to notify the data subject and the authority of the breach of personal data security; (v) the obligation of transparency with regard to internal data processing procedures; (vi) the introduction of fundamental principles and new rights and (vii) the establishment of a single supervisory authority, with the modification of the sanctions regime.

Companies that actively participate in the European trade market must find manners in which to comply with the exigencies of the Regulation. Although this task is by no means an effortless stroll, it seems that data controllers that already instilled internal procedures to comply with Directive 95/46/CE will be in a significantly better position. Adapting to the Regulation is far better than starting from zero as far as data protection is concerned, as many of the rights and obligations the Regulation codifies either already existed, under the Directive or could have been easily derived from the Court of Justice of the European Union's case law. For example, the right to be forgotten already existed, ever since the famous Google Spain case, even though the Directive did not expressly mention it. Now, the same right is codified under the Regulation. It is easy to see how transitioning from a proper program of protecting rights under the Directive to fully functional internal procedures of GDPR compliance can and should be a rather smooth process.

However, the vast majority of companies are not in such a privileged position. According to a survey (Curtis, 2017, pp.7-8), out of 400 of the leading companies in their fields, only 8% of managers declared themselves ready for the entry into force of the Regulation, with 28% unaware of it. Another 26% said they would not be able to complete their internal measures by May 2018. Accordingly, the main focus of the present study will be to analyze the manners in which such companies can create compliance programs.

The premise of this study is that almost all low and middle tier companies will process data in some form during their activity. Processing is defined under Art. 4, para.2 of the Regulation as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. From the outset, it is clear that the European legislator intended to maintain a large scope of protection for the Regulation, building upon the blocks set under the Directive 95/46/CE. As such, merely storing employee personal data is a form of data processing. Almost any online activity will also raise questions of compliance. Even if ad- related profiling is not in place on a certain online platform, processing data such as a user's IP number, MAC address, information concerning his online account or persona or using cookies fall under the scope of the definition of data processing set forth by the Regulation. Recently, the Court of Justice of the European Union, in the case of Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein vs Wirtschaftsakademie Schleswig-Holstein GmbH, decided that responsibility for protecting personal data arises even when using a third-party platform, such as a Facebook fan page account. Moreover, even companies that reside outside of the EU, but

process data of European citizens have to find ways in which to comply with the GDPR, which some (Codevilla, 2018, p.12) regard as an important challenge.

General steps for implementing the GDPR

The first step in the process of adapting company policies to fulfill the standards imposed by the GDPR should always be conducting an internal audit (Khan, 2016, pp.7-8). In order to know what steps must be taken the controller must be aware of the current state of affairs in the company. In this sense, this would be an ideal moment for conducting the preliminary steps for a future Data Protection Impact Assessment, that would be carried out under the supervision of the Data Protection Officer (Voss, 2016, p.804). Secondly, the controller should verify whether the conditions are fulfilled for the mandatory appointment of a Data Protection Officer. Accordingly, changes should be made in order to comply to this obligation, whether that means externalizing this service, hiring a data protection officer or changing the work contracts of an already existing employee in order to encompass such responsibilities. Nevertheless, it is mandatory to appoint a person in upper management to supervise the process of implementing the Regulation.

Thirdly, internal procedures should be codified, concerning the handling of personal data. These procedures should not be generic and must actually take into consideration the nature of the processing and the types of data that are being processed. The philosophy of implementation should be that of data protection by design (Varotto, 2015, p.79). Sensitive data should be distinguished from normal processing. All employees that have attributions that either explicitly or implicitly involve data processing should be briefed and trained to respect the new procedures. Nevertheless, at this time, procedures should be instilled in dealing with Personal data breach notification, taking into consideration all potential breaches and possible worst case scenarios. The second part of reforming internal procedures should consist of ensuring that personal data of employees and other contractual staff are properly stored and protected. In this sense, it is essential that their consent is taken concerning upcoming processing necessary (Bevitt & Stack, 2016, p.12). Special attention should be given to situations where CCTV cameras are used in the workplace, during work hours, since they gather biometric data, which is a special category with higher standards of protection.

Lastly, the final step should be ensuring that the contracts used with third-party use proper means of obtaining consent for data processing. The Regulation significantly changes the legal regimen of consent, which must be express and cannot be deduced from other factual circumstances, as controllers could have done under the Directive 95/46/CE (Taylor & Smith, 2017, p.14).

