EDITORIAL NOTE

Two-Year Anniversary of the GDPR: Where Do We Stand?*

The European Union's (EU's) General Data Protection Regulation[1] (GDPR) is well into its second year. The GDPR is one of the most significant and talked-about pieces of legislation in the recent past. Its ambitious and substantial developments included extraterritorial application, extensive transparency and information requirements, the right to be forgotten, data portability, data protection impact assessments, data breach reporting, accountability, and, of course, hefty administrative fines, to name a few.

As Andrus Ansip, then Vice-President for the Digital Single Market, and Věra Jourová, then Commissioner for Justice, Consumers and Gender Equality, stated on its first anniversary last year, 'The GDPR has changed the landscape in Europe and beyond'.[2] A year later, this statement proves to be even more true.

Considering this, and in lieu of a second birthday cake, this second edition of the Global Privacy Law Review (GPLR) focusses on the GDPR.

In our previous and special issue on new and emerging technologies, we analysed, among other things, how these have transformed our lives over the last twenty-five years and will continue to do so unceasingly.[3] We also recognized the new privacy and data protection challenges posed by ever-advancing technology.

Those were the very same challenges that prompted the European Commission (Commission) to propose 'a fundamental reform' of the EU's 1995 Data Protection Directive.[4] Following a number of public consultations throughout 2009 and 2010,[5] the Commission engaged in enhanced dialogue with Member States' data protection authorities and the European Data Protection Supervisor to look at applying data protection rules more consistently across the EU. Further to these consultations, on 25 January 2012, the Commission concluded[6]:

> The EU's 1995 Directive, the central legislative instrument for the protection of personal data in Europe, was a milestone in the history of data protection. Its objectives, to ensure a functioning Single Market and effective protection of the fundamental rights and freedoms of individuals, remain valid. However, it was adopted 17 years ago when the internet was in its infancy. In today's new, challenging digital environment, existing rules provide neither the degree of harmonisation required, nor the necessary efficiency to ensure the right to personal data protection. That is why the European Commission is proposing a fundamental reform of the EU's data protection framework.

On 27 April 2016, four years after the Commission's proposal,[7] the EU adopted the GDPR. It entered into force on 24 May 2016[8] and has applied since 25 May 2018.[9] It replaced the 1995 Data Protection Directive

Notes

* Special thanks to Nick Potter (Linklaters, Madrid) for proofreading this editorial note.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 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), Official J. L. 119, 1–88 (4 May 2016).

2 European Commission Press Release, General Data Protection Regulation: One year on, 22 May 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2610.

3 1(1) Global Privacy L. Rev. (2020).

4 Directive 95/46/EC on the protection of individuals with regard to the protection of personal data and on the free movement on such data, OJ. L. 281, 31 (23 Nov.1995).

5 The Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data from 9 July to 31 Dec. 2009, and the Consultation on the Commission's comprehensive approach on personal data protection in the European Union from 4 Nov. 2010 to 15 Jan. 2011.

6 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World a European Data Protection Framework for the Twenty-First Century, COM/2012/09 final.

7 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM/2012/011 final.

8 Article 99(1) of the GDPR states, 'This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*'. The publication date was 4 May 2016.

9 Article 99(2) of the GDPR.

© 2020 Kluwer Law International BV, The Netherlands

that was adopted at a time when most of today's technologies were in early development or simply did not exist.

Although not perfect or entirely free of controversy or criticism,[10] the GDPR is an important milestone in data protection and has been regarded as a new *gold standard* for data protection across the world.

The EU's regulation led the world, from Australia[11] to Brazil[12] to India,[13] to review their national legislation or enact or propose 'GDPR-like' privacy and data protection laws. Perhaps the most notable is the California Consumer Privacy Act (CCPA), which constitutes the most comprehensive privacy law in the United States. It was signed into law on 28 June 2018 and came into force on 1 January 2020.

The CCPA gives California residents similar protections to those established by the GDPR and control over their 'personal information' defined broadly as any data that 'identifies, relates to, describes, is capable of being associated with or could be reasonably linked, directly or indirectly, with a particular consumer or household'.[14] Accordingly, personal information includes, among other things, IP addresses, browsing or internet search histories, information regarding a consumer's interaction with a website or advertisement, geolocation data, professional or employment-related information, and education information. The CCPA specifies that any 'inferences drawn' from different data elements of personal information to 'create a profile about a consumer reflecting the consumer's preference, characteristics, psychological trends, preferences, predispositions, behaviour, attitudes, intelligence, abilities, and aptitudes' are also considered personal information.[15]

Prof. Jordan M. Blanke (*Protection for 'Inferences Drawn': A Comparison Between the General Data Protection Regulation and the California Consumer Privacy Act*) analyses the protection for 'inferences drawn' from personal information under the CCPA. He writes that inferences drawn from personal data have arguably become more dangerous to individual privacy than the vast collection and storage of the data itself.[16]

Blanke notes that questions have been raised recently about whether the GDPR provides sufficient protection for these inferences. He concludes that, probably not surprisingly, the CCPA specifically includes 'inferences drawn' as part of its definition of personal information. He explores the widespread use of inferential data and compares the protection provided under the GDPR and the CCPA.

