SLAUGHTER AND MAY

Data Protection and Privacy Newsletter

July 2019 / Issue 11

Selected legal and regulatory developments in data protection and privacy

Quick Links

As the number and frequency of GDPR fines and enforcement actions increases, we are beginning to get an idea of the regulators' areas of focus: no longer is data breach the primary risk in town. As we discuss on page 3, regulators are also looking at organisations' broader GDPR compliance.

This message was confirmed by Elizabeth Denham when we heard her speak at the ICO's Data Protection Practitioners' Conference in May. She emphasised the importance of accountability and the need for data protection to be embedded in organisations from the board down and demonstrated by their policies and procedures, their DPO and their DPIAs. As the Commissioner said: "*Accountability encapsulates everything the GDPR is about. It enshrines in law an onus on companies to understand the risks that they create for others with their data processing, and to mitigate those risks.*"

A number of EU data protection authorities (DPAs) are also focusing on the interrelationship between tech and data protection compliance. In the UK, the ICO published its update report into adtech at the end of June. While the regulator concluded that the adtech industry still has substantial distance to travel to achieve GDPR compliance, the ICO's approach to bring about change seems relatively measured and pragmatic (see page 2).

In March we called for such regulatory pragmatism to be applied to blockchain technology in our ground-breaking joint publication with Cravath, Swaine & Moore: March of the blocks, GDPR and the Blockchain. The paper emphasises that with some innovative yet practical thinking from regulators and technology providers, technological solutions that respect the fundamentals of data privacy are achievable.

It is with this optimism that we look forward to the next few months' privacy developments!

Rebecca Cousin
Partner

Regulator guidance

Key pieces of guidance published by the Information Commissioner's Office (ICO) and the European Data Protection Board (EDPB) in the first half of 2019 are included in the table below.

Key Regulator Guidance	
ICO	
Right to be informed	March 2019
Age appropriate design: a code of practice for online services (draft for public consultation – closed 31 May 2019)	April 2019
Lawful basis for processing - Contract	June 2019
Cookies[1]	July 2019
EDPB	
Processing of personal data under Art 6(1)(b) GDPR (draft for public consultation – closed 24 May 2019)	April 2019
Guidelines on Codes of Conduct and Monitoring Bodies (version adopted after public consultation)	June 2019
Guidelines on certification and identifying certification criteria in accordance with Articles 42 and 43 GDPR (updated version including new annexes)	June 2019
Guidelines on the accreditation of certification bodies under Article 43 GDPR (updated version includes finalised Annex 1)	June 2019

Draft age appropriate design code

The ICO's **age appropriate design code of practice** sets out 16 standards expected of organisations designing, developing or providing online services which are "likely to be accessed by children", as required by s. 123 Data Protection Act 2018. Notably, the code has broad application as organisations do not need to be specifically targeting children to be in scope. The code requires affected organisations to have the best interests of children as their primary consideration when developing online services. Consultation on the code ended on 31 May 2019 and we are expecting the final version to come into effect by the end of the year.

ICO guidance: Adtech update report

At the end of June the ICO published an **update report on adtech and real time bidding**. The report follows a number of complaints about the adtech industry received by the ICO[2] and the ICO's own **adtech fact finding forum** in March. The report concludes that the adtech industry appears immature in its understanding of data protection and that the ICO has general, systemic concerns about the level of compliance in the industry. It focuses in particular on failings relating to lawful bases for processing and

[1] A high level alert on the new guidance will be published soon.
[2] Notably the ICO report references the concerns raised by **Michael Veale, Jim Killock and Dr Johnny Ryan** made in September 2018 and by **Privacy International** in November 2018.

issues around direct marketing, the treatment of special category data, and real time bidding supply chains.

Despite the ICO's robust conclusions, organisations should find some comfort in the ICO's pragmatic and iterative approach, which appears to focus more on continued engagement rather than immediate enforcement. For example, the ICO has given the industry six months to adjust its practices before it carries out a further review. Notably, the ICO acknowledges the economic vulnerability of smaller UK publishers, the complexity of the market, and ongoing industry initiatives as drivers for its measured approach. However, after this six month period, the ICO states it will expect market participants to have addressed the concerns identified in the report, which suggests that continued non-compliance could then trigger enforcement action.

Adtech is also on the radar of other DPAs[3]. For example, the Irish Data Protection Commission has **launched** a statutory enquiry into Google Ireland Limited's processing of personal data in the context of its online Ad Exchange. The Irish DPA received similar complaints as the ICO so it will be interesting to see how the DPAs approaches develop.

