

DATA PRIVACY NEWSLETTER

SELECTED LEGAL AND REGULATORY DEVELOPMENTS IN DATA PRIVACY

QUICK LINKS

[LEGAL UPDATES](#)[CASE LAW UPDATE](#)[REGULATOR GUIDANCE](#)[ICO ENFORCEMENT OVERVIEW](#)[EU GDPR ENFORCEMENT OVERVIEW](#)[VIEWS FROM ... SOUTH AFRICA](#)[THE LENS AND OUR PODCASTS](#)[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

It was so very close... But, unlike the football, we got the result we wanted..

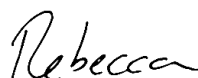
On 28 June, the EU adopted its adequacy decisions for the UK under the EU GDPR and the Law Enforcement Directive, two days before the expiry of the temporary ‘adequacy bridge’ between the EU and UK (that we discussed in our [January briefing](#)). We were relieved to have this certainty for EU-UK data flows, even amongst the widespread recognition that the decisions may well be subject to challenge.

We were also very pleased with the developments on international transfers of data from out of the EU, with the final version of the EU’s new standard contractual clauses (SCCs) and the European Data Protection Board’s (EDPB) supplementary measures guidance also being published in the last couple of months (both discussed below). However, with a ground-swell of Schrems II compliance enforcement building in the EU, implementing the steps recommended in the new guidance will be both important and practically challenging for those operating across Europe in the coming months.

The future of the UK’s international transfer regime, however, remains less clear. As organisations await the UK’s own new SCCs, [a report](#) published by the Government’s Taskforce on Innovation, Growth and Regulatory Reform has suggested significant reforms to the UK GDPR. The report submits that the GDPR is “already out of date”, and “overwhelms people with consent requests and complexity they cannot understand, while unnecessarily restricting the use of data for worthwhile purposes”. Elizabeth Denham, the outgoing Information Commissioner, has rejected this ‘false dichotomy’ between growth and innovation on one side and data privacy on the other. She has emphasised that privacy regulation is only going one direction - towards higher standards. Either way, it seems likely that the UK data privacy landscape will not stay still for long!

In addition to regulatory developments, we are keeping a firm eye on the courts, particularly as [Lloyd v Google](#) was heard in the Supreme Court at the end of April. The much awaited judgement is expected to play an important role in shaping the future of mass claims in the UK and seems even more pertinent following BA’s recent settlement of its data breach group action, as we discuss below.

We will continue to keep you updated as these events play out over the next few months and in the meantime, we hope you have a wonderful summer.



Rebecca Cousin
Partner

LEGAL UPDATES

International transfers update

The last few months have seen significant developments in relation to the EU GDPR's international transfers' regime, giving organisations some long awaited clarity and increased certainty.

EU adopts adequacy decisions for the UK

By granting the UK's adequacy decisions, the EU confirmed that the UK regime provides an 'essentially equivalent' level of protection for personal data to that provided by the EU GDPR. The adequacy decisions recognise the current alignment between the UK and EU, in particular because the EU GDPR was largely 'copied' in to UK legislation following Brexit (to become the UK GDPR) but also as a result of the UK's international commitments, such as the European Convention on Human Rights and Convention 108. However, the possibility that the UK's data protection regime may evolve and diverge from that of the EU has been acknowledged as a concern by both the EDPB in its [opinions](#) on the draft adequacy decisions and ultimately in the final adequacy decisions from the EU. As a result, both adequacy decisions require the European Commission to continually monitor the UK regime and include a four year 'sunset clause' after which time they expire, unless they are renewed. Following the Court of Appeal's decision in the [Open Rights Group](#) case in May, the adequacy decision under the GDPR also includes a carve-out for data sent from the EU to the UK in connection with the immigration exemption in the Data Protection Act 2018.

