

DATA PRIVACY NEWSLETTER

SELECTED LEGAL AND REGULATORY DEVELOPMENTS IN DATA PRIVACY

QUICK LINKS

[LEGAL UPDATES](#)

[CASE LAW UPDATE](#)

[REGULATOR
GUIDANCE](#)

[ENFORCEMENT
OVERVIEW](#)

[VIEWS FROM ...
GERMANY](#)

[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

We were all relieved last week when the European Commission announced that they had published draft adequacy decisions for transfers of personal data to the UK. The news is all the more welcome given the current complexities around international transfers (and the additional challenges for many of having to deal with both EU and UK data protection regimes). As Elizabeth Denham said last week, the adequacy announcement 'gets us a step closer to having a clear picture for organisations processing personal data from the EU'.

The focus will now be on whether the European adequacy process can be concluded ahead of the expiry of the temporary EU-UK data 'bridge' at the end of June and, unsurprisingly, how swiftly and in what form the inevitable challenges to the EU's UK adequacy assessment will arrive (as we discuss [here](#)). Our January [briefing](#) contains further details on the 'bridge' arrangements for EU-UK data flows. Of course, international transfers generally are likely to remain a key area of focus for everyone in the coming months, with standard contractual clauses expected from the EU (in final form) and the UK.

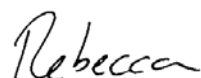
In terms of other developments in 2021, e-Privacy is back on the EU's agenda with progress made this month on the e-Privacy Regulation (ePR) in the European Council. Although the UK hasn't yet stated whether it will enact equivalent provisions, the ePR's extraterritorial reach means that UK businesses will need to keep monitoring privacy developments across the Channel as discussions heat-up between the EU institutions.

On the contentious side, the much-awaited Supreme Court decision is due in the first half of this year, and will provide some clarity on the future of representative actions in the UK.

Meanwhile, the Information Commissioner's Office (ICO) anticipates that their [workload](#) for 2021 will focus on supporting organisations with pandemic-related privacy compliance challenges and ensuring that individuals' rights continue to be upheld. The ICO has also [indicated](#) that it will pick up work paused due to pandemic such as its investigation into adtech which it has resumed. Elizabeth Denham will remain at the ICO's helm through much of this next period, as her term as Information Commissioner has been extended until 31 October.

While we cannot meet face to face, we will continue to keep you up to date with developments and support you with your privacy compliance.

We hope to catch up for a virtual coffee soon.



Rebecca Cousin
Partner

LEGAL UPDATES

EU Commission publishes draft UK adequacy decisions

As mentioned above, on 19 February the European Commission **published** two draft adequacy decisions for transfers of personal data to the UK, one under the GDPR and one under the Law Enforcement Directive. We discuss the next steps in the adequacy process and the challenges remaining in our recent **briefing**.

ePrivacy Regulation progresses as EU Council reach agreed stance

Following nearly four years of negotiations across eight EU Council Presidencies, the EU Member States have reached an agreement on a draft of the much delayed ePrivacy Regulation (ePR) that will now form the basis of their negotiations with the European Parliament (overseen by the European Commission). As discussed in past newsletter issues (see **issue 7**), the ePR is due to replace the EU's 2002 ePrivacy Directive and was previously envisaged as taking effect at the same time as the GDPR. Now the log-jam in the EU Council has been cleared, the ePR is able to progress to these final trilogue negotiations. It is anticipated that there may be substantial revisions to the current EU Council draft text in the course of the negotiations given the differing views of the European Parliament.

CASE LAW UPDATE

UK court extends deadline in BA data damages claim to gather more claimants

Following British Airways' high-profile 2018 data breach that led to a £20 million regulatory fine from the ICO (see our previous **blog post**), the airline is now facing the largest ever group claim for a data breach. In a Costs and Case Management Conference for the 'opt-in' class action earlier this month, Mr Justice Saini **agreed** to extend the deadline for claimants to opt in to the litigation from 3 April to 3 June 2021. The Judge also concluded that the claimant's lawyers cannot recover their advertising spend in building the group action, as we discuss in our recent **blog post**.