International transfers

Japan adequacy decision

On 23 January 2019 the European Commission **announced** the adoption of its adequacy decision on Japan, completing the process launched in September 2018. An equivalent decision was granted in favour of the EU by Japan, with both decisions effective from 23 January. Prior to the adoption of the adequacy decisions, Japan put a number of additional safeguards in place to ensure that data transferred from the EU was protected in line with European standards, including putting in place a set of supplementary rules to bridge differences between Japan and the EU's data protection systems, particularly in relation to the treatment of sensitive personal data. The adequacy decision will be subject to a joint review by Japan and the EU after two years, in January 2021, which should recognise and address any issues.

Looking towards future adequacy decisions, Bruno Gencarelli of the European Commission confirmed, at the Privacy Laws & Business Conference in Cambridge on 2 July 2019, that adequacy discussions between the EU and South Korea are at an advanced stage.

Standard Contractual Clauses: Schrems II case update

On **31 May 2019**, the Irish Supreme Court decided against Facebook and dismissed its attempt to stop the Irish High Court referring questions about the validity of the standard contractual clauses to the European Court of Justice (ECJ). A hearing date of 9 July 2019 has now been set for the ECJ to evaluate the validity of the standard contractual clauses in light of the **11 questions** referred from the Irish High Court to the ECJ last year. We will continue to monitor this case closely and are expecting a decision from the ECJ after the summer.

[3]The CNIL **announced** on 28 June that it has made targeted online advertising a priority topic for 2019-2020. It confirmed that it will repeal its 2013 cookie recommendations and publish new guidelines in July.

Brexit: glimpses of clarity

Although we have recently been enjoying a brief hiatus in Brexit focus as there is a cast-change in Westminster, the last six months have seen a number of incremental developments in the UK and EU's data protection preparations for Brexit, although unhelpfully no developments in relation to the EU's adequacy assessment for the UK:

- in February the EDPB published information notes on **data transfers under the GDPR in the event of a no-deal Brexit**; and **BCRs for companies which have the ICO as their BCR Lead Supervisory Authority** confirming that companies transferring personal data from the EU to the UK will need to put safeguards in place, likely to be the standard contractual clauses in most cases, and organisations with the ICO as lead BCR authority will need to identify a new lead authority within the EU post-Brexit;

- the UK has been added to a number of countries' "white lists" to receive free flows of data (without additional protections being required) following Brexit, including Japan, Guernsey and the Isle of Man; and

- the US has **confirmed** that Privacy Shield participants need to make only minor amendments to their public commitment to comply with the Privacy Shield, to include the UK, to enable them to receive transfers of personal data from the UK in reliance on the Privacy Shield following Brexit.

For more information on Brexit and data protection see our **January 2019 newsletter** and our publications, **Brexit: Edging Closer** and **Brexit Essentials: an update on data protection and privacy**.

Enforcement overview

Focus shifts to transparency, consent and data retention

As has been widely reported, in January the French DPA, the CNIL, brought the first headline-grabbing GDPR fine of €50 million against Google for failing to comply with its transparency obligations and for processing on the basis of invalid consent. This action was significant as it proved both that DPAs were prepared to use the GDPR's financial penalty fire-power and that their focus would be on broad GDPR-compliance, rather than just data security breaches. Subsequent DPAs' actions have followed a similar trend.

For example, the Polish DPA took a hard line in relation to transparency obligations in their **action announced in March**. It found that the controller in question (a company providing entity verification services) could not rely on the "disproportionate exemption" in relation to the provision of transparency notices to data subjects for whom the controller did not have email addresses. This was despite the very significant cost of providing the information to them by post (reported to have been higher than the company's total turnover from 2018). The ICO's most **recent guidance** on the availability of the disproportionate exemption suggests that the ICO would have adopted a more pragmatic line, indicating there may not be complete alignment between different supervisory authorities in terms of their GDPR interpretation and enforcement priorities.

A number of recent fines issued by DPAs have stated data retention/data deletion issues as one of the reasons for the fine. See for example the Danish DPA's fines against taxi firm Taxa 4x35 and furniture company IDdesign in the table below. It is worth noting that the Taxa fine, although less than 200,000 euros was reported to be 2.8% of the organisation's turnover. This level of fine was justified, in a large part, because the controller retained data in non-anonymised form for three years longer than the two years they told the DPA they held it for. Data retention and deletion should therefore be an area of focus for organisations in the next year.

The table below sets out a selection of the most significant GDPR fines brought by DPAs to date, along with an indication of the principal areas of non-compliance addressed by each enforcement action.

