ERA Forum (2019) 19:505–509
https://doi.org/10.1007/s12027-019-00549-x

EDITORIAL

GDPR and beyond—a year of changes in the data protection landscape of the European Union

Magdalena Kędzior[1]

Published online: 14 February 2019

In May 2018 the data protection legal reform package—consisting of the General Data Protection Regulation (henceforth GDPR)[1] and the Law Enforcement Directive[2]—became applicable. This is generally perceived as the most comprehensive data protection law reform undertaken since Directive 95/46/EC was adopted.[3] ERA responded to these new developments by organising a series of events dedicated to data protection law. When assessing this reform, one should bear in mind that this process is a multi-layered one and has not yet been completed. The reform of the European Union data protection landscape is ongoing: sectoral provisions in the Member States and new *lex specialis* regulations are being adopted or still discussed at the European and national levels. The arrival of the end of the year 2018 inclines us to reflect on the motives and challenges of the reform, on how its goals may be achieved as well as on the possible effectiveness and adequacy of the methods of reform adopted.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (*Police Directive, Law Enforcement Directive*).

[3] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

✉ M. Kędzior
MKedzior@era.int

[1] Trier, Germany

The EU legislator took careful note of the point that the rapid development of technology had led to a situation in which the provisions of Directive 95/46 could no longer guarantee the required degree of protection of data subjects rights.[4] Consequently on 25 January 2012 the European Commission submitted a legislative proposal in order to modernise and replace the provisions of the Directive, consisting of the GDPR as well as the Law Enforcement Directive. Meanwhile, the Council of Europe too modernised its Convention No. 108 laying the foundations for the comprehensive and modern legal framework for Europe-wide data protection.[5] As noted by Reding, apart from rapid technological progress, the globalisation of data flows and the wide access to personal data by law enforcement agencies constituted factors which triggered the current reform process.[6]

The GDPR constitutes the *lex generalis* in the legal framework of personal data protection law. It introduced benefits both for business (mainly by the introduction of the one-stop-shop principle) and for citizens. Individuals, on the one hand, have been awarded new instruments—such as a right to be forgotten, easier access to one's data, a right to data portability, and a right to know when one's data has been hacked—enabling them to gain more control over their data. Data controllers, on the other hand, have been obliged to follow the principle of data protection by design and by default.[7] An institutional novelty of the GDPR is that the newly established European Data Protection Board has been equipped with the competence to issue binding decisions in the case of disputes between national data protection authorities, in addition to that of issuing guidelines on the application of the GDPR. Last but not least—and probably the most commonly known novelty—is, that the GDPR contains clear rules on the conditions for imposing administrative fines on legal entities which do not comply with the new EU rules. National data protection authorities in the Member States have already started making use of this competence.[8]

The ERA Annual Conference on Personal Data Protection in April 2018 was focused on personal data processing in a commercial context, with particular reference to the protection of personal data in the course of automated individual decision-making and profiling activities. The GDPR provides data subjects with new rights such as the right not to be subject to automated decision making and the right to data portability. The overall goal of the conference was to provide legal practitioners and data protection specialists with the necessary guidance on how to combine data sub-

[4]See e.g., Rec. 6 of the GDPR, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (20.11.2018).

[5]Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data—consolidated text/https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf (20.11.2018).

[6]*V. Reding*, The upcoming data protection reform for the European Union, International Data Privacy Law, Volume 1, Issue 1, 1 February 2011, p. 3. https://academic.oup.com/idpl/article/1/1/3/759666, 22 November 2018.

[7]See on that *L. Jasmontaite, I. Kamara, G. Zanfir-Fortuna, S. Leucci*, Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR, European Data Protection Law Review, Vol. 4 (2018), Issue 2, p. 168–189.

[8]The first example comes from Portugal where Data Protection Authority imposed €400,000 fine on Hospital for the non-compliance with the GDPR, notably for violation of confidentiality of patients' data and non-conformity with the principle of data minimization.

jects' rights as provided for by the General Data Protection Regulation (GDPR) with the demands of the contemporary economy. In this issue you will find a contribution of Professor Paul de Hert co-authored by Elena Gil González, presented at this year's annual conference on personal data protection entitled '*Practical guidance to the provisions in the GDPR on lawful grounds and on profiling. Fairness and transparency as guiding principles with some help of competition law*'. The authors address the issues of legal grounds for data processing according to the General Data Protection Regulation and the regime of profiling. They claim that certain concepts in the GDPR could undermine data subjects' rights. In such a case they see a solution in the principle of transparency and fairness of personal data processing and, interestingly, see this outside data protection legislation, for instance in competition law.

It may be assumed that the European Commission deliberately decided to use a regulation as an instrument of legal integration in the field of data protection rather than, as previously, a directive. In the first place, using a regulation enables speedy implementation. Secondly, it ensures effective implementation without discrepancies occurring between Member States. While the application of a regulation in practice remains the domain of data controllers and processors across the EU and beyond, its interpretation by the Court of Justice is likely to attract much attention. In spite of the fact that the GDPR has not yet formed the basis for any case-law by the Court, there is already an increasing number of cases related to Directive 96/45 and the fundamental right to privacy which have either already been decided by the Luxembourg Court in recent times or are still pending before the court.[9] In order to address the new jurisprudence on data protection and privacy matters ERA plans to organise a dedicated conference in December 2019.

