

# DATA PRIVACY

## SELECTED LEGAL AND REGULATORY DEVELOPMENTS IN DATA PRIVACY

### QUICK LINKS

[LEGAL UPDATES](#)[CASE LAW UPDATE](#)[REGULATOR GUIDANCE](#)[UPDATES FROM THE ICO](#)[UPDATE FROM THE EDPB](#)[UK ENFORCEMENT OVERVIEW](#)[EU ENFORCEMENT OVERVIEW](#)[VIEW FROM INDIA](#)[THE LENS](#)

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

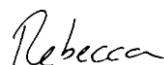
Well, it certainly has been a busy autumn. We were delighted to discuss data commercialisation over breakfast with a number of you in September. It is clear that many organisations are looking to use data to increase revenue or to drive efficiency savings, or are at least interested in doing so, given recent tech advances. We discussed that good data governance is the necessary foundation for such projects. For some, getting the cross-organisational support for less glamorous but essential ‘data hygiene’ exercises, such as ensuring data is accurate and up to date, remains challenging. Recent enforcement actions from the EU around data quality (discussed on p.6) emphasise the broader importance of these projects.

A recurring theme from within our data commercialisation discussions was cookie compliance. Despite the ICO tending to focus its enforcement action on processing that poses a high risk to individuals (such as telemarketing to vulnerable individuals, discussed on p.5), senior figures at the ICO have indicated the regulator will be looking more closely at companies deploying non-compliant cookie banners and that it will be looking to enforce in this area. With the DPDI (No. 2) Bill now expected to be in force by next summer, with its escalated penalties for e-marketing and cookies, this is likely to remain an area of focus and challenge for us all.

Last but not least, the [UK-US data bridge](#) has now been finalised, normalising transfers from the UK to the US for the first time post-Schrems II. We can see the clouds of further legal challenge continuing to gather, particularly in relation to the EU-US arrangement. Focus will now fall on the EU’s existing adequacy decisions, including those for New Zealand and Canada, after an EU Commission official suggested at a conference in September that their reviews would be published soon and may involve new additional safeguards being put in place.

We are looking forward to welcoming many of you or your colleagues to our Data Privacy Forum Academy on 30 November when we will be reflecting further on a number of these developments.

Rebecca Cousin, Partner



## LEGAL UPDATES

### UK-US data bridge finalised and operational

As anticipated in our [previous newsletter](#), the UK-US data bridge (the UK's partial adequacy assessment for the US) was finalised earlier this autumn and took effect on 12 October, when the [Data Protection \(Adequacy\) \(United States of America\) Regulations 2023](#) became law. The UK-US data bridge confirms that the US provides an adequate level of protection for data transfers under the UK GDPR where the US recipient organisation has signed up to participate in the UK Extension to the [EU-US Data Privacy Framework \(DPF\)](#). The Government has helpfully published a number of supporting documents for the UK-US data bridge, including a [factsheet](#) which provides additional detail for UK organisations on the scope of the data bridge, and a [supporting analysis](#) for the Government's adequacy assessment. At the recent Data Protection Practitioners' Conference (DPPC), the ICO recommended that UK organisations making transfers to US entities outside the scope of the data bridge (i.e. not registered under the DPF) make reference to that supporting analysis document in their transfer risk assessments. We discuss the data bridge further in our [blog post](#).

Meanwhile, the first of the widely expected legal challenges against the EU-US DPF (discussed in our July [blog](#)) has reached the CJEU. An application for interim suspension of the framework, lodged by MEP Philippe Latombe, has been rejected. However, the MEP has lodged another case against the EU Commission in relation to the DPF, which is still proceeding in the EU's General Court.

### Online Safety Bill becomes law

On 19 September, the text of the [Online Safety Bill \(OSB\)](#) was finally agreed by Parliament, some eighteen months after its first reading. The OSB, which imposes a host of new duties on in-scope online services, will, according to the government, "make the UK the safest place in the world to be online". We discuss this in more detail in our recent [blog](#).

