MAYER | BROWN

May 2019

Legal Update

The GDPR: One Year On

The European General Data Protection Regulation (GDPR) came into force on 25 May 2018. In this article, we look back at its impact and the trends relating to its interpretation and enforcement over the last twelve months.

1. INCREASED PERSONAL DATA BREACH NOTIFICATIONS

The EU data protection supervisory authorities (DPAs) have seen a huge increase in the number of personal data breaches being reported, to comply with the "without undue delay" / 72-hour breach notification deadline under GDPR, with over 89,000 personal data breaches being notified to DPAs in just under the first twelve months.[1] The broadened definition of personal data (and therefore the types of incidents involving data that constitute a personal data breach) and the introduction of a standardised notification requirements with penalties for failure to comply has substantially increased the number of reported incidents. Only 63% of cases investigated by DPAs have been closed.[2]

2. INCREASED REQUESTS TO EXERCISE RIGHTS BY DATA SUBJECTS

GDPR has granted data subjects greater rights relating to their personal data, including the right to data portability, and further promoted existing rights of erasure and access. Significant publicity about this in advance of the implementation of the GDPR has naturally led to an increase in awareness by data subjects of their rights and a substantial increase in the number of requests being received to exercise those rights[3].

3. COMPLAINTS

Over 144,000 queries and complaints are reported to have been made to DPAs by individuals who believe their rights under GDPR have been violated. The majority of these complaints have concerned activities including telemarketing, promotional emails, and video surveillance/CCTV.[4] Lack of transparency and information provided by controllers about the processing activities they conduct and insufficient consent being sought to conduct processing activities have been a regular subject of complaints.

4. ENFORCEMENT

For the first few months after GDPR came into force, DPAs conducted exploratory investigations, offered recommendations and gave time to companies to improve compliance with GDPR. This initial phase lasted a few months, after which DPAs have increased their investigations and enforcement efforts.[5]

- **Investigations** – In just under the first twelve months, DPAs initiated 446 cross-border investigations, following individuals' complaints and on their own initiative.[6]
- **Orders requiring the temporary or indefinite suspension of processing** – DPAs have ordered the suspension of processing by certain organisations as a means of enforcement. For example:

1 https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en
2 https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en
3 http://www.pulsetoday.co.uk/partners-/practice-business/bma-subject-access-requests-to-gps-increased-by-more-than-a-third-since-gdpr/20037951.article
4 https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf
5 https://gdpr.report/news/2019/04/30/gdpr-one-year-on-what-have-we-learned/
6 https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en

- The UK DPA ordered a Canadian based political consultancy and technology company to erase all personal data held by it belonging to individuals in the UK by reference to the domain names used in the email addresses relating to those individuals.[7]
- The Dutch DPA sanctioned the country's tax authorities for using the national identification number as part of the VAT return number for self-employed individuals. The DPA stated that the use of the national identification number had no legal basis and increased the risk of identity fraud. As of 1 January 2020, the processing of the national identification number for VAT purposes is prohibited.[8]
- Malta's DPA imposed a temporary suspension of processing on the country's national land register while it investigated how the national land register has been responding to a personal data breach.[9]

- **Fines**
  - One of the key features of GDPR is that DPAs are able to impose significant fines for failures to comply with European data protection law. These fines can reach up to 4 percent of an organisation's annual global turnover in the preceding financial year per infringement. So far, whilst fines have been issued by DPAs under the GDPR, substantial fines have been rare. In the first nine months of the GDPR coming into force, the total fines issued by DPAs totalled just over €55 million [10].
  - Fines included:
    - The State Commissioner for Data Protection and Freedom of Information Baden-Wuerttemberg, a German DPA, fining a social media/chat platform €20,000 for its data storage practices, after it discovered that over 800,000 user passwords and email addresses were compromised as a result of them being stored in an accessible format.[11] The swift response and remediation of the incident by the social media platform following its discovery is thought to be the reason for the low level of fine issued.
    - The Portuguese DPA fining a hospital €400,000 after determining that patient records could be accessed by IT users not entitled to see them using accounts that were being held in the names of doctors not practicing at the hospital.[12]
    - The Polish DPA fining a digital marketing company €220,000, for aggregating personal data concerning over six million individuals from publicly available registers without providing the data subjects to whom the information related with the information required to be provided under the GDPR when collecting personal data from sources other than the data subject. The Polish DPA also ordered the provider in question to send the required information to the six million individuals in question within a three month time frame (an exercise which the company estimated may cost in excess of €8 million if notices are sent to individuals by post).[13]

