

DATA PRIVACY NEWSLETTER

SELECTED LEGAL AND REGULATORY DEVELOPMENTS IN DATA PRIVACY

QUICK LINKS

CASE LAW UPDATE

REGULATOR GUIDANCE

ENFORCEMENT OVERVIEW

VIEWS FROM... EGYPT

THE LENS

DATA PRIVACY AT SLAUGHTER AND MAY

For further information on any Data Privacy-related matter, please contact the [Data Privacy team](#) or your usual Slaughter and May contact.

One Bunhill Row
London EC1Y 8YY
United Kingdom
T: +44 (0)20 7600 1200

On behalf of the whole team at Slaughter and May, I hope you are still keeping safe and well during these challenging times.

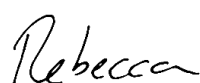
As many of you will know, we ran our annual Data Privacy Forum 2020 virtually in October. The event was aimed at senior individuals with responsibility for data privacy and was very well-attended, generating some interesting discussion on topics such as Brexit planning, the rise of funded mass litigation and international transfers. If you would like to see a copy of the Forum Report, please do get in touch.

Of course, since our Forum, there have been some further key developments in the world of data privacy. The European Data Protection Board (EDPB) has finally published detailed draft guidance on international transfers following the CJEU Schrems II decision. Not to be outdone, the EU Commission has published its long-awaited draft Standard Contractual Clauses for international transfers of personal data and, the cherry on top, draft standard processor clauses! Although there is no doubt that some of these will be complicated and time-consuming to implement in practice, it is becoming increasingly difficult for organisations to justify ignoring them.

On the enforcement side, amidst a backdrop of increasing collective actions in respect of data breaches, the ICO has published its final fines for British Airways, Marriott and Ticketmaster. These will provide some important learnings in relation to data security requirements and incident management.

And last but not least, the end of the Brexit transition period is almost upon us. Will the UK obtain an adequacy decision in time? It's not looking likely at the time of writing but then again, 2020 continues to be full of surprises... If you would like to hear more about the other aspects of Brexit planning that may be required in relation to data privacy, do listen to our podcast, available [here](#). And of course, please do not hesitate to get in touch with any of the team here if you have any data privacy queries, or even just for a quick virtual coffee and hello - all the more important given we haven't been able to meet you in person for a while now!

I wish you all an enjoyable run up to the festive season, despite the ongoing restrictions, and hope to catch up with you soon.



Rebecca Cousin
Partner

CASE LAW UPDATE

Schrems II

The news of the summer was of course the CJEU Schrems II decision. We discussed the decision in our [blog post](#). Subsequent developments are referred to below, including the recent guidance published by the EDPB.

The rise of funded mass litigation

In addition to regulator fines, organisations now face the growing risk of collective claims in connection with their data breaches. High-profile data breach claims have been issued in the last year against the likes of British Airways, Marriott, EasyJet, YouTube, TalkTalk, Facebook, Salesforce and Oracle and Equifax (the Equifax claim has now been withdrawn). A number of other potential claims are also reportedly pending, awaiting the outcome of the Lloyd v Google case (see our previous Newsletter Issues [10](#) and [13](#)), which will reportedly be heard by the Supreme Court in 2021.

Our [article](#) looks at the latest developments in this area, including the consultation by the Department for Digital, Culture, Media and Sport (DCMS) on whether to allow certain non-profit bodies to bring a type of ‘opt-out’ action on behalf of individuals under the Data Protection Act 2018, and the practical steps organisations can take to address this developing risk.

REGULATOR GUIDANCE

Key pieces of guidance published by the Information Commissioner’s Office (ICO), the DCMS and the EDPB since June 2020 are included in the table below. Some of these are explained in more detail in the following sections.