Meanwhile, **two competing class actions** have been filed against Facebook for the harvesting of data without users' consent, following the ICO's £500,000 **fine** against the social media company in 2018 (the maximum penalty under the pre-GDPR regime).

GDPR extraterritoriality considered by English court

In **Soriano v Forensic News and Others**, the High Court had to decide whether the processing of Mr Soriano's personal data by a US-based investigative journalism website, Forensic News, fell within the scope of the GDPR's extraterritoriality. This analysis came in the context of an application by Mr Soriano to serve proceedings on Forensic News in the US, under CPR Practice Direction 6B. Justice Jay's judgment held that Forensic News had no establishment in the UK and the website in question was not UK orientated and had no UK employees. The Judge held that 'less than a handful' of UK subscribers was not enough to amount to a 'stable arrangement' for an establishment under the GDPR and that the website was not seeking to target individuals in the UK or EU. Although the judgement dismissed the GDPR elements of the application, it is useful to see the court's practical application of the GDPR's extraterritorial provisions.

REGULATOR GUIDANCE

Key pieces of guidance published by the ICO and the European Data Protection Board (EDPB) since November 2020 are included in the table below. Some of these are explained in more detail in the following sections.

KEY REGULATOR GUIDANCE	
ICO	
Role of data ethics in complying with the GDPR (consultation closed 8 January 2021)	January 2021
Data protection and coronavirus - advice for organisations (updated)	January 2021
Standard Contractual Clauses (SCCs) after the transition period ends (updated)	January 2021
Information rights at the end of the transition period - FAQs (updated)	January 2021
Data Sharing Code of Practice (final version)	December 2020
EDPB	
Guidelines 01/2021 on Examples regarding Data Breach Notification (consultation closes 2 March 2021)	January 2021
EDPB - EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors	January 2021
EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries	January 2021
Guidelines 10/2020 on the permitted restrictions to certain provisions of the GDPR by Union or member state law under Article 23 GDPR (consultation closes 12 February 2021)	December 2020

ICO guidance on SCCs after the transition period ends

The ICO has published more [detailed guidance](#) on the application of Standard Contractual Clauses (SCCs) for international transfers now the UK-EU transition period has ended. It confirms that the existing EU SCCs can continue to be used for restricted transfers made from the UK ahead of the publication of the UK's own SCCs, which the ICO intends to consult on and publish during 2021. As a temporary measure, the ICO has [published](#) two UK versions of the EU SCCs (controller-to-controller and controller-to-processor) that it has amended to refer to the UK context. In the guidance, the ICO reminds organisations that the European Commission's draft EU SCCs will not be valid for transfers from the UK. The ICO also explains that the Schrems II decision continues to apply to restricted transfers from the UK. The ICO is intending to issue its own guidance on the 'essential equivalence' assessment organisations are required to make when using SCCs following Schrems II (which it acknowledges 'is undoubtedly complex') and the supplementary measures that may be required. We discussed international transfers following Schrems II in our briefing [International transfers of personal data - a way forward?](#)

EDPB & EDPS publish joint opinions on SCCs

The EDPB and the European Data Protection Supervisor (EDPS) have published [a joint Opinion 2/2021](#) on the EU Commission's draft decision on standard contractual clauses for international transfers of personal data (including [comments](#) on the draft clauses themselves). The opinion states that the draft SCCs present a reinforced level of protection for data subjects and the provisions intended to address the issues identified in the Schrems II judgement are particularly welcome. However, the EDPB and EPDS also put forward a number of suggested amendments, including in

relation to third party beneficiary rights, obligations for onward transfers and aspects of the assessment of third country laws.

