

# DATA PRIVACY

## SELECTED LEGAL AND REGULATORY DEVELOPMENTS IN DATA PRIVACY

### QUICK LINKS

[LEGAL UPDATES](#)

[CASE LAW UPDATE](#)

[REGULATOR GUIDANCE](#)

[ICO ENFORCEMENT OVERVIEW](#)

[EU GDPR ENFORCEMENT OVERVIEW](#)

[VIEW FROM ... THE UNITED STATES OF AMERICA](#)

[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

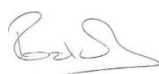
The last few months have seen rhetoric turn into reality in relation to the government's promised updates to the UK data protection regime. The Data Protection and Digital Information Bill received its first reading in Parliament on one of our hottest ever days this week but while the climate was uncomfortable, the more moderated proposals put forward in the DPDI Bill would have reassured many businesses, especially those concerned about the potential threat to the UK's EU adequacy decision. It remains to be seen whether the DPDI Bill will deliver the benefits promised to businesses but in any event, it was encouraging to hear the Department for Digital, Culture, Media & Sport (DCMS) confirm at the [2022 PL&B annual conference](#) in Cambridge that large organisations with developed GDPR accountability programmes should have to make few (if any) changes to remain compliant with the new regime. We will continue to closely monitor the DPDI Bill as it progresses through Parliament.

We have also seen recent progress on the persistently hot topic of international data transfers, with the UK government announcing its first adequacy agreement (in principle) with one of its priority candidates, the Republic of Korea. The ICO also gave us a preview of its new TRA guidance during its conference this week, confirming that it will retain its pragmatic risk-based approach to risk assessments for international data transfers, unlike many of its European counterparts that remain focused on the challenges posed by US transfers made via Google Analytics.

We have been encouraged by recent publications from the regulators: the ICO25 strategy (discussed below) was warmly welcomed by DCMS at a roundtable we attended last week, and should offer businesses insight into the ICO's plans and workings, which will be particularly useful if and when the ICO evolves in accordance with the DPDI Bill. The [European Data Protection Board's Vienna statement](#) promises greater cooperation, consistency and potentially man power for the EU data protection authorities (DPAs), which may enable complex cases to be dealt with more efficiently in the EU.

It has been fantastic to finally see many of you in person again during this summer's data privacy conference season and we are looking forward to catching up with you again soon. In the meantime, if you would like to discuss any of the recent developments covered in the newsletter or any other data privacy concerns, please do get in touch.

Have great summer,



Rob Sumroy, Partner

## LEGAL UPDATES

### *UK data protection law reform - progress update*

The government's personal data law reform agenda has made significant progress over the last few months, with the May 2022 Queen's Speech first confirming that a data reform bill would be tabled this Parliamentary term. This was followed by the publication of the [government's response](#) to its 2021 [Data: a new direction consultation](#) in June (we discussed the original consultation in our [September blog](#)). The government's response document outlined which of the consultation's proposals were to be progressed to form part of the new UK data protection regime and which were not, in light of the public response to the consultation. Some of the consultation's more controversial proposals were dropped leading to many commentators welcoming the government's moderated approach. We discuss the consultation response in more detail in our Lens blog: [What we can expect in the Data Reform Bill: UK Government publishes consultation response on UK data protection law reform](#).

Finally, on 18 July, the government introduced the new [Data Protection and Digital Information Bill](#) (the DPDI Bill) to Parliament outlining changes to the UK's data protection regime and largely reflecting the positions taken in the government's consultation response (discussed above). We consider the DPDI Bill in more detail in our [Lens blog](#).

### *ICO funding model update*

Following a new agreement between the DCMS and the Treasury, from this year onwards the ICO will be able to retain some of the funds paid by out by organisations as civil monetary penalties for breaches of data privacy legislation. The funds were previously passed in their entirety into the government's central Consolidated Fund but now the ICO will be able to retain fine income up to a maximum of £7.5m annually, to cover "pre-agreed, specific and externally audited litigation costs". While the new funds must be used specifically for litigation costs, supporting the ICO in litigating complex cases, the regulator has recognised that this will free up other funds for its business advice and support services. The [announcement](#) of the funding uplift for the ICO came within days of the publication of the government's response to its data reform consultation which outlined major changes to the structure and duties of the ICO.