New EU SCCs finalised

The EU Commission has issued the final version of its standard contractual clauses (SCCs) for international data transfers which came into force on 27 June 2021. The new SCCs are in a modular format and supersede all the previous versions of the EU SCCs with which many organisations are familiar. We discuss the key changes and deadlines that accompany the new EU SCCs in our briefing: [Get set, update! European Commission publishes finalised SCCs for data transfers](#).

EDPB publishes final guidance on supplementary measures

The EDPB has published its final [Recommendations on Supplementary Measures](#) (01/2020) following a significant response to its public consultation on the draft version. The final version of the guidance is broadly similar to a draft issued last year but includes some changes including:

- a greater role for the subjective experience of the data importer, e.g. in relation to the absence of prior instances of public authority requests for data access, as a relevant but not sufficient consideration in the analysis of the effectiveness of the Article 46 transfer tool;
- emphasis on the data exporter taking into account practices in force in the third country which undermine the protection for personal data formally provided in the legislation; and
- in circumstances in which the data transfer falls, or might fall, within the scope of problematic legislation in the third country, a new 'third option' for exporters (along with suspending the transfer or implementing supplementary measures) to proceed with the transfer without implementing supplementary measures if they have no reason to believe the problematic legislation will actually be applied in practice to the data being transferred and/or the importer in question and are able to demonstrate/document that.

EDPB publishes guidelines on Codes of Conduct as a tool for transfers

The EDPB have just published [draft guidance](#) for consultation on how they consider Codes of Conduct (CoC) could work as a GDPR international transfers mechanism, under GDPR Article 40(3) and 46(2)(e). The EDPB envisages that an organisation in a non-adequate third country could adhere to a CoC to enable a controller / processor within the EU to make an international transfer to that organisation in compliance with the GDPR without using SCCs or binding corporate rules (BCRs) and without the EU entity themselves necessarily being party to the CoC. CoCs would be developed by trade associations, or equivalent bodies, to reflect the needs and challenges of specific sectors (e.g. financing or insurance) and as such will be more 'bespoke' than other GDPR transfer mechanisms. The EDPB detail a lengthy list of requirements that CoC must satisfy (in part to ensure compliance with Schrems II), which has at least a superficial similarity to the GDPR's

lengthy requirements for BCRs. However, organisations exporting data will still need to carry out transfer impact assessments, even where the recipient has adhered to a CoC.

From a practical perspective, it will be a while yet before organisations are able to make use of CoCs: the consultation period doesn't end until October and following that, a CoC will need to be prepared, approved by the competent supervisory authority, be subject to an opinion from the EDPB and then finally be approved by the Commission (although the exact process may depend on the nature of the CoC).

In the UK we have heard a number of references from the DCMS/ICO in the last few months to the under-used elements of the 'GDPR toolbox' for international transfers as a possible answer to some of the challenges faced by organisations following the Schrems II judgement. It will be interesting to see the extent to which the ICO chooses to follow the EDPB in relation to CoCs for international transfers.

UK international transfers update

Meanwhile, the ICO has announced that it [is currently working](#) on bespoke UK SCCs. John Whittingdale, Minister of State for Media and Data, gave more detail on the ICO's plans during his session with Rebecca Cousin at the Privacy Laws & Business (PL&B) annual conference at the start of July. He informed the audience that the new UK SCCs will be known as the UK's 'International Data Transfer Agreement' (ITDA) and that the ICO intend to put a draft IDTA out for consultation later this month along with accompanying guidance.

The Minister also suggested during the conference that a significant announcement about the UK adequacy assessments could be expected later in July. It would potentially identify the front-running countries to be considered as candidates for adequacy by the UK.

Australia is likely to be on this list, given that the recent agreement in principle on a UK-Australia Free Trade Agreement includes a 'commitment to enable cross-border data flows'. The UK government's approach to data protection in the context of trade deals has been considered by the House of Commons Trade Committee in its recent report on [Digital Trade and Data](#), with the report highlighting that the UK Government needs to properly consider and explain the impact of any new trade agreements on UK data protection and particularly its adequacy decision from the EU. This is discussed further in our recent blog post, [Strategy and Accountability in Digital Trade Deals](#).