Due to the specificities of data protection in criminal matters, the EU legislator decided to regulate the issue of personal data protection in the field of law enforcement in a separate legal act.[10] The adoption of a directive on the protection of personal data relating to cooperation in criminal matters in the EU certain. In this context, questions may arise as to the practical implications of the adoption of this directive for the protection of the rights of individuals involved in criminal offences. It can be questioned whether a clear, coherent and predictable system of protection of rights has been created in this area. Similarly, the necessity of the enactment of a separate regulation in this area might be doubted. In order to address *inter alia* these topics ERA organised a conference on Data Protection in the Judiciary (held on 18–19 October 2018 in Vienna) and co-organised the conference 'Freedom and Security' with Europol's Data Protection Experts Network (EDEN) (held on 22–23 November 2018 in The Hague).

[9]See e.g. Case C-687/18 *Associated Newspapers, Facebook Ireland and Schrems*, Case C-311/18, C-623/17 *Privacy International*, Case C-345/17 *Buivids*, Case C-136/17 *G. C. and Others* (*Déréférencement de données sensibles*), Case C-40/17 *Fashion ID*, Case C-25/17 *Jehovan todistajat*, Case C-136/17 *G. C. and Others* (*Déréférencement de données sensibles*).

[10]Additionally on 27 April 2016, the European Parliament and the Council adopted Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (The PNR Directive). The provisions of the directive oblige air carriers to transfer the PNR data of passengers on international flights to the Member States of arrival or departure, where the PNR data are to be analysed and used for the purpose of fighting serious crime and terrorism.

It should be noted that the rules for the processing of personal data in the Law Enforcement Directive are largely consistent with the general data protection norms laid down in the GDPR. Certain exceptions, however, are required by the specificity of cooperation in criminal matters and for reasons of public interest. While in the general data protection system it is assumed that the processing of personal data is substantially dependent upon the consent of the personal data subject, consent cannot be used to the same extent as a legal basis for data processing in the activities of judicial authorities. In accordance with the principle of legality, the processing of such data should be carried out on the basis of a legal act and in accordance with the legal grounds set out in that act. Such processing should be carried out solely in connection with the fulfilment of specific tasks provided for by law. Other differences relate to the broad understanding of the principle of the purpose limitation of data processing and to the modification of information obligations towards data subjects. Another novelty is also that the Directive urged Member States to differentiate regarding the categories of data processed as between different categories of data subjects. The concrete implementation of this provision and therefore the final determination of which data shall be processed in relation to a given data subject remains within the competence of Member States.

The GDPR and the Law Enforcement Directive are not the only new legal acts in the field of data protection. On 21 November 2018, the long awaited Regulation 2018/1725 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and the free movement of such data and repealing the Regulation No 45/2001 was published.[11] Its purpose is to align data protection principles in EU institutions (i.e., to the GDPR). The Regulation, which became effective as of 12 December 2018, strengthens the role of the European Data Protection Supervisor (EDPS), who is able to fine EU institutions or bodies which do not comply with new provisions. In order to discuss the new Regulation on data protection in EU Institutions, ERA decided to organise a conference in January 2019 dealing with the main novelties, which include the new powers of the European Data Protection Supervisor and processing of operational personal data. Another novelty is also that the revised Regulation will apply to Eurojust as soon as the reform of this agency is completed and furthermore, that in 2022, the rules should be extended to Europol and the European Public Prosecutor's Office.[12] This seems to have been the most debated part of Regulation 2018/1725.

As yet unknown is the date of entry into force of the proposed E-Privacy Regulation which aims at adjusting the level of privacy in electronic communications and internet services to GDPR standards.[13] In this context it is worth mentioning that the E-Privacy Regulation should be treated as *lex specialis* in relation to the GDPR, tailoring its provisions to electronic communications data that are personal data. The substitution of the previously valid E-Privacy Directive by a regulation should—similarly to the case of the GDPR—help to unify diverging e-privacy rules

[11] [2018] OJ L 295/39.

[12] http://www.europarl.europa.eu/news/en/press-room/20180906IPR12126/stronger-data-protection-rules-for-eu-institutions-and-agencies (22 November 2018).

[13] On 10 January 2017 the European Commission adopted a proposal for a Regulation on Privacy and Electronic Communications to replace the 2009 Directive.

between the Member States of the EU. In particular legal certainty for users and businesses alike is intended to be safeguarded by avoiding divergent interpretations in the Member States. The areas of unsolicited marketing, cookies and confidentiality are covered in a more specific context. The enforcement mechanisms of GDPR and E-privacy Regulation remain however the same. This is due to the fact that the same authority is going to be responsible for the enforcement of the GDPR as for the E-Privacy Regulation. The implications and novelties of the upcoming E-privacy Regulation are to be addressed in ERA's Annual Conference on Data Protection 2019 scheduled for 28–29 March 2019.

Due to the amount and variety of legal acts in the field of data protection, the challenge for national legislators will undoubtedly be to safeguard coherence between all the legal acts in this area. It should be borne in mind that as a result of the application of the GDPR, numerous issues such as certification mechanisms, the organisation of national Data Protection Authorities and the procedure in the event of infringements of data protection provisions shall be laid down at domestic level. At the time of writing, the process of adoption of relevant sectoral provisions on a national level as the result of GDPR application may already be observed.

Even more legislative work is necessary for the implementation of the Law Enforcement Directive on the national level. Whether the aim of the Directive, which is the increase of mutual confidence and the effectiveness of the same data exchange in criminal matters, will be achieved depends to a large extent on how the provisions of the Directive are implemented. It also remains to be seen how the Directive will be implemented in practice and which prerogatives will be left to data protection authorities. Due to the fragmentation of the system being created, certain concerns about its transparency and internal coherence may however arise.

We hope you enjoy reading this issue of ERA Forum.