ISSN 2704-8012

European Journal of Privacy Law & Technologies

Special issue (2020)

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

Special issue (2020)

Edited by Massimo Foglia

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

Published Online by G. Giappichelli in September 2020
www.ejplt.tatodpr.eu

NEW DATA PROTECTION REGULATION IMPACT ON EUROPEAN INSTITUTIONS [*]

Pelopidas Donos, Data Protection Officer (DPO)
of the European Investment Bank (EIB)

Abstract:

Purpose of the paper is: a) to briefly present the main changes introduced by the New Data Protection Regulation applicable to all EU Institutions and bodies, b) to present the main actions undertaken in order to ensure compliance with the legal framework and c) to describe some differences regarding the application of the legal framework in comparison with private entities and public authorities in the EU Member States.
European Institutions and Bodies were under extreme time pressure in order to implement compliance actions with their data protection Regulation because there was no transition period between the adoption and the entering into force of the new legal framework. The new "accountability" model enhances the responsibilities of the institutions and requires a change of data protection culture not only for the institutions but also for the Supervisor. On the other hand, European Institutions, because of their robust data protection regime can substantially contribute to the development and establishment of future "Best Data Protection Practices".

Keywords: New Regulation for EUIs, Accountability model

1. Introduction

In April 2016 the comprehensive Data Protection Reform was approved. It includes (1) the General Data Protection Regulation (GDPR replacing Directive

[*] Although the activities of the DPOs and the legal obligations of the EUIs are similar, this Article is based only on the experience of the EIB's DPO and reflects his personal opinion.

95/46) establishing a single legal regime over the Members States, (2) a Data Protection Directive on the Police and Criminal Justice sector harmonizing laws in order to facilitate cross border cooperation in the fight against crime and terrorism. These two instruments entered into force in May 2018.

Through those legal acts important changes have been introduced: (a) the idea "one continent/one law" which, together with the "one stop shop" (leading of a single supervisory authority) will facilitate procedures and clarify responsibilities for many companies, businesses and European citizens, (b) the idea "European rules on European soil" (a new territorial scope in order to include EU third countries companies offering services in the EU), (c) major responsibility for Controllers (privacy by design and by default, data protection impact assessments), (d) a major control of data subjects over their own data (right to be forgotten and portability, right to be informed about serious incidents on data protection), (f) increased accountability and enforcement (significant fines can be applied for breach of data protection rules).

The third act of the reform, the Regulation (hereinafter New Regulation) dedicated to European Union Institutions and Bodies (hereinafter EUIs), which aligns the data protection provisions with the provisions of the GDPR, entered into force on 11 December 2018 [1]. The main difference with regard to the EUIs was that other than the GDPR, the New Regulation entered into force without a transition period, which means that the EUIs had less time to prepare and implement the necessary changes. During 2018, the EUIs activities in this particular field have therefore continued to be governed by the previous Regulation (EC) No 45/2001, until the entering into force of the new one on 11 December 2018. That means that complaints (also to the European Data Protection Supervisor) and other cases having started before the date of entry into force were handled, and continued to be handled until they were finalised, under the provisions of the previous Regulation.

On the other hand, the EUIs were for several years closely supervised by the EDPS and under the guidance of the Supervisor had initiated several preparatory actions in order to ensure compliance with the New Regulation [2]. That means that for the EUIs the new data protection provisions and their implementation constitute an evolution rather than a revolution. Nevertheless, there is no doubt that the new legislation indeed introduces a new model of Supervision, enhanc-

[1] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

[2] EDPS Accountability on the Ground, part. 1, part. 2, available on https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en.

ing the accountability of the EUIs with regard to their compliance with their legal obligations.

In practical terms, the most important changes introduced by the New Regulation, concern the enhanced obligations of the EUIs and the responsible Controllers and Processors inside the institutions. Furthermore, they concern the conducting of Data Protection Impact Assessments (DPIAs), the obligation to consider in advance the data protection requirements, whenever new information systems or automatized processing operations are introduced (data protection by design and by default), or the obligation to report data protection breaches. Finally yet importantly, the New Regulation provides the data subjects with more rights and enhances the powers of the EDPS, including the power to impose fines.