The EDPB and the EDPS have also issued a [joint Opinion 1/2021](#) on the EU Commission's draft decision on standard clauses between controllers and processors (where a controller appoints a processor within the EEA), including [comments on the draft clauses](#).

EDPB guidance on data breach notification examples

The EDPB draft guidelines 01/2021 provide practical guidance on data breach notification based on case studies to complement the Article 29 Working Party's Guidelines on Personal Data Breach Notification under the GDPR published in 2017. We examine the new guidelines in our recent [blog post](#).

ICO publishes final Data Sharing Code

In December 2020, the ICO published the final version of its [Data Sharing Code of Practice](#) and supplemented it with a [set of resources](#) available via a new data sharing information hub on its website. The Data Sharing Code was submitted to the Secretary of State on 17 December to be laid before Parliament as soon as reasonably practicable. Once the Code has been before Parliament for 40 sitting days it will come into force (i.e. later this Spring).

ENFORCEMENT OVERVIEW

The table below sets out a selection of the most substantial GDPR fines brought by the 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
CNIL (France)	Google, Google Ireland and Amazon	€135 million	10 December 2020	<ul style="list-style-type: none"> • Unlawful consent • Data subjects rights
DPC (Ireland)	Twitter	€450,000	15 December 2020	<ul style="list-style-type: none"> • Breach notification
UODO (Poland)	ID Finance Poland	1 million zloty (€250,000)	30 December 2020	<ul style="list-style-type: none"> • Data security
LfdI (Lower Saxony)	Notebooksbilliger.de	€10.4 million	December 2020	<ul style="list-style-type: none"> • Unlawful processing (video surveillance) • See 'Views from...' below for further details
AEPD (Spain)	CaixaBank	€6 million	19 February 2021	<ul style="list-style-type: none"> • Unlawful consent • Data subjects rights
Datatilsynet (Norway)	Grindr	€6 million	26 January 2021	<ul style="list-style-type: none"> • Unlawful consent

CNIL fines Google, Google Ireland and Amazon

The French DPA, the CNIL, imposed the largest fines under the GDPR to date against Google and Amazon for cookie contraventions. The CNIL fined Google 100 million euros (split between Google Ireland and the US firm, Google LLC) and Amazon 35 million euros. The two companies were found to use non-essential, advertising cookies on their websites

without obtaining GDPR compliant consent from website visitors or providing sufficient information to individuals. See more in our [blog post](#).

Google has [subsequently challenged](#) the fine and the CNIL's authority to bring the action under the GDPR's one-stop-shop enforcement mechanism.

Increases in GDPR penalty values accompanied by increase in appeals

Across 2020 there was a significant increase in GDPR penalties brought by data protection authorities across the EU (a 40% uplift according to a [recent survey](#)). Notable big-hitting penalties include those brought against H&M by the Hamburg Commissioner ([€35.3 million](#)) in January, the TIM ([€27.8 million](#)) and Wind Tre ([€17 million](#)) fines brought by the Garante (the Italian DPA), as well as the headline grabbing penalties against British Airways (just over [€22 million](#)) and Marriott (over [€20 million](#)) by the ICO.

As has been much publicised in the UK in relation to the BA and Marriott penalties (originally c. £183 million and £99 million respectively, as we discuss in our [briefing](#)), regulators' fines have started to come up against more substantial challenge and/or been reduced. Fine reductions are also picked up in the German context by our 'Views from...' contributors, Hengeler Mueller, below. As the regulators continue to flex their muscles we can expect more fines to be tested on appeal. For example, the ICO's first-ever GDPR [fining decision](#) (against Doorstep Dispensaree) is now being appealed, suggesting that the regulator may also be on a post-GDPR learning-curve. The ICO has acknowledged it made errors in relation to its decision but told the First Tier Tribunal in December that the fine should still stand. We discussed the decision previously in issues [12](#) and [13](#) of our Newsletter.