DPA (Country)	Company	Amount	Date	Description
AEPD (Spain)	La Liga	€250,000	11 June 2019	• Unlawful processing • Unlawful consent
CNIL (France)	SERGIC	€400,000	6 June 2019	• Data breach • Data security • Data minimisation
Datatilsynet (Denmark)	IDdesign	€200,800	3 June 2019	• Data minimisation
UODO (Poland)	Bisnode	€220,000	26 March 2019	• Transparency
Datatilsynet (Denmark)	Taxa 4x35	€161,000	26 March 2019	• Data minimisation
Datatilsynet (Norway)	Bergen Municipality	€170,000	March 2019	• Data security
CNIL (France)	Google	€50,000,000	21 January 2019	• Transparency • Unlawful consent
CNPD (Portugal)	Centro Hospitalar Barreiro Montijo	€400,000	17 July 2018	• Data minimisation • Data security

More fines soon

The UK and Irish Commissioners indicated in May that they each planned to issue their first significant GDPR-level fine over the next few months and Elizabeth Denham confirmed this during her session at this week's Privacy Law & Business Conference in Cambridge.

E-marketing: EE enforcement action

Although the ICO frequently takes enforcement action against companies for breaches of the direct marketing rules, the recent EE action of 24 June is worth highlighting. This is because the ICO appears to have taken a particularly strong position as to what amounts to a 'marketing' message as opposed to a 'service' message.

The ICO **fined** EE Limited £100,000 for failing to comply with the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). The enforcement action related to messages sent by EE to its existing customers in 2018 to encourage them to download and use the "My EE" app. Of the 16,620,416 messages sent by EE, 2,590,456 were sent to individuals that had already opted-out of receiving marketing from the company. EE considered the messages to be service messages and outside the scope of the direct marketing regime. However, the ICO concluded they were marketing on the basis that: a first message to individuals included reference to users upgrading their iPhones (which the ICO held to be a promotion); and users had the option to make additional purchases (such as upgrades) by logging in to the "My EE" app. By sending marketing to users who had opted-out, EE was found to be in breach of PECR.

The ICO's conclusions and the level of fine imposed can be explained to some extent by the significant aggravating factors present in the case, including the sheer number of individuals targeted with the marketing messages and the very substantial number of opt-outs; and the fact that users received a first message that was then followed up by a second message. The ICO's new Direct Marketing Code of Practice is due to be published imminently[4], and may provide more clarity on the service message/marketing message distinction.

Case law update

Dawson-Damer v Taylor Wessing

In the latest judgment in this long-running case[5] concerning data subjects' right of access, the High Court issued an important clarification on the definition of "relevant filing system" under the Data Protection Act 1998 putting forward a broader interpretation, with implications for the equivalent definition under the GDPR. The Court concluded that contrary to the finding in *Durant*[6], it is not necessary for a "manual filing system" to closely replicate the search-functionality of a computerised system (for example by having a sophisticated and detailed index). Instead, the Court followed the *Tietosuojavaltuutettu*[7] ECJ case and held that a "relevant filing system" requires three elements: (i) the data must be structured by reference to specific criteria; (ii) the criteria must be "related to individuals"; and (iii) the specific criteria must enable the data to be easily retrieved. Significantly, the Court took a broad view of what amounted to "easily retrieved" on the facts: it held that a search requiring a trainee solicitor to leaf through 35 chronologically-ordered files page by page was not unduly onerous. The personal data in question were still "easily retrieved" and the files in question constituted a "relevant filing system".

Organisations should take note of this judgment as it has implications for the application of the GDPR to legacy paper files. More historic files will potentially be within the scope of subject access requests and within the remit of the GDPR's obligations for data accuracy and data minimisation. Given the focus we are seeing from DPAs on data retention issues, this case provides further encouragement for organisations to reassess their data deletion and file destruction programmes.

[4] The ICO is expected to publish the Code for consultation in June: see p. 8 of the **ICO's GDPR: One year on publication**.
[5] *Dawson-Damer v Taylor Wessing* [2019] EWHC 1258 (Ch).
[6] Durant v Financial Services Authority [2003].
[7] Proceedings Brought by Tietosuojavaltuutettu (C-25/17).

Horizon scanning and data protection contagion

The last few months have seen a steady trickle of papers published by governmental and regulatory authorities that engage data protection, most notable are the House of Lords Communications Select Committee report on **regulating in a digital world** and the Digital Competition Expert Panel's **report on unlocking digital competition**[8]. Both these papers engage with GDPR concepts, such as data portability, data subjects' right of access and transparency. Both papers also put forward suggestions for additional responsibilities for the ICO, including to pursue competition in digital markets. The Government's **response** to the House of Lords report does demonstrate caution about increasing the ICO's remit and instead suggests responsibility falls to the Centre for Data Ethics where the ICO was put forward, such as in relation to developing best practice for algorithms.