## CASE LAW UPDATE

### CJEU to consider further non-material damages questions

The issue of non-material damages is set to be reconsidered by the CJEU. The Latvian Supreme Court has asked the court to clarify [three issues](#), which will provide useful guidance for controllers addressing cyber/data breaches. The CJEU has been asked to clarify whether an apology is sufficient compensation for non-material harms; whether unlawful processing alone breaches the right to data protection; and whether the attitude and motivation of a processor can result in a reduction of compensation for damages. In making the request the Latvian court acknowledged the CJEU had set a framework to determine compensation in the Austrian Post judgment (see our [November 2022 newsletter](#)) but that questions remained for how domestic case law is compatible with the GDPR when assessing claims for damages. Separately, Advocate General Collins has relied on the Austrian Post decision when stating, in a non-binding [opinion](#), that the theft of personal information may lead to non-material damages where there is a causal link between the infringement and the cause of damage.

### CJEU to hear more fine calculation questions

A Danish court is [seeking](#) clarity from the CJEU on the meaning of 'undertaking' for the purpose of GDPR Article 83, in the context of a corporate group. The Danish Data Protection Authority (DPA) had recommended a 1.5 million Kroner (\$200,000) fine for furniture company, ILVA, for storage limitation and accountability failings, based on the turnover of ILVA's parent company. However, the Danish court of first instance rejected the Danish DPA's fine on the basis that the relevant turnover is that of ILVA itself, rather than its parent. The court's decision was further appealed on the basis that "undertaking" should be construed in line with antitrust case law. However, in finding that the GDPR did not provide the correct metric to calculate fines, the Danish High Court has asked the CJEU for clarification.

## REGULATOR GUIDANCE

KEY REGULATOR GUIDANCE	
ICO	
<a href="#">Employment practices and data protection – monitoring workers (final version)</a>	October 2023
<a href="#">Consultation on draft data protection fining guidance (consultation closes on 27 November 2023)</a>	October 2023
<a href="#">A 10-step guide to sharing information to safeguard children</a>	September 2023
<a href="#">Call for views on period and fertility tracking apps</a>	September 2023
<a href="#">Information about workers' health (final version)</a>	August 2023
<a href="#">Guidance on sending bulk communications by email</a>	August 2023
<a href="#">Consultation on draft biometric data guidance (consultation closed on 20 October 2023)</a>	August 2023
<a href="#">Guidance on "likely to be accessed" by children (final version)</a>	July 2023
EDPB	
<a href="#">EDPS Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments</a>	October 2023
<a href="#">EDPS Opinion 42/2023 on the Proposal for two Directives on AI liability rules</a>	October 2023
<a href="#">EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679</a>	September 2023
<a href="#">Statement 1/2023 on the first review of the functioning of the adequacy decision for Japan</a>	July 2023
<a href="#">EDPB adopts information note on Data Privacy Framework</a>	July 2023

## UPDATES FROM THE ICO

### ICO consults on draft data protection fining guidance

The ICO has published [draft guidance](#) for consultation on how it decides to issue penalty notices and calculate fines under the UK GDPR and Data Protection Act 2018 (DPA18). The draft guidance covers the legal framework that gives the ICO the power to impose fines, the circumstances in which the ICO would consider it appropriate to issue a penalty notice, and how the ICO calculates the appropriate amount of the fine, including the factors that determine that it is effective, proportionate and dissuasive. Like the EDPB, the ICO has proposed a five stage process for setting fines with the starting point being percentage of turnover (see our discussion of the EDPB's [Guidelines on the calculation of administrative fines](#), in our [July newsletter](#) and [blog](#)). In addition, the guidance clarifies that where a controller has breached multiple provisions of the UK GDPR/DPA18 the most serious individual infringement will determine the maximum applicable fine, although there may be fines for each further infringement from similar or linked processing operations. We discuss this draft guidance in more detail in our [blog](#). Views on the draft guidance can be [submitted](#) to the ICO until 27 November 2023.

### ICO consults on biometric data guidance

The ICO has issued initial draft [guidance on biometric data and technologies](#) for consultation with further draft guidance due early next year. The guidance covers what biometric data is, its use in biometric recognition systems and the data protection requirements organisations need to comply with. Both identification (matching biometric data of one person to the data of many others to determine who the person is) and verification (matching one person's biometric data to their own stored record to determine if they are who they claim to be) is included within the scope of biometric recognition. The guidance includes a number of examples of biometric systems, including employee access controls and customer identity verification. The guidance highlights, among other things, that biometric data will be considered special category data where it is used for the purpose of uniquely identifying someone. The guidance also explains when a DPIA will be required, the importance of being clear on controller/processor roles and how explicit consent may be the only valid ground for processing special category biometric data.