### *UK announces adequacy 'agreement in principle' with the Republic of Korea*

The UK has signed an adequacy [agreement in principle](#) with the Republic of Korea, the first of the UK's priority jurisdictions for adequacy (discussed in our [November 2021 newsletter](#)) to be progressed to this stage. Once an operative adequacy regulation is in place, UK organisations will be able to transfer data to the Republic of Korea securely and without any restriction, however, it is currently unclear how quickly the UK government will finalise an operative adequacy regulation following this initial agreement. The UK's recent agreement with the Republic of Korea follows the EU's adoption of an adequacy decision for the country [last December](#).

## CASE LAW UPDATE

### *High Court confirms Warren's restriction on claimant costs recovery in cyber-attack cases*

In welcome news for controllers, in [Smith and others v TalkTalk Telecom Group plc](#), the High Court confirmed the position in [Warren v DSG Retail Ltd](#) (discussed in our [November 2021 newsletter](#)). The Smith case was concerned with the cyber-attacks on TalkTalk (in relation to which TalkTalk was fined a total of [£500,000 by the ICO](#) in 2016 and 2017). The High Court struck out the claim for misuse of private information (MPI) on the basis that there had not been positive wrongful conduct by the defendant telecom company that amounted to a misuse of the claimants' data. Smith and Warren reduce the availability of costs recovery for claimants in these types of cases (particularly for after-the-event insurance premiums), as the procedural rules in relation to MPI costs recovery are less restrictive than those for statutory data breach claims. Subject to successful appeal, this latest finding will likely further reduce the financial viability of such individual claims against organisations following third party cyber-attacks.

## *Lloyd v Google impact continues*

The ramifications of last year's Lloyd v Google decision (discussed in our [November blog](#) and in our [April newsletter](#)) are continuing to be felt with data privacy mass claims being significantly curtailed, for example:

- the high profile opt-out claim against TikTok (discussed in our [April newsletter](#)) led by former UK Children's Commissioner Anne Longfield has been withdrawn, as the financial risks of the claim were too great for the litigation's funders and insurers according to [statements by Longfield](#);
- the representative action against Experian, in which lead claimant Elizabeth Williams was seeking £750 each for approximately 40 million affected individuals in the UK in relation to data protection failings identified in the [ICO's 2020 enforcement notice](#), has also been discontinued. In the meantime, we still await the outcome of Experian's First Tier Tribunal appeal against the ICO's action (discussed in our [April newsletter](#)).

While they are more scarce, some privacy mass claims are proceeding - at the end of April a new representative action was filed against Deepmind, in relation to a data sharing agreement between the Google subsidiary and the Royal Free NHS Foundation Trust in 2015 (that was the subject of [ICO investigation](#)). This follows a previous similar claim against Google and Deepmind that settled (discussed in our [April newsletter](#)).

## REGULATOR GUIDANCE

KEY REGULATOR GUIDANCE	
ICO	
<a href="#">ICO25 strategic plan</a> (consultation closes on 22 September 2022)	July 2022
<a href="#">ICO and NCSC joint letter to Law Society on ransomware payments</a>	July 2022
<a href="#">Privacy in product design</a> (consultation closes on 31 August 2022)	May 2022
<a href="#">Updated AI and data protection risk toolkit</a> (updated version)	May 2022
European Data Protection Board (EDPB) / EU Commission	
<a href="#">EDPB moves ahead with closer cooperation on strategic cases</a>	July 2022
<a href="#">Statement 02/2022 on personal data transfers to the Russian Federation</a>	July 2022
<a href="#">Guidelines 07/2022 on certification as a tool for transfers</a> (consultation closes on 30 September 2022)	June 2022
<a href="#">EU Commission: Questions and Answers for the two sets of Standard Contractual Clauses</a>	May 2022
<a href="#">Guidelines 04/2022 on the calculation of administrative fines under the GDPR</a> (consultation closed on 27 June 2022)	April 2022

## UPDATES FROM THE ICO

### *ICO publishes 2022-2025 strategic plan*

On 14 July 2022 the ICO [published](#) its new three year strategy plan, [ICO25](#), for consultation.

ICO25 sets out that the overriding purpose of the ICO is to “empower people and organisations through information.” The strategy then includes four “enduring objectives”: (i) to safeguard and empower people particularly the most vulnerable, by upholding information rights; (ii) to empower responsible innovation and sustainable economic growth; (iii) to promote openness, transparency and accountability, support the development of a modern Freedom of Information (FOIA) and Environmental Information (EIR) practice framework in the UK; and (iv) to continuously develop the ICO’s culture, capability and capacity.