Having said that, not all challenges will be successful, as evidenced in the appeal by [Leave.EU and Eldon Insurance Services](#) against the ICO's enforcement action. The appeal in the Upper Tribunal Administrative Appeals Chamber, relating to the ICO's enforcement actions stemming from the two companies' contravention of the e-marketing rules under the Privacy and Electronic Communications Regulations 2003 were dismissed on every ground.

Investigations and Enforcement Outlook 2021

In our [podcast](#) on Investigations and Enforcement Outlook 2021 - GDPR Enforcement and Litigation Trends, we discuss the increased (and varied) risks of regulatory enforcement and follow on civil litigation arising from breaches of data protection and privacy legislation.

VIEWS FROM ... GERMANY

Contributed by Vera Jungkind (Partner), Susanne Koch (Counsel), and Alla Droessler (Senior Associate) from Hengeler Mueller

In Germany, the GDPR is supplemented by the German Federal Data Protection Act (Bundesdatenschutzgesetz, (BDSG)), which is applicable to both private companies and the public sector, with additional provisions to protect employee data and national specification of individuals' rights. Further regulations for data processing can be found in certain sector specific data protection laws applying, for example, to schools or hospitals.

The responsibility for GDPR enforcement in Germany is divided between 17 data protection authorities (DPAs): While the 16 DPAs of the states (Länder) supervise the private sector in their respective state territory, the Federal Commissioner for Data Protection and Freedom of Information (BfDI) is mainly responsible for the public sector, including telecommunications. Internationally active companies therefore sometimes find it hard to get clear GDPR guidance from German DPAs.

Lately, German DPAs have initiated two much disputed enforcement cases:

State Commissioner for Data Protection of Lower Saxony (Niedersachsen) vs. notebooksbilliger.de

In January 2021, the relevant DPA imposed a fine of 10.4 million euros against notebooksbilliger.de AG, an IT hardware online retailer, which is approximately one percent of the company's annual turnover. notebooksbilliger.de has been accused of monitoring workplaces, sales rooms, warehouses and common areas by video surveillance measures over a period of two years. The authority stressed that the video surveillance was neither limited to a specific period of time, nor was it performed only on selected employees. In addition, the recordings were stored for 60 days which, in the view of the DPA, was significantly longer than required.

The company has filed an appeal against the decision arguing that the video surveillance was not intended to monitor the employees' behaviour or performance. Rather, the cameras were installed in order to uncover criminal acts or resolve disputes with suppliers and customers, in the event of missing or damaged goods. Furthermore, the company claims that the amount of the fine is excessive. The case is still pending.

BfDI vs. a German telecommunication service provider

In November 2019, the BfDI imposed a fine of 9.6 million euros against a German telecommunications service provider that had provided data of an individual customer to a caller without proper identification. As a result, the customer was stalked by the caller, which led to a criminal investigation. The BfDI ruled that identification of the caller by name and date of birth was insufficient and a grossly negligent violation of Article 32 GDPR. Before providing contact information to the caller, the provider should have applied more stringent security measures.

Upon appeal by the service provider, the District Court of Bonn recently reduced the fine to 900,000 euros. In a subsequent press release, the service provider highlighted that the court found its violation minor, non-intentional, and not deserving of a fine in the millions, especially because there never was a risk of a mass release of data.

Both cases show that German DPAs make use of their new enforcement powers under the GDPR. DPAs tend to measure the fines against the company's turnover rather than the impact of the individual case. However, fines are subject to scrutiny by the courts, and we expect to see more court decisions that correct the amount of the fine in light of the individual circumstances of the case.

THE LENS

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:

- [Mass claims for data breaches: perhaps a change of heart by the Government but don't forget Lloyd v Google](#)
- [Data privacy and M&A: the issues you really can't ignore](#)
- [Pay to play: Judge rules lawyers leading group action against British Airways cannot recover costs of advertising](#)

Our blog [Beyond Brexit - 'a new chapter'](#) covers the implication 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 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