5. THE INFLUENCE OF THE GDPR IN OTHER COUNTRIES

The implementation of the GDPR has had an undoubted influence on the data protection laws and practices being adopted in other jurisdictions, with various countries taking inspiration from GDPR for their own data protection laws. The most common aspects of the GDPR influencing the laws and practices in other countries include the approach taken with respect to the provision and exercise of rights by individuals as well as the personal data breach and accountability requirements that have to be complied with by organisations that use personal data.[14]

7 https://ico.org.uk/action-weve-taken/enforcement/aggregate-iq-data-services-ltd/
8 https://gdpr.report/news/2019/04/30/gdpr-one-year-on-what-have-we-learned/
9 https://gdpr.report/news/2019/04/30/gdpr-one-year-on-what-have-we-learned/
10 http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf
11 https://www.welivesecurity.com/2018/11/27/german-chat-site-faces-fine-gdpr/
12 https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/
13 https://iapp.org/news/a/polands-dpa-issues-first-gdpr-fine/
14 https://gdpr.report/news/2019/04/30/gdpr-one-year-on-what-have-we-learned/

- Switzerland, Norway, Iceland, and Liechtenstein have aligned their laws relating to the processing of personal data with the GDPR.[15]
- Various U.S. states have passed or proposed laws that mirror some of the protections provided by GDPR, particularly data subject rights[16]:
  - » The California Consumer Privacy Act (CCPA), which comes into force on 1 January 2020, is partly inspired by GDPR. It requires detailed information to be provided to individuals about how their personal data is being used and provides similar data subject rights to those provided under the GDPR, including the right to deletion and the right to data portability.[17]
  - » Other U.S. states have proposed laws similar to the CCPA, including Massachusetts, Illinois, New York, Maryland, and several others. While the proposed laws are all based on the CCPA, their scope and obligations differ, which could potentially result in a patchwork of CCPA-like laws. Accordingly, federal data protection laws that would pre-empt such state laws are also being considered but none have passed.
- In Brazil, the Brazilian General Data Protection Law (LGPD) will come into force on 15 August 2020. The LGPD is inspired by and shares many elements in common with the GDPR.[18]
- In the Cayman Islands, the Cayman Islands Data Protection Law will come into force on 30 September 2019.[19]
- India is currently debating data protection legislation reflecting aspects of GDPR.[20]
- Various countries in Africa, such as South Africa[21] and South East Asia, such as Singapore and Indonesia[22], are also developing their data protection laws.[23]
- South Korea is updating its laws to achieve adequacy.[24]
- Japan received an adequacy decision on 23 January 2019, in relation to the export of personal data from the European Union to Japan. Japan has put in place a number of additional safeguards to ensure that personal data originating from the EU is adequately safeguarded under Japanese privacy laws.[25]

6. GUIDANCE

The EDPB have adopted previous guidelines issued on the GDPR by the Article 29 Working Party (the body which the EDPB has replaced) and has issued the following new guidelines on GDPR for consultation:

- Guidelines on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects[26] - the guidelines explain the narrow scope of the contractual necessity legal basis, which requires processing to be 'objectively necessary' for a purpose 'integral' to the delivery of a contractual service to the data subject.[27]
- Guidelines on Codes of Conduct and Monitoring Bodies under GDPR[28] – the guidelines provide practical guidance in relation to Articles 40 (codes of conduct) and 41 (monitoring of codes) of the GDPR. They provide a framework for assessing the procedures and the rules in relation to codes at both the national and European level.

15 https://gdpr.report/news/2019/04/30/gdpr-one-year-on-what-have-we-learned/
16 https://www.mayerbrown.com/en/perspectives-events/publications/2019/05/the-california-consumer-privacy-act--key-takeaways-for-insurers-and-insurance-regulators
17 https://www.mayerbrown.com/en/perspectives-events/publications/2018/07/california-enacts-gdprlike-consumer-privacy-protec
18 https://www.mayerbrown.com/en/perspectives-events/publications/2018/07/brazil-is-going-to-have-a-general-data-protection/
19 https://ombudsman.ky/data-protection
20 https://gdpr.report/news/2019/04/30/gdpr-one-year-on-what-have-we-learned/
21 https://www.saica.co.za/Technical/LegalandGovernance/Legislation/ProtectionofPersonalInformationAct/tabid/3335/language/en-ZA/Default.aspx
22 https://www.refinitiv.com/perspectives/big-data/navigating-gdpr-data-regulation-asia/
23 https://gdpr.report/news/2019/04/30/gdpr-one-year-on-what-have-we-learned/
24 https://gdpr.report/news/2019/04/30/gdpr-one-year-on-what-have-we-learned/
25 https://www.mayerbrown.com/en/perspectives-events/publications/2019/01/free-flow-of-personal-data-between-the-european-un
26 https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf
27 https://www.mayerbrown.com/en/perspectives-events/publications/2019/05/using-performance-of-a-contract-as-a-legal-basis-for-processing-in-the-context-of-online-services
28 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-20190219_guidelines_coc_public_consultation_version_en_0.pdf