CASE LAW UPDATE

BA reaches data breach class action settlement

British Airways (BA) has reached a confidential settlement with a number of claimants involved in an opt-in group action relating to the company's 2018 data breach. However, reports suggest that a minority of claimants, represented by a separate law firm to those that have accepted the settlement offer, continue to pursue their action against BA. We discuss this further in our Lens blog post: [British Airways negotiates the settlement of mass data claim](#).

Ticketmaster penalty appeal paused until civil claims decided

In April, the [First-tier Tribunal \(FTT\)](#) granted Ticketmaster's application to stay proceedings in the company's appeal against the [ICO's £1.25m fine](#) for their 2018 supply-chain cyber incident, until the conclusion of the civil litigation relating to the same cyber incident in the High Court. Although the FTT's decision was limited on its facts, it is an interesting insight into how proceedings relating to regulatory penalties can interact with data breach litigation claims. The High Court is not expected to hear the civil claim against Ticketmaster until late 2022 or early 2023 meaning the outcome of the appeal against the ICO's penalty is likely to take place 5 years after the original incident.

Clarification of GDPR representatives' liability

In [Rondon v LexisNexis Risk Solutions](#), the High Court ruled that an EU representative appointed under GDPR Article 27 is not directly liable for the GDPR breaches of the entity it represents. The claimant had sought to bring an action against LexisNexis Risk Solutions UK Limited as the representative of the US based company World Compliance Inc (the controller).

In reaching its determination, through a detailed analysis of the GDPR and relevant guidance, the court provided useful clarification of the role of GDPR representatives. For example, at paragraph 74 it states: “*Even the language of ‘conduit’ or ‘liaison’ does not fully capture the job the GDPR gives to representatives. The role is an enriched one, active rather than passive. At its core is a bespoke suite of directly-imposed functions. [...] The job focuses on providing local transparency and availability to data subjects, and local regulatory co-operation*”.

REGULATOR GUIDANCE

Key pieces of guidance published by the ICO, the EDPB and European Data Protection Supervisor (EDPS) since March 2021 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 the EU in detail	July 2021
The role of data ethics in complying with the GDPR (a summary of consultation)	June 2021
Opinion on the use of live facial recognition technology in public places	June 2021
Anonymisation, pseudonymisation and privacy enhancing technologies guidance (draft - consultation closes on 28 November 2021)	May 2021
ICO call for views: AI and data protection risk mitigation and management toolkit (draft - consultation closed 19 April 2021)	April 2021
EDPB and EDPS	
Guidelines on Codes of Conduct (CoCs) as a tool for transfers (consultation closes on 1 October 2021) (discussed above)	July 2021
Guidelines on Virtual Voice Assistants (VVA) (final version)	July 2021
Guidelines 07/2020 on the concepts of Controller and Processor in the GDPR (final version) (discussed below)	July 2021
Recommendations U1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (final version) (discussed above)	June 2021
Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom	April 2021
Guidelines 8/2020 on the targeting of social media users (final version)	April 2021
Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications (final version)	March 2021

Updates from the ICO

ICO publishes new guidance on Data Protection and the EU

Following the adoption of the UK’s adequacy decision from the EU, the ICO has updated its guidance to include a new section on ‘[Data protection and the EU](#)’. Although most of the content has been moved across from its previous guidance on ‘Data Protection at the end of the Transition Period’, the ICO has included some additional content reflecting details of the EU’s adequacy decisions. Interestingly, and perhaps significantly, the guidance alerts businesses to the limited duration, potential suspension and possibilities for challenge to the adequacy decisions and sets out how the ‘Frozen GDPR’ would once again be a relevant consideration in a situation in which the adequacy decisions ceased to apply. This perhaps could be read as a cautionary signal from the UK authorities as to the probability of challenge to UK adequacy.