2. Model change in Data Protection Supervision and new powers for the EDPS

The new "Accountability model" indicates a shift of responsibilities for both the EUIs and the Supervisor (EDPS). Under the previous system, the EUIs (DPOs and Controllers inside the EUIs) had to invest more time and resources in order to notify the most risky processing operations to the EDPS to be prior checked (prior notification model). After the operations have been prior checked, the EUIs had to implement the recommendations but on the other hand, they had at their disposal a kind of "compass and roadmap" with regard to the necessary actions ensuring compliance. Accountability goes beyond "passively" ensuring compliance, in the sense that the EUIs shall be in the position to "actively" demonstrate at any time their compliance with the Regulation vis-à-vis the data subjects or/and the EDPS. That means that the EUIs and consequently the DPOs have to introduce a "risk based approach" in order to be able to identify the data protection risks inside the institutions and to take all necessary measures to ensure, document and demonstrate compliance. Furthermore, the DPOs have to develop enhanced monitoring actions, enabling the follow up of the risk mitigating actions. This risk-based approach together with the reinforcement of the responsibility of the Controllers requires a new data protection culture within the EUIs. More awareness sessions, policies, and procedures that are more detailed can be the outcome of a gap analysis conducted by the DPOs.

The accountability model requires also a shift of activities also from the side of the Supervisor. Besides the consultation provided to the EUIs, it is expected that the EDPS will invest more time in the future for ex post compliance checks, audits and inspections, conducted either "on site" or remotely. This development coincides with the enhanced powers of the EDPS introduced by the New

Regulation, consisting mainly of: a) the possibility to impose a definite limitation, including a ban on processing, b) suspending data flows to a recipient, c) being informed about security breaches, and ordering the notification of the affected persons, and d) imposing administrative fines in cases of non-compliance of 25.000 to 250.000 EUR.

3. New obligations for the institutions

The main new obligations for the EUIs and their controllers are presented in the following four areas:

a) Register

The Register is the data protection "mirror" of the EUIs, containing a detailed description of all processing operations. The Register has an important function not only for Controllers and DPOs but also for the data subjects, which they can find there all information about the way their personal data are processed by the EUIs.

Also under the previous Regulation, all personal data processing operations should be prior notified to the DPO by the Controller and a publicly accessible Register containing all notifications should be also kept. Nevertheless, there was a distinction between "simple" notifications and those related to more sensitive cases, which should subsequently be notified by the DPO to the EDPS. After the 11th of December 2018, the prior check obligation to the EDPS ceased to exist. The text of the New Regulation foresees the replacement of the DPO Register by records kept by the Controllers. Nevertheless, and upon the strong recommendation of the EDPS, the EIB together with the vast majority of the EUIs will continue to have those records kept centrally by the DPO. This solution ensures business continuity and enhances the overall visibility of the processing operations. In addition, the DPOs have to ensure that the Register is publicly accessible also outside the institutions.

b) Data Protection Impact Assessments (DPIAs)

Under the New Regulation, the Controllers responsible for a processing operation of personal data have the obligation to conduct a DPIA whenever the operation is likely to create a high risk for the rights and freedoms of data subjects. This is the case especially for new automated systems containing sensitive data on a large scale.

In practice, the DPIA looks like a set of questions, which allows Controllers to conduct a precise evaluation of the process' risks and to envisage concrete measures to address them. The New Regulation foresees an obligatory consulta-

tion of the DPO during the DPIA. Only in cases where the risks cannot be mitigated will the EDPS be consulted.

In order to prepare the organisations for this important obligation, the EIB's DPO has conducted a threshold inventory to identify the processing operations that could be subject to a DPIA. The inventory was based on a questionnaire proposed by the European Data Protection Supervisor (EDPS) after consultation with the DPOs of the European Institutions and bodies. The inventory was also used in order to identify sensitive processing operations which had not been sent to the EDPS for prior checking under the previous regime. Ideally, the EUIs have to develop a methodology for conducting the DPIAs and a related procedure including the monitoring of the implementation of the risk mitigating measures.

c) Adjustment of Data Protection clauses (DP) in Procurement Rules and Contractual Clauses

One of the most challenging issues, especially for the big institutions like the EIB, was the adjustment of Data Protection clauses (DP) in Procurement Rules and Contractual Clauses to the requirements of the New Regulation. The new responsibilities of the processors, the obligations related to the security breaches and to the conducting of DPIAs had to be reflected and translated in the contractual clauses and in the calls for tenders. In 2018, the EDPS addressed two letters to all European institutions and bodies describing the necessary changes and adjustments required by the New Regulation in the matter of procurement rules and contractual clauses, especially those related to outsourcing activities. The adjustment of the provisions is of upmost importance in order to meet also the requirements of privacy by "design and by default" as reflected in Article 27 of the New Regulation. Especially for new systems and applications, the EUIs will have the opportunity to describe the relevant data protection requirements from the very beginning namely during the procurement phase.