- Guidelines on the accreditation of certification bodies under Article 43 of GDPR[29] – the guidelines aim to help member states, supervisory authorities and national accreditation bodies establish a consistent, harmonised baseline for the accreditation of certification bodies that issue certification in accordance with the GDPR.
- Guidelines on the territorial scope of GDPR[30] - the guidelines clarify what constitutes an establishment in the EU, the status of tourists and factors determining whether data subjects in the EU are being targeted.[31]

7. LOOKING AHEAD

Certification schemes - we anticipate that certification schemes, which are a way for organisations to demonstrate compliance with GDPR, will gain traction over the next year. The EDPB has published guidance on the accreditation of certification bodies[32] and the ICO has recently shown its support for certification schemes, welcoming enquiries from organisations interested in developing certification schemes and providing guidance on certification under GDPR.[33]

Class actions – whilst there has not been the deluge of group litigation that might have been expected under GDPR, we expect this will change over the next year, with the development of Article 80 representative bodies and claimant lawyers expected to gain a better understanding of the types of individual claims that have gained the most traction to date.

Brexit – Brexit is likely to have minimal impact, as the UK government has made it clear that it will seek an adequacy agreement with the EU, to ensure the continued flow of data between the UK and EEA countries. In the event of a no-deal Brexit, alternative transfer mechanisms, such as the Standard Contractual Clauses, can be used to ensure GDPR compliance.

For further information about the impact the GDPR is having on organisations that process personal data, trends on enforcement and the actions that your business should be taking to become or remain compliant with the GDPR, please contact one of the contacts identified below or your usual Mayer Brown contact.

Oliver Yaros
Partner, London
E: oyaros@mayerbrown.com
T: +44 20 3130 3698

Mark Prinsley
Partner, London
E: mprinsley@mayerbrown.com
T: +44 20 3130 3900

Charles-Albert Helleputte
Partner, Brussels
E: chelleputte@mayerbrown.com
T: +32 2 551 5982

Diletta De Cicco
Associate, Brussels
E: ddecicco@mayerbrown.com
T: +32 2 551 5945

Ulrich Worm
Partner, Frankfurt
E: uworm@mayerbrown.com
T: +49 69 7941 2981

Guido Zeppenfeld
Partner, Franfurt
E: gzeppenfeld@mayerbrown.com
T: +49 69 7941 2241

Lei Shen
Partner, Chicago
E: lshen@mayerbrown.com
T: +1 312 701 8852

Kendall Burman
Counsel, Washington DC
E: kburman@mayerbrown.com
T: +1 202 263 3210

29 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_4_2018_accreditation_en.pdf
30 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf
31 https://www.mayerbrown.com/en/perspectives-events/publications/2018/12/edpbs-new-draft-guidelines-on-the-territorial-scop
32 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_4_2018_accreditation_en.pdf
33 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/certification/

Mayer Brown is a distinctively global law firm, uniquely positioned to advise the world's leading companies and financial institutions on their most complex deals and disputes. With extensive reach across four continents, we are the only integrated law firm in the world with approximately 200 lawyers in each of the world's three largest financial centers—New York, London and Hong Kong—the backbone of the global economy. We have deep experience in high-stakes litigation and complex transactions across industry sectors, including our signature strength, the global financial services industry. Our diverse teams of lawyers are recognized by our clients as strategic partners with deep commercial instincts and a commitment to creatively anticipating their needs and delivering excellence in everything we do. Our "one-firm" culture—seamless and integrated across all practices and regions—ensures that our clients receive the best of our knowledge and experience.

Please visit mayerbrown.com for comprehensive contact information for all Mayer Brown offices.

0422ipt