Horizon scanning

Other noteworthy developments from the ICO on the horizon include:

- The coming into force of the ICO's [Age Appropriate Design Code](#) on 2 September.
- The coming into force of the ICO's Data Sharing Code of Practice, which was laid before Parliament on 18 May for 40 sitting days before coming into force. We discussed the significant features of the Data Sharing Code in draft form in [this briefing](#).
- Further chapters of the ICO's guidance on anonymisation and pseudonymisation. The ICO set out its roadmap for publishing guidance on this topic in its blog post in March '[Building on the data sharing code - our plans for updating our anonymisation guidance](#)'. The first part of its draft guidance was put out for consultation on 28 May (closing on 28 November). It provides an introduction and defines key concepts such as 'anonymous information' and 'pseudonymisation'. From this initial chapter it appears that the ICO will maintain its previous pragmatic position in relation to anonymisation (recognising for instance, that information can be personal data in the hands of one organisation but anonymous in the hands of another).
- Final (or interim) findings from the ICO's ongoing investigation into the adtech industry (which [resumed in January 2021](#)).

Updates from the EDPB

EDPB publishes final version of controller, processor and joint controller guidance

Following consultation, the EDPB has published the [final version](#) of its guidance on controllers, processors and joint controllers that was first published in draft in September last year. The updated version includes a number of additional examples and clarifications including further emphasis that the controller/processor allocation is a matter of fact and is non-negotiable and additional guidance on the relationship between controllers and processors, including in relation to data breach notifications and audit costs.

ICO ENFORCEMENT OVERVIEW

ICO enforcement

The ICO has been relatively quiet on the UK GDPR enforcement front since March, although it has issued a relatively consistent string of PECR fines against companies carrying out nuisance marketing (for example, in June it [announced fines totalling £415,000 against three separate companies](#)). In May this trend extended to more household names, when the ICO issued a [monetary penalty notice](#) to American Express Services Europe Limited (Amex) for sending 4,098,841 unsolicited marketing emails between 1 June 2018 and 21 May 2019 to customers who had not consented to receive them. The ICO's penalty notice against Amex centres around the distinction between 'servicing' and 'marketing' emails, a distinction that the ICO found Amex got wrong on occasion. The ICO also recently fined pizza company [Papa John's \(GB\) Limited](#) £10,000 for sending 168,022 nuisance marketing messages to its customers without valid consent.

As we discuss in our recent [blog post](#), the ICO has issued its fifth GDPR data breach fine against [Mermaids](#), a charity that supports transgender young people, for security failings that allowed sensitive and special category personal data to be accessible through internet search engines. While the ICO's action in this instance was driven by the sensitivity of the subject matter, the penalty notice emphasises the importance of regular staff training and privacy policy reviews: the regulator specifically highlighted that a number of the charity's policies had not been updated for the GDPR.

EU GDPR ENFORCEMENT OVERVIEW

The table below sets out a selection of the most substantial EU GDPR fines brought by European data protection supervisory authorities (DPAs) in the last 4 months, along with an indication of the principal areas of non-compliance addressed by each enforcement action.

DPA (Country)	Company	Amount	Date	Description
AEPD (Spain)	Vodafone	€8.15 million	12 March 2021	• Unlawful processing arrangements
AP (Netherlands)	Booking.com	€475,000	2 April 2021	• Breach notification
Datatilsynet (Norway)	Disqus Inc.	NOK 25 million (approx. €2.4 million)	5 May 2021	• Unlawful processing, transparency
AP (Netherlands)	Locatefamily.com	€525,000	18 May 2021	• Lack of EU representative
AEPD (Spain)	EDP	€1.5 million	18 May 2021	• Unlawful processing, transparency and data protection by design
IMY (Sweden)	MedHelp	SEK 12 million (approx. €1.1 million)	7 June 2021	• Data security, transparency
Garante (Italy)	Foodinho	€2.6 million	5 July 2021	• Unlawful processing, transparency

Post Schrems II developments

A number of German DPAs have this week [announced](#) a coordinated, nationwide, assessment of companies' compliance with the Schrems II ruling, which includes sending companies a standardised compliance questionnaire. This follows on from the Bavarian DPA's [application](#) of the Schrems II ruling in March that called for a German company to cease using US-based Mailchimp, a marketing automation and email marketing platform. The Bavarian DPA said that as Mailchimp could qualify as an 'electronic communication service provider' under US surveillance law, the company should have assessed and put in place additional measures (to supplement the EU SCCs) to ensure that the transferred data was protected from US surveillance.