KEY REGULATOR GUIDANCE	
ICO	
Data protection and coronavirus information hub	Maintained
Age appropriate design code	July 2020
Guidance on AI and data protection	July 2020
Accountability framework	September 2020
Data subject access request guidance	October 2020
Draft statutory guidance on regulatory action (consultation closed on 12 November 2020)	October 2020
DCMS	
Data protection and data flows—further Brexit transition guidance	October 2020
EU COMMISSION	
Standard contractual clauses for transferring personal data to non-EU countries (SCCs) (consultation closing on 10 December 2020)	November 2020
Standard contractual clauses between controllers & processors located in the EU (consultation closing on 10 December 2020)	November 2020

KEY REGULATOR GUIDANCE	
EDPB	
Guidelines on consent under Regulation 2016/679	May 2020
Guidelines on the concepts of controller and processor in the GDPR (consultation closed on 19 October 2020)	April 2020
Guidelines on the targeting of social media users	September 2020
Draft Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (consultation closing on 21 December 2020)	November 2020
Recommendations 02/2020 on the European Essential Guarantees for surveillance measures	November 2020

EDPB guidance following Schrems II and EU Commission draft SCCs and processor clauses

Our [client briefing](#) contains further details on the EU Commission’s draft SCCs and the EDPB guidance on supplementary measures and how to assess surveillance laws.

The second set of clauses recently published by the EU Commission relate to the appointment of a processor by a controller (within the EEA) and contain the clauses required by Articles 28(3) and (4) of the GDPR. They are optional clauses in the sense that there is nothing preventing a controller and processor negotiating an individual, bespoke agreement between themselves rather than using the EU Commission’s clauses. The EU Commission has also helpfully clarified that its clauses could be used in a wider contract, and that the parties can add other clauses or additional safeguards to them. However, these must not contradict, directly or indirectly, the EU Commission’s clauses or prejudice the fundamental rights or freedoms of individuals.

EDPB draft guidelines on the concepts of controller and processor

One of the key takeaways from these guidelines is the likely increase in the prevalence of joint controllership. Given the EDPB draft guidelines follow CJEU case law in this area (e.g. Fashion ID), it will come as no surprise that applying them may well result in more instances of joint controllers, where previously organisations had considered their relationships with third parties (including other intra-group entities) to be either that of two independent controllers or controller to processor.

In practice, for controllers that already include detailed clauses in their arrangements with other controllers, re-classification as joint controllers, if necessary, may not have much of an impact. However, they will need to check that they meet the transparency requirements of Article 26 of the GDPR by making the ‘essence of the arrangement’ clear to individuals. For others that had perhaps relied on shorter agreements, going forward they may wish to revisit the level of detail in any new joint controller agreements, including in particular paying closer attention to the allocation of responsibilities and liability clauses. The draft guidelines contains recommendations on what each type of contract (controller to processor and joint controller) should include.

ICO guidance on AI

The ICO has been fairly active in relation to AI, in line with its statement that AI is one of its top three strategies priorities. Further details on its July guidance on AI are on our [blog](#) and our [website](#). The ICO has also published guidance on explaining AI - see this [blog post](#) for further details.

ICO final guidance on Data Subject Access Requests (DSARs)

On 21 October, the ICO published [new DSAR guidance](#) following a consultation which ended earlier this year. Although the ICO has retained much of what was in its [draft guidance](#), there are a few areas that have been amended, including:

- The efforts required to search and find the personal data requested need only be “reasonable” rather than “extensive”.
- There is further detail on when the recipient of a DSAR can refuse to comply with it if it is manifestly “unfounded” (in relation to motives of the employee) or “excessive” (in relation to the burden placed on the employer).
- Where the recipient of DSAR processes a large amount of information about an individual, it may ask the individual to specify the information or processing activities that their request relates to before responding. Helpfully, the ICO has now confirmed that the time limit for responding to the request will be paused whilst awaiting such clarification (i.e. ‘the clock is stopped’).

ICO draft statutory guidance on regulatory action

On 1 October, the ICO opened a consultation on new draft statutory guidance around how it will enforce data privacy legislation in the UK. The finalised guidance will sit alongside the ICO’s Regulatory Action Policy. The draft guidance includes a new “nine-step mechanism” for calculating proposed monetary penalties, including further detail on the ICO’s starting point (which, it suggests, should be turnover-based and therefore potentially leading to higher fines in the future). For further details, please see our [blog post](#).

ICO guidance on accountability

In early autumn, the ICO published comprehensive draft guidance on accountability in the form of a practical framework to help organisations manage their approach to privacy and to understand what good accountability looks like. Given that pre-COVID-19 the ICO had made clear the importance of accountability for organisations’ compliance, we would expect the ICO to re-focus on this area in 2021 following publication of the final version.