Preliminary audit and the Data Protection Impact Assessment

As previously mentioned, the first step in complying with the GDPR should be conducting a thorough and sincere evaluation of current internal policies and procedures. Nevertheless, the manner in which the audit is to be conducted is dependant upon the existence or lack of prior procedures, aimed at respecting the obligations imposed by the Directive 95/46/CE. When such procedures already exist the focus should be placed on adapting them to the higher exigencies of the Regulation. If the

controller was not sufficiently diligent to create such procedures the task will be significantly more laborious. The preliminary audit should either be externalized or conducted by a current employee with expertise in data protection. Ideally, the audit should be externalized, as it would contribute to the objectivity of the results, given that a purely internal assessment could be subject to pressure from managers or other employees responsible for data protection to hide previous breaches or avoid findings that could only be resolved by means of costly investments.

The first objective of the preliminary audit should be to determine what data is currently being processed. This is necessary in order to verify whether the company has the obligation of naming a Data Protection Officer. Appointing a DPO is mandatory in three situations:, namely when: (i) processing is carried out by a public authority or body, with the exception of courts acting in their judicial role; (ii) the principal activities of the controller or of the person in charge of the controller consist of processing operations which, by their nature, scope and/or purposes, require regular and systematic monitoring of the large-scale targeted persons; or (iii) the main activities of the controller or the processor by the controller consist scale processing of special categories of data referred to in Articles 9 and 10. Nevertheless, when a company will voluntarily choose to name a DPO, although the conditions for mandatory appointment are not fulfilled, Art 37-39 of the Regulation are fully applicable to said controller (Article 29 Working Party, p.5).

Although the notions of main activity, large scale and periodic and systematic monitoring are not clearly defined by the Regulation, several criteria can be used to understand their scope. The main activity encompasses operations necessary to achieve the social or lucrative purpose of the controller or processor. It also includes the case where data processing is logically interlinked to the nature of the controller's business (Article 29 Working Party, p.7). The notion of large scale, however, remains volatile enough to not be explicitly defined. Whether processing is large scale will be determined on a case by case basis, taking into consideration (i) the nature of processed data; (ii) the reasons for processing the data and (iii) what types of data subjects are affected by the processing, where aspects such as geographical, social and gender distribution should be addressed.

Finally, monitoring is periodic when it is continuous for certain periods of time or repeated at specified and systematic intervals when organized, follows a specific method, is part of a data or strategic data collection program. In addition to profiling, which is mentioned expressly in the statement of reasons, determining location by applications, health status through devices or telecommunications services are forms of monitoring.

After this initial assessment, the company should appoint a Data Protection Officer, either to fulfill its mandatory legal obligation or if this is the strategy for data protection adopted by the management of the company. However, the aforementioned rule, namely that appointing a Data Protection Officer when it is not mandatory will result in being held liable to the same standards as any company that must fulfill such an obligation, should be taken into consideration when making such a decision. If the processing falls under the scope of protection enshrined by Art. 37- 39 of the Regulation, the audit should continue only after a person in higher management is appointed to supervise personal data protection.

The preliminary audit should also establish how much data is currently stored or otherwise used by the company. This should include reference to any form of processing, including profiling of users. Next, steps should be taken towards data minimization. We consider that data should be classified in three categories: (i) necessary data, which includes data that is essential for the functioning of the company (e.g. a hospital cannot function without processing patients' medical records); (ii) useful data, which includes information that can aid the company in growing and expanding its activity (e.g. user data collected from the company's Facebook page, which includes the age groups of average visitors of the page, can be used as an important tool in targeted advertising) and (iii) unnecessary data. When data is unnecessary it should either be deleted, when possible, according to the rules imposed by the Regulation or it can be anonymized or pseudoanonymized (von dem Bussche Freiherr, Zeiter, 2016, p.577). Nevertheless, it should be established whether the data that is processed stems from vulnerable categories of data subjects, such as minors.

Once aspects concerning the nature of the data have been settled, the audit should focus on the current manner in which data is stored. The auditor should verify what parts of the data are physically stored and how much is digitally stored. It should be verified if there are current mechanisms in place to protect said data. Each type of data should have specific methods of protection. While installing CCTV cameras is a decent method for protecting data stored on physical mediums, digital data must also be secured against cyber-attacks. The operator should make sure to verify how data was collected and if (and how) the consent for processing the data was taken. The Regulation also applies to consent that has already been obtained, which means that the controller must ensure that consent for processing which was legally obtained at the time, but doesn't fulfill the current exigencies, set forth by the Regulation, is renewed.

The audit should also establish who has access to personal data in the company and for what purpose must they use the data. Most probably, the Human Resources department will use data for different purposes than the IT department. It should also be verified who was responsible for data protection before creating new procedures. Moreover, the audit should clearly show what data is distributed to third parties or data processors.