### ICO publishes new guidance on monitoring in the workplace

After research conducted by the ICO revealed that individuals were increasingly concerned about how their employers monitor them, the ICO has issued new (final) guidance on [employee monitoring](#), following on from the draft [guidance on monitoring at work](#) that was issued last October (discussed in our [November 2022 newsletter](#)). The guidance distinguishes between those recommendations organisations 'must' follow (as legal requirements) and those they 'should' or 'could' choose to adopt (in line with the ICO's latest approach to its guidance as confirmed at its annual DPPC event). In particular, the guidance focuses on the use of automated monitoring tools and the use of biometric data, with checklists being provided to aid compliance. We discuss the new employee monitoring guidance and the ICO's recent [guidance on workers' health information](#) in more detail in our October [Employment Bulletin](#).

### ICO publishes guidance on sending bulk communications by email

The ICO has also issued [new guidance](#) on how to protect personal information when sending bulk emails. The guidance highlights that even where an email does not contain sensitive information, the recipient list could by itself reveal personal information, as seen in the HIV Scotland data breach (discussed in our [November 2021 newsletter](#)). The guidance highlights that the blind carbon copy (bcc) function should not be used for sending bulk information as it risks mistakenly sharing personal information.

### Increasing regulatory collaboration

Recent months have seen increasing evidence of collaboration and alignment between the ICO and other UK regulators and bodies operating in the digital arena:

- In August, the ICO and the Competition and Markets Authority (CMA) [issued](#) a joint paper examining the impact of harmful online design on consumer choice and the control individuals have over their personal data under the banner of the [Digital Regulation Cooperation Forum](#) (DCRF). The paper acknowledges how harmful web design can lead to data protection harms through influencing consumer decisions in a manner they are not aware as well as raising potential competition and consumer protection harms.
- A new AI and Digital Hub [regulatory advice pilot](#) will launch next year, backed by £2 million in government funding. Its goal is to provide a multi-agency approach to innovative technologies such as AI through the DCRF, with the ICO participating alongside Ofcom, the CMA and Financial Conduct Authority (FCA). It is hoped this will enable businesses to demonstrate that their technology meets regulatory requirements across different sectors and allow them to bring innovations to market faster.
- The ICO and National Cyber Security Centre (NCSC) have signed a [memorandum of understanding](#) reaffirming that the NCSC will never share confidential information with the ICO without seeking consent from the sharer organisation. The memorandum aims to encourage organisations faced with a cyber incident to engage with the NCSC. We discuss this MOU in more detail in our recent [blog](#).

## UPDATE FROM THE EDPB

### EDPB and EDPS issue joint statement on the GDPR Procedural Regulation

The EDPB and the European Data Protection Supervisor (EDPS) have adopted a [Joint Opinion 01/2023](#) on the EU Commission's proposed GDPR Procedural Regulation (discussed in our [July newsletter](#)). The statement recognises that the proposed regulation gives effect to many aspects of the "wish list" of reforms the EDPB submitted to the EU Commission to promote cooperation between EU DPAs and swift enforcement of the GDPR. As such, the statement largely supports the proposals but warns that the 'timely adoption' of the regulation is essential and notes that the regulation will increase the current workload of the EU DPAs, so to allow effective enforcement of the GDPR both the EDPB and EU DPAs will need to be 'provided with sufficient resources'.

## UK ENFORCEMENT OVERVIEW

### Recent reprimands

The ICO has issued statements and public reprimands to a number of public authorities over recent months following high profile data breaches, including the [Police Service of Northern Ireland, Norfolk and Suffolk Constabularies](#) as well as the recent breach at the [Electoral Commission](#). The ICO has also issued a [warning](#) to organisations that data breaches are putting domestic abuse victims lives at risk after the ICO issued seven organisations (public and private sector) with reprimands in the past fourteen months for breaches impacting domestic abuse victims. Key contributing common features of the breaches included lack of staff training and failing to have robust procedures in place to handle personal data safely (such as access controls).