Each year the ICO will publish an ‘annual plan’ to outline the priority work it will deliver in the next 12 months to help achieve these four objectives. Its annual plan for October 2022 to October 2023 (annexed to the ICO25 strategy) includes:

- **Safeguarding and empowering people:** development of a subject access generator tool and new FAQs on data rights to help individuals make access requests and understand their rights; continued focus on children’s privacy including enforcing compliance with the Children’s Code; launching an investigation into AI discrimination in recruitment processes and producing refreshed guidance on algorithmic fairness for AI developers.
- **Empowering responsible innovation and sustainable economic growth:** creation of new template materials to assist with accountability/privacy management programme requirements; introduction of iAdvice, a fast feedback service for innovators; production of ‘data essentials’ training modules aimed at SMEs; publication of a ‘guidance pipeline’ to inform organisations of upcoming guidance (currently to include the updated direct marketing code and guidance on emerging tech among others); and providing increased transparency about what regulatory action is being taken and why.

The ICO has also proposed within ICO25 to take a revised approach to public sector enforcement to reduce the impact of fines in the public sector. Fines will only be issued in the most serious cases, with the ICO planning to work more closely with the public sector to encourage compliance and prevent harms before they happen. This new approach [was announced](#) ahead of ICO25, with the revised approach being adopted in relation to enforcement actions against the [Tavistock and Portman NHS Foundation Trust](#) and the [NHS Blood and Transplant Service](#) early in July.

ICO25 also includes an extensive list of performance targets it will report against annually, including referring or closing 80% of personal data breach reports within 30 days and concluding 95% of all formal investigations within 12 months of them starting.

The ICO is consulting on the plan until 22 September 2022 and will use feedback to shape the final version of the ICO25, with a final version expected in October 2022. While the strategy document acknowledges the governments’ data law reform work-stream (“[the] ICO25 plan anticipates, embraces and looks beyond those changes”) the plan may well need amendment to reflect developments during the consultation period following the publication of the Data Protection and Digital Information Bill.

### *ICO publishes joint letter with NCSC on ransomware payments*

On 7 July 2022, the ICO and the National Cyber Security Centre (NCSC) [published a joint letter](#) to the Law Society to ask for assistance in sharing key messages with the legal profession in relation to ransomware incidents. The letter confirms that the ICO will not consider the payment of ransomware demands a mitigating factor when considering enforcement action. It also outlines that the ICO will consider early engagement and cooperation with the NCSC positively when considering an enforcement response. We discuss this development in more detail in our Lens blog: [Has the ICO just told lawyers not to advise clients to pay ransoms?](#)

## UPDATES FROM THE EDPB

### *Guidelines 04/2022 on the calculation of administrative fines under the GDPR*

The EDPB has published [draft guidelines](#) on the calculation of fines under the GDPR, with the aim of harmonising and providing transparency on the methods used by DPAs. The draft guidelines introduce a 5-step calculation method. This includes an approach to multiple infringements, a starting point for calculations and guidance towards achieving consistency with taking aggravating or mitigating factors into account. The final amount of a fine is at the discretion of a DPA, subject to the calculation rules laid out in the GDPR, with fines required to be determined on a case-by-case basis and effective, proportionate and dissuasive.

### *EU Commission: Questions and Answers for Standard Contractual Clauses*

To assist organisations with practical application of the EU's 2021 Standard Contractual Clauses (SCCs) (discussed in our [June 2021 Lens blog](#)), the EU Commission has published a [Questions and Answers \(Q&As\) document](#) on the SCCs based on the feedback received from various stakeholders on using the new SCCs. We discuss the key takeaways from the Q&As and practical compliance with the EU SCCs in [July's edition of the Privacy Laws & Business journal](#).

## ICO ENFORCEMENT OVERVIEW

### *Clearview AI fine confirmed*

The ICO [has fined](#) Clearview AI Inc just over £7.5m in connection with its use of images collected from the web and social media to create a global online database for facial recognition purposes. The fine was reduced from the provisional figure of £17m included in the ICO's preliminary enforcement notice in November 2021 (which we discussed in our [April newsletter](#)). The ICO have also issued an [enforcement notice](#) against Clearview requiring it to stop obtaining and using the publically available personal data of UK residents from the internet, and to delete the data of UK residents from its systems. The ICO's final action against Clearview finds the company in breach of a broad range of GDPR requirements including for a lawful basis for processing, transparency, data minimisation and in respect of individuals' access rights and special category data. It also takes an expansive view of the extraterritorial scope of the UK GDPR. It has been confirmed that Clearview AI is appealing against the ICO's action. We discuss some of the key aspects of the ICO enforcement action in [our blog](#).