Finally, a Data Protection Impact Assessment (DPIA) must be conducted. Although some scholars argued that it is a mere compliance check (Wright & De Hert, 2012, p.34), it has been defined as *an instrument for eliminating or mitigating privacy and personal data risks which recognizes what data is being or is going to be processed in the future and justifies that processing; identifies, analyses and classifies the risks for natural persons; identifies and implements remedies to these risks; produces a report about the DPIA and monitors the processing for compliance with the DPIA and/or changes in the risks* (Yordanov, 2017, p.487). It is mandatory, according to Art. 35 of the Regulation, when a type of processing is likely to result in a high risk to the rights and freedoms of natural persons. Such an Assessment must include, at minimum: (i) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (ii) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (iii) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph and (iv) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal

data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

It has been shown that the concept of *high-risk* processing is a difficult and ambiguous one, and can differ from region to region, due to the cultural background (Voss, 2016, p.804). However, according to Article 29 Working Party, the main body for consultation and harmonization on all data protection matters within the EU, according to Paul De Hert and Vagelis Papakonstantinou (2016), several factors should be taken into consideration when assessing whether certain data processing imposes a high risk, which includes (Article 29 Working Party, pp.7-8): (i) Evaluation or scoring, including profiling and predicting, especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements"; (ii) Automated-decision making with legal or similar significant effect. When the controller uses systematic methods that automatically assess data subjects' information there is a higher risk for misuse of data. The European legislator seems particularly distrustful concerning these types of practices, which will affect a large number of companies, especially in the field of Big Data (Zarsky, 2017, p.1017); (iii) Systematic monitoring since such processing can collect data that the subject is unaware of. This includes CCTV surveillance; (iv) whether data which is sensitive according to Art. 9 or stems from vulnerable data subjects is processed and (v) whether data is processed on a large scale; (v) Datasets that have been matched or combined; (vi) Innovative use or applying technological or organizational solutions and (vii) the processing in itself "prevents data subjects from exercising a right or using a service or a contract.

Putting new internal procedures into place and adapting contracts

There are three essential phases in actually implementing the GDPR, once the preliminary audit is finished. These include undertaking remediation activities, implementing operational changes and transitioning to business as usual (Bowman & Gufflet, 2017, p.261). The whole process is dependant upon creating clear internal rules for employees to follow. These procedures should be transparent and accessible to data subjects, also. According to Temme (2017) transparency is a fundamental pillar of the GDPR, and some activities, such as algorithmic decision making, can only be undertaken after ensuring that the *right to an explanation* is respected.

The procedures should, *de minimis*, address the following issues: **(i)** how data is stored, namely by establishing (a) what data will be stored on physical mediums; (b) what data will be only digitally stored; (c) clear rules as to the duration of data storage; (d) who will be responsible with checking the duration of data storage and deletion of data; (e) if any approvals are necessary in order to access the data and (f) procedures for tracking of data and its use; **(ii)** how the data will be protected, from both internal threats, such an employee-led data breaches or external attacks, especially cyber-attacks; **(iii)** how the rights of the data subject will be respected. For each of the rights enshrined by Art. 12-22 of the Regulation, a distinct procedure, which should include rather strict deadlines, should be established. These should include, (a) a procedure to provide information to the data subject, concerning how his data is used and the purpose for using it. Distinct procedures should be designed for data that was not obtained from the data subject; (b) a right to access procedure, which could be similar to the aforementioned one, since, it also entails providing information. This should include the

manner in which information is transmitted to the data subject (*e.g.* via e-mail, personal account on the company's site etc.); (c) a rectification procedure; (d) an erasure procedure; (e) a procedure to ensure that the data subject can restrict the processing of his data. The former three procedures should include clear rules for handling the requests from users and their route through different departments of the company.

Another important point is establishing an (f) portability procedure, which should establish which common and machine-readable format will be used by the controller, how the information given to the data subject will be extracted from company logs and rules concerning the secure transmission of information to other controllers. Moreover, a guideline for respecting the subject's right to object must be designed. It should include the manner in which objections are filled and information concerning decision making and communicating decisions concerning requests based on this right. Janal (2017) emphasizes that the Regulation does not provide a reasonability or proportionality in respecting portability.