### Focus on telemarketing to the vulnerable

In September, the ICO announced that [fines amounting to £590,000](#) had been given to five companies who made 1.9 million unwanted marketing calls in total. This action comes as part of an ICO focus on companies using pressurising sales techniques to sell insurance for domestic appliances, often to vulnerable individuals. This aligns with the regulator's [ICO25 strategic plan](#), which references the regulator continuing to focus on predatory marketing calls as part of its work in countering issues that may be aggravated by the cost of living crisis.

### ICO issues preliminary enforcement notice against Snap

The ICO [has issued](#) a preliminary enforcement notice against Snap Inc and Snap Group Limited (Snap) over potential failure to properly assess the privacy risks posed by Snap's generative AI chatbot 'My AI'. The ICO's investigation provisionally found the risk assessment Snap conducted before it launched 'My AI' did not adequately assess the data protection risks posed by the generative AI technology, particularly to children. The ICO's action follows the regulator publishing guidance on approaching generative AI in April. The preliminary enforcement notice does not at this stage mention a potential financial penalty for Snap, unlike previous notices of intention (e.g. against [BA](#), [Clearview](#), [TikTok](#)) that have seen the proposed penalty amount reduced materially when the final penalty is issued. However, this latest notice stresses that the Commissioner's findings are provisional at this stage. We discuss the notice further in our recent [blog post](#).

### Clearview AI successfully appeals ICO penalty as FTT considers GDPR extraterritoriality

Clearview AI [has successfully appealed](#) against the ICO fine issued against it in May 2022 (discussed in our [blog](#) at the time). While the First-tier Tribunal (FTT) ultimately ruled that Clearview's data processing was outside the material scope of the GDPR and UK GDPR and so the ICO lacked jurisdiction to impose the penalty (as the use of Clearview's services by its clients were for criminal law enforcement or national security functions), the FTT also considered the extraterritorial effect of the UK GDPR and provided helpful clarification. The FTT endorsed a wide interpretation of the GDPR's extraterritoriality, including of processing 'relating to' behavioural monitoring, as put forward by the ICO. We discuss the decision further in our [blog post](#) on the appeal.

### FCA fines Equifax for 2017 cyber security breach

On 13 October, the FCA announced an £11.2 million fine for Equifax in relation to its 2017 cyber security breach and connected outsourcing failings. This follows the ICO's £500,000 (pre-GDPR maximum) penalty issued against the



company for the same incident in September 2018. In announcing the fine, the FCA's Chief Data, Information and Intelligence Officer said that: "cyber security and data protection are of growing importance to the security and stability of financial services", suggesting that FCA regulated firms should not assume that enforcement action for cybersecurity failings will be limited to, or arguably even led by, the ICO. We discuss these developments further in our [blog](#).

## EU ENFORCEMENT OVERVIEW

The table below sets out a selection of the most substantial EU GDPR fines brought by European data protection 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)	Groupe Canal	€600 000	12 October 2023	Data security
AZOP (Croatian DPA)	EOS Matrix	€5,47 million	5 October 2023	Data security
Garante	Axpo Italia	€10 million	28 September 2023	Data accuracy, lawful basis
Datatilsynet (Denmark)	Arp Hansen Hotel Group	DKK 1 million (circa €134,000)	27 September 2023	Storage limitation
CNIL (France)	SAF Logistics	€200 000	18 September 2023	Data minimisation
DPC (Ireland)	TikTok	€345 million	15 September 2023	Data protection by design and default, data security, transparency
IMY (Sweden)	Trygg Hansa	€3 million	5 September 2023	Data security

### Irish DPA fines TikTok €345 million

The Irish DPA [has fined](#) TikTok €345 million for failings relating to children's data. The Irish DPA adopted its final decision on 1 September 2023, following a [binding decision](#) from the EDPB. The main contraventions identified were in relation to the app's settings for children which contravened the GDPR's requirements for data protection by design and default and data security. For example, the profile settings for children were set to public by default and the app included a 'family pairing' feature which allowed adult users to enable direct messages to children over 16. The Irish DPA also found that TikTok failed to provide sufficient transparency information to child users, and that it implemented 'dark patterns' to influence users to adopt more privacy-intrusive options. As well as imposing the significant financial penalty, TikTok has been ordered to bring its processing into compliance within three months. However, TikTok is pursuing a number of approaches to challenge the decision (an approach previously taken by Meta, as discussed in our [newsletter previously](#)): it has lodged a [case](#) against the EDPB at the CJEU, a judicial review action with the Irish High Court and is pursuing an appeal against the Irish DPA's decision in the Irish High Court.