Laura Drechsler (*Comparing LED and GDPR adequacy: One standard two systems*) compares adequacy assessments under the Law Enforcement Directive (LED) and the GDPR. She notes that the 2015 *Schrems* case established that to get an adequacy decision authorizing personal data transfers from the EU to a third country, that third country has to ensure a level of protection of fundamental rights and freedoms 'essentially equivalent' to that in the EU. Drechsler notes that, since May 2018, the Commission has had sole authority to make assess third-country adequacy decisions in relation to both the GDPR and LED. So far, there have been no LED adequacy findings.[17]

Drechsler proposes a comparative analysis of adequacy decisions under both EU instruments to assess whether GDPR adequacy findings could serve as guidance for decisions under the LED, as suggested by the Commission. She further argues that LED adequacy decisions would have to be properly separated from GDPR findings, as even though they aim to achieve the same standard of essential equivalence, their system of protection in relation to the processing of personal data in a law enforcement context differs.

Maja Nišević (*Profiling consumers through Big Data Analytics: Strengths and weaknesses of Article 22 GDPR*) argues that Big Data gives rise to new forms of knowledge production through data analysis techniques: profiling. She defines profiling generally as any form of discovering or constructing knowledge from large sets of data originating from a variety of sources; and in a narrow sense, as a way of drawing up individual profiles, which are sets of characteristics, features, and attributes through which a person or group can be discerned from another person or group.[18]

Notes

[10] Winfried Veil, *The GDPR: The Emperor's New Clothes – On the Structural Shortcomings of Both the Old and the New Data Protection Law*, 10 Neue Zeitschrift für Verwaltungsrecht 686–696 (2018). SSRN, https://ssrn.com/abstract=3305056.

[11] On 12 Dec. 2019, the Australian Government released its response and implementation roadmap to the Australian Competition and Consumer Commission's Digital Platforms Inquiry. The Australian Government's response includes 'conducting a review of the Privacy Act and ensuring privacy settings empower consumers, protect their data and best serve the Australian economy'. *See* the Australian Government's response to the Digital Platforms, https://ministers.treasury.gov.au/ministers/josh-frydenberg-2018/media-releases/response-digital-platforms-inquiry.

[12] Brazilian General Data Protection Law, *Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018* published on 15 Aug. 2018.

[13] On 24 Aug. 2017, the Supreme Court of India in its landmark judgment *Justice K. S. Puttaswamy (Retd.) and Anr. V. Union of India and Ors.* unanimously held that 'the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution'. This led to the Personal Data Protection Bill 2019.

[14] Section 1798.140 (o) (1) of the CCPA.

[15] Section 1798.140 (o) (1) (K) of the CCPA.

[16] Jordan M. Blanke, *Protection for 'Inferences Drawn': A Comparison Between the General Data Protection Regulation and the California Consumer Privacy Act*, in this issue, at 81.

[17] Laura Drechsler, *Comparing LED and GDPR Adequacy: One Standard Two Systems*, in this issue, at 93.

[18] Maja Nišević, *Profiling Consumers Through Big Data Analytics: Strengths and Weaknesses of Article 22 GDPR*, in this issue, at 104.

Nišević argues that profiling is a relatively new concept in EU data protection law and that Article 22 of the GDPR is ambiguous. She focusses on its interpretation by analysing its wording, limitation and potential regulatory gaps.

Under the report section, Thiago Luís Sombra (*The General Data Protection Law in Brazil: What comes next?*) analyses the new Brazilian Data Protection Law (LGPD) coming into force in August 2020. Sombra notes that Brazil was one of the few countries among the major global economies not to have a regulatory framework for personal data protection, which has been regulated through various legislation such as the Civil Rights Framework for the Internet, Civil Code, and the Consumer Protection Code.[19]

Sombra argues that, similar to the data protection principles of the GDPR, the LGPD's general principles, including purpose limitation, necessity, open access, transparency, security, liability and accountability, aim to adjust the balance of power, increase transparency and responsiveness, and empower data subjects in their interactions in cyberspace.

Finally, in the case note section, Raul Torres and Carlos González Uli (*The ECHR Grand Chamber 'López Ribalda II' judgement dated 17 October 2019. Analysis on the validity of concealed cameras based on case law from the Spanish Constitutional Court*) analyse the recent judgment of the Grand Chamber of the European Court of Human Rights (ECHR), in the case known as 'López Ribalda II', which assessed the validity of video surveillance evidence in the context of a Spanish employment dispute following dismissal. Torres and González conclude that the ruling of the ECHR justifies the use of hidden cameras to monitor an employee, when there are reasonable suspicions of irregularities, the decision is proportionate and there are no less intrusive measures.[20]

Torres and González also examine the view of the Spanish Constitutional Court and the first judgment of the ECHR in the López Ribalda case, in order to understand the evolving position and the importance of the new ECHR decision for the future of employment relationships.

We hope you will enjoy reading GPLR's second GDPR-special issue.

Happy Birthday GDPR!
Ceyhun Necati Pehlivan
Editor-in-Chief
IE Law School

Notes

[19] Thiago Luís Sombra, *The General Data Protection Law in Brazil: What Comes Next?*, in this issue, at 116.

[20] Raul Torres & Carlos González Uli, *The ECHR Grand Chamber 'López Ribalda II' Judgment Dated 17 Oct. 2019. Analysis on the Validity of Concealed Cameras Based on Case Law from the Spanish Constitutional Court*, in this issue, at 720.