Moreover, a central point of the regulation is notifying users of data breaches. As previously mentioned, as part of the preliminary audit, the problem of data breaches must be analyzed. The main purpose of this analysis is to establish the main causes of potential information leaks. Several distinct procedures should be established to accommodate the anticipated braches. They should establish deadlines for notifying both the data subject and the national authority. Furthermore, a general procedure should be established, concerning other types of unanticipated problems concerning losing user information or fraudulent subtraction of said data. If the company also acts as a processor it must also notify the controller of the breach. When the data of a vulnerable person is processed, the competent authorities for supervision should also be notified. When data of a minor, for the processing of which parental consent is required, the controller must notify the parents or legal guardians (Esayas, 2014, p.352). Finally, the procedure should also contain subsequent measures for limiting the leaks.

Finally, internal sanctions should be established for potential failures of properly handling data and respecting the rights of the data subject. It is important that internal accountability exists and that the role of participants in processing data is defined, in order to ensure that any potential negligence can be attributed to a certain person or group.

Furthermore, clear procedures for requesting the consent of data subjects should be enacted. In this sense, employees who handle this issue should be instructed to adapt to the particular situation, by requesting consent based on the scope of the processing, when it is directly taken from the user. A registry for such information should exist and the procedure for transcription of information concerning the basis for each processing of data.

Conclusion

Although the GDPR imposes significant burdens on data controllers, with proper care, any low and medium tier controller can fulfill its obligations. As we have shown, the first steps in implementing the Regulation are the most important, as after putting the internal mechanism into place, the system should run *on autopilot*. As long as the purposes for processing and the potential risks are identified, the principles of

minimization and data protection by design are respected and clear internal procedures, adapted to the company's activities are adopted, complying with current standards is far from impossible.

Acknowledgments: This study is part of Babeş-Bolyai University of Cluj Napoca's program of scholarships for student researchers.

References

Bevitt, A., & Stack, C. (2016). Preparing for the GDPR - Advice for employers. *Privacy and Data Protection Journal*, 16(6), 12-15.

Bowman, J. & Gufflet, M. (2017). Meeting the Challenge of a Global GDPR and BCR Programme. *European Data Protection Law Review*, 3(2), 257-261.

Codevilla, T., (2018). GDPR compliance tips for small and medium-sized businesses. *Colorado Lawyer*, 47(2), 12-18.

Curtis, R., (2017). European businesses unprepared for GDPR. *Taxation Magazine*, 4(2), November 28..

De Hert, P., & Papakonstantinou, V. (2016). The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals. C*omputer Law & Security Review*, 32(2), 179-194.

Esayas, S. (2014). Breach Notification Requirements under the European Union Legal Framework: Convergence, Conflicts, and Complexity in Compliance. *The John Marshall Journal of Computer & Information Law*, 31(3), 317-368.

European Commission (2016). Article 29 Working Party, Guidelines on Data Protection Officers. Retrieved from ec.europa.eu/newsroom/document.cfm?doc_id=43823.

European Commission (2017). Article 29 Working Party, Guidelines on Data Protection Impact Assessment. Retrieved from ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

Information Commissioner's Office (2014). In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information. Retrieved from https://ico.org.uk/media/1542/cctv-code-of-practice.pdf.

Janal, R. (2017). Data Portability - A Tale of Two Concepts. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 8(1), 59-69.

Khan, S. (2016). Practitioner's Insight into the New EU Data Regulation. *Compliance and Risk Journal*, 5(1), 6-12.

Taylor, C., & Smith, R. (2017). UK regulator's guidance on GDPR consent - is the definition any clearer?. *Privacy and Data Protection Journal*, 17(5), 13-17.

Temme, M. (2017). Algorithms and Transparency in View of the New General Data Protection Regulation. *Data Protection Law Review*, 3(4), 473- 485.

Varotto, S. (2015). The European general data protection regulation and its potential impact on businesses: some critical notes on the strengthened regime of accountability and the new sanctions. *Communications Law*, 20(3), 78-86.

von dem Bussche Freiherr, A., & Zeiter, A., (2016). Implementing the EU general data protection regulation: a business perspective*. European Data Protection Law Review*, 2(4), 576-581.

Voss, GW. (2016). Internal Compliance Mechanisms for Firms in the EU General Data Protection Regulation. *Revue juridique Thémis de l'Université de Montréal*, 50(3), 783-820.

Wright, D., & De Hert, P. (2011). *Privacy Impact Assessment*. Heidelberg: Springer.

Yordanov, A. (2017). Nature and Ideal Steps of the Data Protection Impact Assessment under the General Data Protection Regulation. *European Data Protection Law Review*, 3(4), 486-495.
Zarsky, T.Z. (2017). Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, 47(4), 995-1018.