The EIB DPO prepared a questionnaire and conducted an extensive survey within the Bank to establish an inventory of all EIB Data Protection (DP) clauses used in outsourcing activities. The exercise has identified three types of DP clauses that would need to be adjusted: Procurement rules and templates (1), Contractual DP clauses (2) and Service Level Agreements (SLA) (3). The exercise identified approximately 500 objects being subject to the adjustments.

Given the big amount of contracts, one important question was whether it would be necessary to also adjust existing contracts, and if yes, which ones. A dedicated Working Group composed of DPOs and the EDPS has been established in order to discuss all parameters of the matter and initiate the setting up of Standard Contractual Clauses for outsourcing activities.

As a follow up of the relevant discussions, the EDPS proposed to the institu-

tions to conduct a risk assessment for all categories of contracts in order to identify them under the following categories: No risk, Low risk and High risk. For those identified as High risk contracts, the EUIs shall, on their own initiative, address the contractual counterparties and propose to amend the contracts by using the standard contractual clauses prepared by the EDPS and the European Commission. The EDPS finally communicated the Standard Contractual Clauses shortly before the entering into force of the New Regulation.

Furthermore, the EIB DPO together with the other DPOs (OLAF, Commission and EIF) took the initiative to consult the EDPS on the way the EUIs have to proceed in cases where contractual parties ask for changes because of their GDPR obligations. The result of the consultation was a model letter prepared by the EDPS to be used by the institutions in those cases.

d) New rights for the data subjects

With regard to the rights of the data subjects, the New Regulation introduces additional safeguards related to the validity of the consent of the data subject. Consent is valid only via an "affirmative action" of the data subject (opt-in) and EUIs have the obligation to always document and demonstrate that consent has been provided. Nevertheless, the processing operations where the consent of the data subjects is legally required, is limited to those cases where the data subjects have a real choice to provide the information or not (like e.g. in the EIB for staff members having their pictures published in the intranet or for travelers and visitors providing their diatery preferences to the organisation). In the vast majority of the cases in the EUIs, the legal basis for the specific processing operations derives from a contractual relationship (e.g contract of employment) or represents a legal obligation of the institution.

New is also the right to "data portability" (Article 22 of the New Regulation) entitling data subjects to receive their personal data in a structured machine-readable format, and ask to transfer the data to another Controller. Taking into consideration that this Article is copied from the GDPR and applies mostly to the private sector e.g. whenever a customer changes the service provider, it is expected that the impact to the EUIs will be rather limited. The famous "right to be forgotten" has been also included in the Regulation as an extension of the already applicable right to ask for an erasure (deletion) of the data. The additional obligation of the Controller not only to erase the data but also to inform other Controllers about the request, if the data have been made public, will have probably a limited impact to the EUIs taking into consideration that this provison is also copied by the GDPR and it is more related to Internet or social media providers (Big data companies like e.g. Google or Facebook).

One of the most urgent issues following the entering into force of the New Regulation was to prepare and adopt internal rules allowing the restriction of

data protection rights (Article 25 of the New Regulation). Taking into consideration that the possibility to restrict rights on an ad hoc basis (Article 20 of the previous Regulation 45/2001), (e.g. during investigations and administrative inquiries), has been removed from the final text of the New Regulation, internal rules had to be prepared allowing the respective services to fulfil their tasks without hindrance. Those rules have to be published also to the Official Journal of the European Union. Therefore, and due to the time constrains, the DPOs and the EUIs were under extreme time pressure in order to prepare adopt and publish the rules. The EIB has published e.g. two sets of internal rules, one set governing the conducting of investigations and administrative inquiries [3] and one set related to similar activities of the Personnel Department.

e) Adjustment of policies, procedures and "Privacy Notices"

Another important topic was the adjustment of the Data Protection Statements (Privacy Notices) to the requirements of the new legal framework. The DPOs in cooperation with the services concerned had to identify and accordingly amend the most important Privacy Notices, especially those accessible via Internet. It goes without saying that also internal procedures, policies and guidelines had to be also amended or initiated based on a conducted gap analysis.

Although there were no substantial changes with regard to international data transfers, the EUIs have to pay attention in order to carefully document and supervise transfers outside the European Economic Area and especially for those applications based on cloud solutions.