ENFORCEMENT OVERVIEW

ICO fines British Airways £20 million

On 16 October, the ICO issued its final enforcement notice against British Airways in respect of the major data breach that occurred in 2018. The £20 million fine is significantly lower than the ICO had originally indicated (£183 million) for a variety of reasons, including the impact of COVID-19. However, the level of this fine should not be taken as indicative of what the level of fine would be for an incident of this nature in the future, given the current consultation on regulatory action referred to above. The [penalty notice](#) provides a good checklist for clients of security measures and non-ICO guidance on security requirements. Organisations should therefore consider asking their InfoSec teams to assess their own systems and measures against this decision. See our [blog post](#) for further details.

ICO fines Marriott £18.4 million

The ICO [has also fined](#) Marriott International Inc. (Marriott) £18.4 million in relation to a cyberattack. Turnover was relevant to the calculation of the fine but not the starting-point or main basis. The fine was also significantly decreased from the initial fine of £99 million proposed by the ICO in 2019 following Marriott’s representations, co-operation with the investigation, and mitigating steps; and in part also the impact of COVID-19 on Marriott.

The fine related to an issue on systems belonging to Starwood Hotels and Resorts Worldwide Inc. (Starwood), which was acquired by Marriott in September 2016. Neither Marriott or Starwood were aware of the attack at the time of acquisition or during initial IT integration, but this fine emphasises the importance of cyber and data privacy due diligence during an M&A process.

Both the British Airways and Marriott fines were sent to EU data protection authorities (DPAs) before being issued, in accordance with the one-stop-shop mechanism.

ICO fines Ticketmaster £1.25 million for failing to protect payment details

The ICO has issued a [monetary penalty notice](#) to Ticketmaster Ltd for failing to keep its customers' personal data secure. The ICO found that the company failed to put appropriate security measures in place to prevent a cyber-attack on a chat-bot installed on its online payment page. The data breach included names, payment card numbers, expiry dates and CVV numbers and potentially affected 9.4 million of Ticketmaster's customers across Europe including 1.5 million in the UK. The company has said it will appeal the decision.

EU DPAs: GDPR enforcement overview

The table below sets out a selection of noteworthy GDPR fines brought by EU DPAs since our previous Newsletter, along with an indication of the main areas of non-compliance addressed by each enforcement action.

DPA (Country)	Company	Amount	Date	Description
LfdI (Baden-Wuerttemberg DPA) (Germany)	Allgemeine Ortskrankenkasse ('AOK') (health insurance company)	€1.24 million	30 June 2020	<ul style="list-style-type: none"> Unlawful processing
AP (The Netherlands)	Bureau Krediet Registratie	€830,000	6 July 2020	<ul style="list-style-type: none"> Unlawful processing
Garante (Italy)	Wind Tre S.p.A.	€16.7 million	9 July 2020	<ul style="list-style-type: none"> Unlawful processing
APD (Belgium)	Google	€600,000	14 July 2020	<ul style="list-style-type: none"> Data subjects' rights Right of access
CNIL (France)	Spartoo	€250,000	5 August 2020	<ul style="list-style-type: none"> Data subjects' rights
HmbBFDI (Hamburg DPA)	H&M	€35.3 million	1 October 2020	<ul style="list-style-type: none"> Unlawful consent
Garante (Italy)	Vodafone	€12.25 million	12 November 2020	<ul style="list-style-type: none"> Unlawful processing

The Spanish DPA has continued to be very active, with over 60 fines issued between June and November. The trend identified in previous issues of this Newsletter continues - with most EU DPAs (other than the ICO) fining for a range of breaches under the GDPR, rather than data security breaches only. Interestingly, a number of DPA fines across the EU have been, or are in the process of, being appealed. For example, the Bonn Regional Court [has recently ruled](#) that the €9.5 million penalty against 1&1 was far too high, and reduced it down to €900,000.

Note that in June the EDPB launched a [public register](#) of all completed GDPR cross-border cases, which provides a useful oversight of the European cross-border enforcement landscape.