Clearview AI has also been the focus of enforcement action in Europe and beyond, with the Greek DPA [fining](#) the organisation 20m euros earlier this month. Like the ICO, the Greek DPA also required Clearview to cease processing the biometric data of individuals in Greece. The Greek decision follows previous action by the [Italian](#) and [French](#) DPAs against Clearview. A number of actions have also been taken against Clearview in the US, with the ICO enforcement notice against Clearview citing measures taken by Clearview in Illinois in response to a claim.

### *Update on appeals*

This week, the First Tier Tribunal (FTT) published its [judgement](#) in relation to the appeal by DSG Retail Limited (DSG) against the [ICO's £500,000 penalty](#) (the pre-GDPR maximum) in connection with its 2017-2018 data breach. The FTT reduced the penalty by half to £250,000, having rejected the majority of the ICO's findings in relation to the extent of DSG's security failings that led to the cyber-attack. The FTT also disagreed with some of the ICO's findings in relation to the extent of personal data (rather than non-personal data) that was compromised in the cyber-attack. Despite welcoming the substantial fine reduction, DSG have confirmed that it will appeal against the FTT's decision on the basis that the remaining aspects of the ICO's decision warrant review.

Conversely, Ticketmaster has decided not to proceed with its appeal against the [ICO's £1.25m fine](#) against the company, issued in November 2020 in relation to Ticketmaster's 2018 data breach. Ticketmaster's appeal had been stayed pending the outcome of two High Court cases relating to the 2018 data breach, however both cases settled earlier this year without any admission of liability (as discussed in our [April newsletter](#) and our [July 2021 newsletter](#)).

## EU GDPR ENFORCEMENT OVERVIEW

The table below sets out a selection of the most substantial EU GDPR fines brought by DPAs in the last 3 months, along with an indication of the principal areas of non-compliance addressed by each enforcement action.

DPA (Country)	Company	Amount	Date	Description
HDDPA (Greece)	<a href="#">Clearview AI</a>	€20 million	13 July 2022	Lack of lawful basis, transparency, individuals' rights
CNIL (France)	<a href="#">TotalEnergies Electricité et Gaz France</a>	€1 million	30 June 2022	Direct marketing, individuals' rights
AEPD (Spain)	<a href="#">Google LLC</a>	€10 million	18 May 2022	Unlawful data sharing and data deletion
CNIL (France)	<a href="#">Dedalus Biologie</a>	€1.5 million	15 April 2022	Data security, lack of processor terms
AP (Netherlands)	<a href="#">Dutch Tax and Customs authority</a>	€3.7 million	12 April 2022	Lack of lawful basis, transparency, data accuracy, retention
Datatilsynet (Denmark)	<a href="#">Danske Bank</a>	€1.3 million	04 April 2022	Accountability

### EU DPAs bring broad brush enforcement

Recent EU DPA actions include a number of significant fines brought in relation to broad non-compliance with central GDPR principles, with similarities to the ICO's approach in its recent Clearview AI enforcement action (discussed above), for example:

- the Spanish DPA [announced](#) its highest fine to date, €10 million, against Google LLC for unlawfully transferring personal data to a US-based third party without appropriate legal basis, and for hindering data subjects' right to be forgotten;
- the Dutch DPA also [announced](#) its highest fine to date, €3.7 million, against the Dutch tax authorities in connection with their development and maintenance of an anti-fraud database. The Dutch DPA found that the tax authorities lacked a lawful basis for the processing and that the database included inaccurate data which was retained for too long, resulting in significant adverse consequences for individuals wrongly being labelled as fraudsters; and
- the Danish DPA fined [Danske Bank](#) for a lack of GDPR accountability (contrary to GDPR Article 5(2)), after the bank self-reported concerns about its data retention practices. The bank was unable to confirm whether data storage and deletion rules had been implemented for over 400 systems operated by the bank which were connected with the processing of millions of individuals' personal data.