These papers reflect the increasing focus on data protection across the regulatory spectrum: both in respect of the need to safeguard personal information in the digital environment and because the tools developed within the GDPR, particularly data portability, appear ripe to be adapted and repurposed to facilitate the requirements of other regulators. We will be monitoring developments in these areas, conscious that data protection practitioners' remit and the ICO's focus and powers may expand in the future.

Views from… Brazil

Brazil's new GDPR-inspired law

Contributed by Thiago Luís Sombra, Partner, Alan Elias Thomaz, Associate, and Giovanna Ventre, Associate, Mattos Filho

Historically, Brazil has adopted a sectorial regulation on privacy and data protection matters. Those sectorial laws may apply in specific circumstances, such as the Internet Act (Law 12,965/2014), which is applicable only to personal data collected through the internet, or the Consumer Protection Code (Law 8,078/1990), which is applicable whenever a consumer relationship is established between an individual and a service provider or a product manufacturer.

In August 2018, a general data protection regulation (the 'LGPD') was approved in Brazil, in large part inspired by the GDPR. The LGPD establishes detailed rules for the collection, use, processing and storage of personal data. It will affect all economic sectors, including relationships between customers and suppliers of goods and services and between employees and employers and other relationships in relation to which personal data is collected, both in the digital and physical environment.

According to the LGPD, the processing of personal data may only occur if based on one of the legal grounds contemplated in the LGPD. Such grounds include the processing of personal data with the consent of the data subject, for compliance with legal or regulatory obligations, when necessary for the performance of a contract and when necessary to meet the legitimate interest of the controller of the data or third parties. The legal grounds for processing personal data must be documented by organisations.

[8] See also: Government's consultation paper on **Smart Data: putting consumers in control of their data and enabling innovation** (June 2019).

In addition, the LGPD introduces new rights for data subjects, including the right to access, to rectify and delete data, the right to revoke consent at any time, the right of data portability to another supplier of goods and services and the right to obtain the review of automated decisions. The LGPD also requires organisations to adopt technical and organisational measures to protect personal data, and to notify incidents or unauthorised access to the National Data Protection Authority ("ANPD") and affected individuals within a reasonable time.

The LGPD provides for the creation of the ANPD, which is the first data protection authority in Brazil and which will be responsible for overseeing the enforcement of data protection laws. The LGPD establishes that the ANPD will have prevailing jurisdiction to enforce data protection laws over other public bodies. On May 28 and 29, 2019, the Brazilian Congress passed Conversion Law No. 7/2019, which created the ANPD and also introduced some amendments to the original version of the LGPD. Further details on those changes can be found on the **Mattos Filho website**.

Although the LGPD was enacted in August 2018, it will only become effective in August 2020. Once the law is effective, the companies that are not compliant with its obligations may be subject to warnings, total or partial suspension of the database for up to six months or the illegal processing operation, permanent prohibition from carrying out data processing activities (after applying a less burdensome sanction) and/or fines of up to 2% of the legal entity or its group's total revenue in the last fiscal year (limited in total to R$ 50,000,000 per infraction).

Data Protection and Privacy at Slaughter and May

We advise on all aspects of data protection and privacy compliance across the world. This ranges from ad hoc GDPR compliance issues to complex global data risk strategic advice. We regularly advise on cyber and data breaches; data protection issues arising in M&A transactions; global investigations and pension scheme arrangements; the privacy implications for tech such as blockchain or AI; individuals' rights; and data sharing agreements, from simple processor agreements to more complex data pooling arrangements and large strategic sourcings.

In our experience, data protection and privacy issues areas affect all areas of a business. All our fee-earners advise on data protection and privacy issues in their practice area. For more complex or novel queries, our global specialist data privacy team provides the necessary expertise and support. The team is co headed by **Rebecca Cousin** and **Rob Sumroy**.

If you would like further information please contact one of the team below, or your usual Slaughter and May contact.

Our other publications

All our publications on the GDPR and data protection and privacy more generally are available on our **website**.

Rob Sumroy
Partner
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

Rebecca Cousin
Partner
T +44 (0)20 7090 3049
E rebecca.cousin@slaughterandmay.com

Richard Jeens
Partner
T +44 (0)20 7090 5281
E richard.jeens@slaughterandmay.com

Richard de Carle
Partner
T +44 (0)20 7090 3047
E richard.decarle@slaughterandmay.com

Duncan Blaikie
Partner
T +44 (0)20 7090 4275
E duncan.blaikie@slaughterandmay.com

Jordan Ellison (Brussels)
Partner
T +32 (0)2 737 9414
E jordan.ellison@slaughterandmay.com

Peter Lake (Hong Kong)
Partner
T +852 2901 7235
E peter.lake@slaughterandmay.com

Kevin Warburton (Hong Kong)
Counsel
T +852 2901 7331
E kevin.warburton@slaughterandmay.com