VIEWS FROM... EGYPT

Contributed by Ahmed El Sharkawy (partner) and Menna Abouzerky (attorney at law) from Sharkawy & Sarhan

On 13 July this year, Egypt issued its first comprehensive data privacy law: the Data Protection Law (Law No. 151 of 2020) (the Law). The Law seeks to lay down the rules for personal data processing. Further details will be provided in the “Executive Regulations” which are due to be published by April 2021. Although the Law officially came into force on 14 October 2020, there is a one year grace period from when the Executive Regulations are issued which means that enforcement is unlikely before early 2022. The Law is said to be inspired by the GDPR although it diverges from it in a number of areas, including:

- All controllers and processors need a licence to process personal data which comes at a fee of up to 2,000,000 Egyptian pounds (approximately £10,000).
- Licences are also required for the processing of special categories of data and international transfers.
- Any organisation that processes personal data as a controller or processor in Egypt will require a data protection officer.

Other interesting points include:

- The Law has extra-territorial reach, in that it permits the authorities to penalise non-Egyptian persons that process personal data of Egyptian nationals and/or residents in a non-compliant way under the Law. However, action can only be taken to the extent that the action is penalised under the relevant local law (i.e. only if the processing would also be non-compliant under local law).
- The Law only applies to personal data that is partially or completely held in electronic form; hard copies therefore appear to be largely excluded from its scope.
- The definition of “processor” is broader than the definition under the GDPR and includes entities that process personal data on both a controller’s and their own behalf. Unlike the GDPR, processors are subject to a level of obligations under the Law very similar to the level that controllers are under.
- In addition to the concepts of “controllers” and “processors”, there is a third concept of “holders”. In short, these are persons that “legally or factually” hold and retain personal data in any manner, regardless of whether they initially collected or received that data. Holders are subject only to a limited range of obligations under the Law.
- Non-compliance with the Law can lead to serious consequences, including fines up to 5,000,000 Egyptian pounds (approximately £245,000) and up to 3 years imprisonment.

Next steps: Egyptian businesses and foreign businesses that are caught by the Law’s extra-territorial scope should start preparing for when the Law becomes fully enforceable. Further clarifications on the Law will be published in the Executive Regulations.

THE LENS - DIGITAL DEVELOPMENTS IN FOCUS

Our blog, [The Lens](#), showcases our latest thinking on all things digital. It brings together, in one place, content from all of our different practice streams that advise on tech and other digital topics, including Competition, Cyber, Data Privacy, Financing, Financial Regulation, IP/Tech and Tax. To subscribe to the blog please select the subscribe option on the [blog’s homepage](#). Some of our recent posts (other than those already mentioned in this Newsletter) include:

- [ICO audit of political campaigning: a case for transparency that goes beyond Westminster](#)
- [US responds to Schrems II judgment](#)
- [Parliament approves ICO code of practice which aims to make children safer online](#)

Our blog [Beyond Brexit - ‘a new chapter’](#) covers the implications of Brexit on a range of topics, including data privacy. All of our publications on the GDPR, and data privacy more generally, are available on our [website](#).

DATA PRIVACY AT SLAUGHTER AND MAY

We advise on all aspects of data privacy compliance across the world. This ranges from ad hoc GDPR compliance issues from EU and non-EU clients to complex global data risk strategic advice. We regularly advise on data breaches; data protection issues arising in commercial and 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.

Our global data privacy team comprises six expert partners, supported by several associates and professional support lawyers who specialise in this area. As data privacy issues affect all areas of a business, we train all of our other lawyers to advise on these issues within their practice areas. For more complex or novel queries, our specialist cross-practice data privacy team can provide the necessary expertise and support.

CONTACT



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



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



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



Wynne Mok
Partner
T +852 2901 7201
E wynne.mok@slaughterandmay.com



Cindy Knott
Professional Support Lawyer
T +44 (0)20 7090 5168
E cindy.knott@slaughterandmay.com



Bryony Bacon
Professional Support Lawyer
T +44 (0)20 7090 3512
E bryony.bacon@slaughterandmay.com

London
T +44 (0)20 7600 1200
F +44 (0)20 7090 5000

Brussels
T +32 (0)2 737 94 00
F +32 (0)2 737 94 01

Hong Kong
T +852 2521 0551
F +852 2845 2125

Beijing
T +86 10 5965 0600
F +86 10 5965 0650