### EU spotlight on international data transfers

In contrast to the ICO, EU regulators continue to focus on data transfers and particularly those made via Google Analytics. Recently, the [Garante](#) (the Italian DPA) has followed the [French](#) and [Austrian](#) DPAs in confirming that data transfers to the US by Google Analytics violate the GDPR, as the measures adopted to protect the personal data transferred do not currently guarantee an adequate level of protection. The findings follow a series of complaints made by privacy campaign group NOYB. In light of these decisions, in June the French DPA attempted to assist organisations by publishing a [Q&A](#) on the use of Google Analytics. Meanwhile, EU justice commissioner Didier Reynders has suggested that the incoming EU-US partial adequacy decision, the Trans-Atlantic Data Privacy Framework, that promises to ease some of the challenges for EU-US data transfers following the Schrems II decision (discussed in our [Lens blog](#)), is now not expected to be finalised in 2022 but early next year.

## VIEW FROM ... THE UNITED STATES OF AMERICA ON THE AMERICAN DATA PROTECTION AND PRIVACY ACT (ADPPA)

*Contributed by Maneesha Mithal, Partner, Wilson Sonsini Goodrich & Rosati, Washington, D.C.*

The U.S. Congress is moving quickly to try to enact comprehensive federal privacy legislation in the form of the American Data Privacy and Protection Act (ADPPA). This historic, bipartisan bill, if enacted, would significantly change the privacy landscape in the United States. This week, the House Energy and Commerce Committee took another step toward passage, reporting the bill out of Committee, by a vote of 53-2. Here are some quick highlights of the discussion surrounding the ADPPA in the U.S.

**What would the bill do?** For the first time, it would impose broad-based, statutory obligations on companies to protect the privacy of consumers' personal information, requiring them to limit the amount of data they collect, process, or transfer; maintain privacy policies and provide consumers with the right to data access, correction, deletion, and portability; maintain reasonable data security, and obtain consumers' consent for collection, processing, and transfer of sensitive data, among other things.

**Is it stronger than U.S. state privacy law?** Many experts agree that it is stronger than state privacy law. In addition to including general consumer rights provisions contained in state privacy laws, it would prohibit the practice of algorithmic discrimination, require data brokers to register with the Federal Trade Commission, and impose certification requirements on certain corporate officers. The California Privacy Protection Agency (CPPA) raised some objections to the bill on the basis that it would preempt California law, which they view to be stronger. Sharing this concern, two California Members of Congress voted against the version of the bill that was reported out of the House Energy and Commerce Committee.

**What are the sticking points?** For a long time, comprehensive federal privacy legislation was stalled in Congress because of disputes over the extent to which such legislation would preempt state laws and the extent to which the legislation would include a private right of action. The ADPPA reflects a compromise, generally preempting state law and allowing for a limited private right of action. In addition to the preemption issue discussed above, the scope of the private right of action appears to continue to be a sticking point. Other sticking points seem to include the extent to which pre-dispute binding arbitration should be allowed; the extent to which the bill includes a "duty of loyalty" (other drafts have included a more expansive duty to "do no harm" to the consumer); and whether safe harbor provisions should be included, which would allow compliance with approved industry programs to be deemed compliance with the law.

**What is the likelihood of passage?** Although the bill has the support of a bipartisan coalition in the House of Representatives and reflects significant compromises, it does not have the support of a key Senate Democrat Maria Cantwell, Chair of the Senate Committee on Commerce, Science, & Transportation. Without her support, and with time running out in this year's legislative session, experts are not optimistic. Indeed, a companion bill has not yet been introduced in the Senate. Nonetheless, the ADPPA reflects a significant milestone in negotiations on a federal privacy bill and sets an important baseline for future privacy legislation in the United States.

### THE LENS

Our blog, The Lens, showcases our latest thinking on all things digital (including Competition, Cyber, Data Privacy, Financing, Financial Regulation, IP/Tech and Tax). To subscribe please visit the blog's [homepage](#). Recent posts include: [UK promises 'light-touch, pro-growth regulatory regime' in new digital strategy](#); [Do you know how to manage your cyber supply chain risk?](#); [No longer "too big to care": EU's Digital Services Act takes aim at Musk and online platforms](#); and [Google responds to CNIL Cookie Fine - 'Reject All' now on equal footing](#).

## 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 businesses 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](mailto:rob.sumroy@slaughterandmay.com)



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



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



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



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



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



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



Bryony Bacon  
Data Privacy PSL  
T: +44 (0)20 7090 3512  
E: [bryony.bacon@slaughterandmay.com](mailto: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, 2022.  
For further information, please speak to your usual Slaughter and May contact.

[www.slaughterandmay.com](http://www.slaughterandmay.com)