In May, the EDPS [launched](#) two investigations as part of the [EDPS' strategy](#) for EU institutions to comply with the "Schrems II" Judgement; one regarding the use of cloud services provided by Amazon Web Services and Microsoft under Cloud II contracts by European Union institutions, bodies and agencies, and one regarding the use of Microsoft Office 365 by the European Commission.

VIEWS FROM ... SOUTH AFRICA

Contributed by Livia Dyer, Partner, Bowmans

Protection of Personal Information Act 2013 enters into force

The substantive provisions of the long-awaited South African Protection of Personal Information Act 2013 (POPIA) finally became enforceable on 1 July 2021. POPIA was originally signed into law in 2013 and was based on the EU's Data Protection Directive 95/46/EC. The Act is the country's first comprehensive data privacy legislation and will apply to all organisations processing information in South Africa, other than for personal and household purposes.

Certain provisions of POPIA have been in force since 2014, including those establishing the country's Information Regulator. POPIA came into effect on 1 July 2020 and organisations had 12 months to comply. This grace period ended on 1 July 2021. Most organisations have initiated data privacy compliance programmes to comply with POPIA. In many instances, organisations that are subject to the GDPR have extended their GDPR compliance programmes given the overlap between EU law and POPIA.

Now that POPIA is enforceable, organisations face fines of up to 10 million ZAR (approx. £507,000) for contraventions, as well as civil actions and potential criminal liability. It is hoped that the law may pave the way for an adequacy finding from the EU.

POPIA includes many familiar GDPR features including data security obligations, a mandatory breach reporting regime, individual data access rights and restrictions on both international data transfers and unsolicited e-marketing. However, unlike the GDPR the Act also gives protection to 'juristic persons' such as companies and trusts in addition to natural persons, although exactly how this will apply in practice remains to be seen.

THE LENS AND OUR PODCASTS

Our blog, [The Lens](#), showcases our latest thinking on all things digital. It brings together, in one place, content from all 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 include:

- [UK to capitalise on post Brexit independence in new data strategy](#)
- [The return of the determined intruder: the ICO's latest thinking on anonymisation and personal data](#)
- [Europe's groundbreaking AI Act: are "superfines" the price to pay for trust in tech?](#)
- [We can work it out - competition and data regulators agree blueprint for cooperation in digital markets](#)
- [Ransomware: does your board know the right questions to ask?](#)
- [Plenty more phish in the sea? Cyber risks for SMEs in the supply chain](#)
- [Ban facial recognition in public: EDPB calls for new AI law to be tougher](#)
- [Head in the clouds? Codes of conduct may be the way forward](#)
- [DCMS sets out "new, ground-breaking approach" to governing tech in UK](#)
- [Strategy and Accountability in Digital Trade Deals](#)

Our blog [Beyond Borders](#) covers the implication of Brexit on a range of topics, including data privacy. All of our publications on the UK 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 UK, 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 (Brussels)
Partner
T +32 (0)2 737 9414
E jordan.ellison@slaughterandmay.com



Wynne Mok (Hong Kong)
Partner
T +852 2901 7201
E wynne.mok@slaughterandmay.com



Cindy Knott
Senior PSL and Head of Knowledge -
Data Privacy
T +44 (0)20 7090 5168
E cindy.knott@slaughterandmay.com



Bryony Bacon
Data Privacy PSL
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

Published to provide general information and not as legal advice. © Slaughter and May, 2021.
For further information, please speak to your usual Slaughter and May contact.

www.slaughterandmay.com

570912266