4. Status of the Data Protection Officer

The Data Protection Officers (DPOs) of the EUIs (Section 6 of the New Regulation) are integrated in a European framework of data protection entities, headed by the European Data Protection Supervisor (EDPS) located in Brussels (with substantial competences and supervisory powers - Art. 52 of New Regula-

[3] Internal rules concerning the processing of personal data by the Fraud Investigations Division within the Inspectorate General and the Office of the Chief Compliance Officer of the European Investment Bank in relation to the provision of information to data subjects and the restriction of certain of their rights, available on https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2019_065_I_0001&from=EN. Internal rules concerning the processing of personal data by the Personnel Directorate of the European Investment Bank in relation to the provision of information to data subjects and the restriction of certain of their rights, available on https://www.eib.org/attachments/documents/eib_decision_on_the_processing_of_personal_data_en.pdf.

tion), and completed at national level by national Data Protection Authorities (DPAs) and at EUIs level by the DPOs.

In all EUIs the DPO is an independent function. The functional independence of the DPO is enshrined in the New Regulation and complemented by the implementing rules of each institution. The DPOs have the following main tasks:

a) to inform and advise the Controller or the Processor and the employees who carry out processing operations of their obligations,

(b) to ensure in an independent manner the internal application of the Regulation; and to monitor compliance, including the assignment of responsibilities, the raising of awareness and training of staff involved in processing operations, and the related audits,

c) to provide advice where requested as regards the necessity for a notification or a communication of a personal data breach,

d) to provide advice where requested as regards the data protection impact assessment,

e) to consult the European Data Protection Supervisor in different occasions,

f) to respond to requests from the European Data Protection Supervisor, cooperate and consult with the European Data Protection Supervisor at the latter's request or on his or her own initiative,

g) to ensure that the rights and freedoms of data subjects are not adversely affected by processing operations,

(h) to investigate matters and occurrences that directly relate to the DPO's responsibilities,

(i) to cooperate with the DPOs of the other institutions,

(k) to represent the institution with regard to all data protection issues.

The DPO of the EIB e.g. has data protection oversight over all Departments and can use significant investigative powers. In particular, the DPO has access to all premises and to all information systems and applications, may propose administrative measures and issue general recommendations, draw attention to any failure by a staff member to comply with the Regulation, propose an administrative inquiry, and request an opinion from the relevant areas of the Bank on any associated issue. The internal application of data protection rules (Art. 43, 44, 45 of the New Regulation) should be ensured with autonomy, and the DPO should plan his activity in an independent way.

In addition, and under the New Regulation, the EU Institutions have to ensure that the DPO reports directly to the highest management level and that the DPO will be involved in all cases of data protection breaches and of Data Protection Impact Assessments. The contact details of the DPO shall be also made public. Furthermore, the DPOs should be allocated the resources necessary for the performance of her/his duties. The new legal framework provides the EUIs

with the possibility to use external DPOs and to "share" the DPO by appointing one DPO for more EUIs.

Under the new "Accountability model", the responsibilities and the importance of the position of the DPO will increase. Like in the private and public sector of the Member States, the DPOs have to play a central role [4] by preparing the EUIs in the best possible way in order to ensure compliance with the new legal framework. Although the liability lays mainly with the Controllers, remains the main responsibility of the DPO to create awareness for controllers and data subjects, to update about the legal and technical developments, to communicate with the Supervisor and coordinate the actions of all data protection stakeholders.

5. Conclusion

The new data protection framework introduces the new model of "Accountability" for the European Institutions and Bodies. This model means more responsibilities for Controllers inside the institutions and for the Data Protection Officers in order to ensure document and demonstrate compliance. Nevertheless, the new model represents rather an "evolution" than a "revolution" for the data protection regime taking into consideration that the EUIs were under many years under the close supervision of the EDPS. Although the EUIs had less time to introduce and implement the necessary changes they can serve as a "laboratory" of best data protection practices, taking into consideration that they concentrate in a more "controlled environment" all kinds of processing operations, like e.g. staff related operations, business related operations upon personal data, international data transfers and contractual relationships with public and private stakeholders. The EDPS can use this experience in order to further develop and establish those "Best Data Protection Practices" in their proposals, consultations and guidelines.

[4] B. RASLE, *Pour une Désignation 'Idéale' du DPO* (2019) *Le Journal du Management*, 38.