30 András Jóri – Andrea Klára Soós: Data Protection – The Hungarian and European Regulations

János Czigle[*]

Jóri András – Soós Andrea Klára: Adatvédelmi jog – Magyar és európai szabályozás, HVG-ORAC Lap-és Könyvkiadó Kft., 2016., p. 372; ISBN 978 963 258 306 8

Many professionals have long called for the modernization of the Data Protection Directive, in order to better adapt to the changes taking place in the realm of information technology, and to respond to the increasing precariousness of privacy, considered to be 'under siege' both online and offline. It was also feared, that the pace of technological developments may be too fast for legislation to keep up with. Finally, in 2016, following years of preparation and professional debates the General Data Protection Regulation – in short GDPR[1] – was finally approved as the new legal foundation for the European Union's data protection framework. The Regulation will be enforceable from 25 May 2018 replacing the existing Data Protection Directive,[2] which had been in effect for over twenty years. The GDPR seeks to ensure a higher level of protection of EU citizens' personal data, applying to all organizations holding such data, regardless of where they are based in the world. Owing to its nature as a Regulation, the GDPR will not require any national legislative procedures to become enforceable, and will be directly binding and applicable in all EU Member States, promoting legal unification. Its focus reflects the greater emphasis and attention afforded to the growing importance of data protection in Europe and the wider world.[3]

Attorney András Jóri is a renowned professional in the field of data protection, having served as Parliamentary Commissioner for Data Protection and Freedom of Information, and being a member of the Public Body of the MTA (Hungarian Academy of Science). Andrea Klára Soós is an attorney who gathered significant IT and data protection experience in her work with multinational companies. Their abundant theoretical and practical

* János Czigle, PhD researcher at Pázmány Péter Catholic University Faculty of Law and Political Sciences, Budapest.

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.

2 Directive 95/46/EC.

3 For example the NSA-scandal or the election hacking claims, touching base on the issue of cybersecurity as well.

experience is well reflected in the consistent structure of the monograph itself, contributing to a useful handbook for both legal professionals and those active in other sectors, but nevertheless interested in this particular field.

The monograph focuses on the GDPR and its effects on the European, especially Hungarian data protection regulations, while citing and also analyzing the relevant case law. The handbook kicks off with an introduction to the general theoretical socio-legal background, the principles as well as the history of the data protection in Europe and the United States, citing the modern classics such as Westin, presenting the well distinguishable approaches and perceptions, along with the so called 'generations' of data protection-related legislature. The two legal systems pursue a rather different approach, resulting in differences unfolding in their theoretical and practical approach: in the USA data protection maybe considered to be a part of privacy rights, and as such it enjoys legal safeguards similar to those attached to property rights, while in Europe, the core element is the 'private sphere' as the authors do not fail to emphasize.

The relevant Hungarian data protection legislation – Act CXII of 2011 on the Right to Informational Self-determination and Freedom of Information in short DPA – is introduced in parallel to and compared with the GDPR, analyzing and identifying similarities, differences, highlighting novelties, such as the more severe legal consequences for the breach of the Regulation. The so called 'Privacy Shield' bilateral agreement on data transfer between the EU and the USA is also mentioned, such as the famous *Schrems* case which resulted in the nullification of the 'Safe Harbour' framework. However, here the authors unfortunately do not go into further detail. Though these issues are not directly related to the central topic of GDPR, it would definitely be a topic worth elaborating on.

The introduction to the GDPR and the DPA starts with the definition of personal data. The GDPR uses a marginally different language and will most likely not have practical consequence as very accurately stated by the authors. This definition is then analyzed for its components such as the *data subjects*, the *connection* between the data subject and the data. Similarly to the other chapters of the monograph, relevant case law is cited for deeper understanding, such as the *Weltimmo* case or the issue of Google Street View, including also cases from the practice of the Hungarian *National* Authority for *Data* Protection and Freedom of Information, creating a consistent theoretical framework.

The scope of the Regulation and the DPA is analyzed in depth, with reference to the above mentioned *Weltimmo*- case and the Google Spain case. Since the Regulation is a secondary source of European Union law, it will be directly applicable in Hungary as well, even though the Hungarian DPA in some cases is more stringent. These extra requirements enacted by the national legislator are however consistent with the purpose of the GDPR, and as such are permissible under CJEU case law. Hence, additional requirements imposed by the national legislator do not necessarily amount to a breach of European law, on the contrary, they may be viewed as a further extension of the GDPR. The Reg-

ulation introduces a broader legal basis for data management than the DPA, since the latter adopted the language and wording of the earlier legislation and referred to the former Constitution and the decisions of the Constitutional Court as a starting-point. In addition, the GDPR gives significantly more weight to the act of consent, providing detailed guidance. The book also highlights the main issues of concern, for example the question of awareness and its degree, especially in the case of children, public figures, the legally incapacitated, also indicating the issues surrounding sensitive data regarding religious beliefs, ethnic or racial origins etc. The voluntary aspect of providing consent is also noted, supplemented by scenarios, where providing data is mandated by law or by means of a tertiary legislation.

The basic principle of purpose limitation plays a prominent role in both the GDPR and the DPA and is investigated on a case by case basis although from among recent case law the prominent Barbalescu case was omitted, in particular, regarding workplace data collection and processing. For such activities to be lawful, an enabling legal act is required, clearly stating the process and the extension of data collection and control. Principles of fairness, lawfulness and transparency are also imperative, along with the principle of data minimization, accuracy and storage limitation, integrity and confidentiality. Accountability received its own chapter, given its increased importance. After laying down the above fundamentals of privacy law, the analysis moves on to data processing and the data processors – distinguishing them from the data controllers detailed in the previous chapters – i.e. those organizations that are entitled to hold and process personal data, with ensuing legal problems surrounding privacy and international organizations or cyber security. Processors are obliged to maintain records of the personal data they possess as well as their processing activities, while liability and legal consequences like fines are much higher in their case.

One of the most important novelties of the GDPR is the regulation of the transfer of personal data to third countries and international organizations which it regulates in much greater detail than the DPA does. For this type of transfer the Regulation imposes strict conditions, and allows it only where the destination country provides the same level of security as the European Union does. From the list of such countries, Canada and the United States must satisfy additional requirements as well. Canada must meet the criteria set forth in the Personal Information Protection and Electronic Documents Act, while organizations in the USA comply with the Privacy Shield agreement on a voluntary basis, after registering with the U.S. Department of Commerce. A similar agreement was concluded between Switzerland and the EU as well. BCR – Binding Corporate Rules – are also perceived as an additional layer of data protection, but their effects have yet to be seen. This novel instrument is thoroughly analyzed, nevertheless, the past month has seen developments in new case law that would require a revision of the. Finally, BREXIT created a new scenario also from the vantage point of data protection, not to mention

recent fines the European Commission imposed on internet giants such as Facebook in the past couple of months.

Notification of the data subject of the fact of data processing is thoroughly regulated in both the DPA and the GPDR. This is essential for the data subject to be able to exercise their specific rights, such as correction, control and the so called 'right to be forgotten', which means that individuals may sever access to sensitive and private information about them, which may have damaging effect on their social or economic status.

The monograph ends with an annex, containing the text of the GDPR and the DPA in their entirety. Perhaps a compilation of relevant case law would have been even more useful. It is not the goal of this monograph or 'handbook' to highlight a specific challenge or novelty in the area of data protection, but it much rather intends to provide an overall picture of the field of privacy law, offering a comprehensible overview of the relevant law to interested readers. As such it is useful for those legal professionals, who are employed at multinational companies, teach or simply study data protection, which itself is an area prone to constant change and development.