### Focus on data quality

Several significant enforcement actions have been brought by EU DPAs against private sector organisations for data accuracy, storage and retention failings over recent months emphasising the importance of data governance and accountability programmes. As many organisations and sectors continue to struggle with legacy data, we will be monitoring trends in this area closely:

- The Italian DPA fined energy company Axpo Italia €10 million for switching customers to new agreements using outdated and inaccurate personal data. The DPA's investigation found that the company had used third party

agents to sign up customers without verifying the data collected and had failed to distinguish between existing and newly collected customer data.

- The Danish DPA recently had its fine (c. €134,000) against a hotel chain, Arp-Hansen, upheld by the relevant High Court. The fine related to the company's non-compliance with data deletion deadlines the company had set itself and involved approximately 500,000 customer profiles that should have been deleted as no longer necessary.
- Air freight company SAR Logistics has been fined €200,000 by the French DPA for obtaining excessive data from its employees in the course of an internal recruitment exercise, with the company obtaining large amounts of information via online forms, including about family members and special category data including blood type and political affiliation.

## VIEW FROM... INDIA

*Contributed by Harsh Walia, Partner, Khaitan & Co, India*

### Enactment of the Digital Personal Data Protection Act 2023 in India and its implications on companies in the UK and EU

Following the approval by both Houses of Parliament, the Digital Personal Data Protection Act, 2023 (DPDP Act) obtained Presidential assent and was published in the Official Gazette of India on 11 August 2023. While the provisions of the DPDP Act are yet to be brought into effect through enforcement related notifications, it is expected that further clarity will emerge regarding this new legislation with the issuance of rules, which are ready to be rolled out according to the Government. The following key provisions are relevant to note for entities in the EU and UK:

- As far as applicability of the DPDP Act to data fiduciaries (akin to data controllers) outside India is concerned, unlike the EU's GDPR, it does not apply to data fiduciaries profiling personal data of data principals (akin to data subjects) but applies only to those data fiduciaries processing personal data in connection with offering goods and services to data principals in India.
- In contrast to the GDPR, the DPDP Act governs personal data in digital form only. Also, it does not include a sub-category of sensitive or special category personal data.
- Processing of personal data under the DPDP Act can be undertaken either on the basis of consent in the prescribed manner or under legitimate uses (e.g., voluntary disclosure for specific purposes, employment, medical emergency, compliance with law, etc.). Accordingly, entities will have to choose the correct ground for processing in each case. One of the key bases for processing under GDPR, i.e. legitimate interests, is not available under the DPDP Act.
- The DPDP Act sub-classifies certain data fiduciaries as 'significant data fiduciaries' (SDF), based on prescribed criteria such as volume and sensitivity of personal data processed, risk to rights of data principals, etc. An entity will have to comply with certain additional obligations such as appointment of a Data Protection Officer in India, conducting Data Protection Impact Assessments, appointment of independent data auditor, etc. if it is classified as an SDF.
- The DPDP Act defines a child as an individual who has not reached the age of 18 years and, therefore, UK/EU entities' verifiable parental consent mechanisms will likely need to be revisited as the GDPR prescribes a much lower age bracket for children.
- Unlike the GDPR which prescribes risk-based thresholds for personal data breach reporting to authorities and affected individuals, the DPDP Act appears to require notification to both the Data Protection Board of India and the affected data principals in all cases.

It is crucial for entities to take relevant steps to achieve compliance with the new law in the period leading up to the commencement of the DPDP Act, in order to avoid hefty penalties which can go up to INR 250 crores (approx. USD 30 million) in certain cases. There is also no aggregate cap for the penalty amount in case of multiple breaches.

## 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 Government finalises IoT cybersecurity requirements](#), [‘Groundbreaking’ online safety law finally passes](#), [DSA now in force for largest platforms](#).

## 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 Data Privacy Knowledge  
T: +44 (0)20 7090 5168  
E: [cindy.knott@slaughterandmay.com](mailto:cindy.knott@slaughterandmay.com)



Bryony Bacon  
Senior PSL, Data Privacy  
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, 2023.  
For further information, please speak to your usual Slaughter and May contact.

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