

# DATA PRIVACY

## SELECTED LEGAL AND REGULATORY DEVELOPMENTS IN DATA PRIVACY

### QUICK LINKS

[LEGAL UPDATES](#)[CASE LAW UPDATE](#)[REGULATOR GUIDANCE](#)[UPDATES FROM THE  
ICO](#)[UPDATES FROM THE  
EDPB](#)[ICO ENFORCEMENT  
OVERVIEW](#)[EU GDPR  
ENFORCEMENT  
OVERVIEW](#)[VIEWS FROM... CHINA  
AND HONG KONG](#)[DATA PRIVACY AT  
SLAUGHTER AND MAY](#)

### 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

It has been fantastic to catch up with a number of you in recent weeks, particularly during the roundtable breakfasts we held on data breaches in June and most recently at the Privacy Laws & Business conference in Cambridge. As we all discussed, the last few months have seen privacy professionals face new and emerging challenges - from the meteoric rise of generative AI to the widespread supply-chain cyber-attacks. During these conversations, we have been reminded of the value of sharing experiences and knowhow with peers, particularly in the space between developments occurring and regulatory guidance catching up.

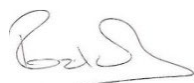
International data transfers, particularly between the EU and US, have remained a hot topic over the last few months and we were grateful to share a stage at PL&B at the start of the month with a Commissioner from the French regulator and a Senior Counsel from the US DOJ to discuss the EU-US Data Privacy Framework. In our preparatory discussions ahead of the session, we talked about the DPF being the next step in a longer-term process for EU-US data flows and perhaps, for now, that is the best way to think about it - as a positive step forward rather than a conclusive solution.

In other developments, the ICO has continued to demonstrate its 'outcomes not outputs' regulatory approach that we discussed last time, with a settlement agreement for Easylife and a reduced fine for TikTok indicating the ICO is focusing its resources where they can create the most impact in practice rather than the most headlines. Meanwhile, headlines have not been in short supply for the Irish Data Protection Commission, with its record-breaking Meta transfers fine. Although much of the sting has now been taken out of that decision by the DPF developments, it was a reminder of the full force of the GDPR's fining powers.

Against this fast-moving backdrop, the ICO is maintaining its focus on emerging tech and AI and has attempted to walk a path between being a pro-innovation regulator and meaningfully enforcing DP law. For example, in the same week the Italian DPA banned ChatGPT (albeit temporarily), the ICO issued guidance on its use for those developing and using the software and it has recently published guidance on a range of tech topics including PETs and neurotech.

We look forward to catching up soon to discuss these and other developments. For those of you we don't see beforehand, we hope you have wonderful summer breaks.

Rob Sumroy, Partner



## LEGAL UPDATES

### Developments in international transfers

On 10 July, the EU-US Data Privacy Framework (DPF) adequacy decision was [adopted](#) by the European Commission, allowing data to flow freely from the EU to organisations registered under the DPF in the US. We discuss the adoption of the DPF and next steps for organisations in the EU and UK, in more detail in our [blog](#). An equivalent agreement for UK-US data flows may not be too far behind the DPF, as an [agreement in principle](#) for a UK-US ‘data bridge’ was announced in June. While the UK and US previously announced an intention to move towards adequacy in October 2022 (discussed in our previous [newsletter](#)), this latest announcement suggests further concrete progress has been made and we now expect the UK-US deal to be in place by the end of the year.

Meanwhile, global initiatives to promote international data flows are gaining some momentum. Data flows were a priority area for the G7 Data Protection Authorities when they met in Japan at the end of June, with the post-summit [communiqué](#) indicating that a working group of countries (co-chaired by the UK and France) are progressing projects to facilitate ‘data free flows with trust’. In April, the UK applied to join the [Global Cross-Border Privacy Rules Forum](#) (CBPR) and in doing so became the first new jurisdiction to join since the inception of the CBPR last year.

### EU Commission proposes new regulation to streamline cross-border GDPR enforcement

The EU Commission has adopted a proposal for a new regulation, the [GDPR Procedural Regulation](#), to boost cooperation between European data protection authorities (DPAs) when enforcing the EU GDPR in cross-border cases, with a view to speeding up the completion of EU GDPR investigations and curbing the amount of cases being escalated to the EDPB’s dispute resolution procedure (nine cases have been escalated [so far](#), with five in 2022 alone as outlined in the EDPB’s [2022 Annual Report](#)). The proposals set out new supplemental procedural rules for EU DPAs in such cases, including: new steps in the cooperation process between EU DPAs to facilitate early consensus building; clarification of the status of complainants under the GDPR; and clarification of the rights of controllers and processors under investigation. The proposals are currently subject to an eight-week consultation period after which they will need to be agreed by both the European Parliament and Council before becoming law.

## CASE LAW UPDATE

### Courts provide guidance on data subject access requests

Recent case law from the Court of Justice of the European Union (CJEU) and UK courts has provided some additional guidance for organisations on the scope of data subjects access requests (DSARs):

- In a [case](#) referred from Finland, relating to access by bank staff to data of a customer and ex-employee, the CJEU stated that individuals have the right to access information concerning the date on which and the purposes for which their data was accessed, but generally do not have the right to find out the identity of employees who carried out the processing on instructions from their employer. That is unless access to the employee’s identity is essential to the individual’s ability to exercise their GDPR rights effectively, and even then, provided the rights and freedoms of those employees are taken into account.
- In the CJEU’s judgement between [Österreichische Datenschutzbehörde and CRIF](#), the Court gave guidance on what it means to have to provide ‘a copy of the personal data undergoing processing’ (GDPR Article 15(3)). The Court was asked to rule on the question of whether the obligation was satisfied by provision of personal data in the form of a summary table, or whether the obligation requires greater disclosure. The Court confirmed that data subjects are entitled to be given ‘a faithful and intelligible reproduction’ of all their data undergoing processing and must be given copies of document extracts, or even entire documents, if the provision of the copy is essential to enable them to effectively exercise their GDPR rights (e.g. to check their data is correct and is being processed in a lawful manner). However, once again, this right must be balanced against the rights and freedoms of others.

- A recent case from the UK High Court, [X v The Transcription Agency LLP and Master Jennifer James](#), has made reference to the purpose of DSARs, holding that the UK DSAR regime has a “specific and limited purpose” to enable a data subject to check whether a controller’s processing of their personal data infringes their privacy rights and take action if so. Contrary to ICO guidance which maintains that DSARs are ‘purpose blind’, the Court held (citing [Durant](#)) that “it is impermissible to deploy the machinery of the Act as a proxy for the wider purpose of obtaining documents with a view to litigation or further investigation”. It is worth bearing in mind that this conclusion came in the context of a relatively extreme fact-pattern, in which a claimant made a DSAR against the costs judge in their case.

Further new guidance on DSARs has come from the ICO in their [DSARs Q&A for employers](#). The new guidance reflects the ICO’s existing guidance on the right of access, but contains new helpful examples on the various exemptions that may allow employers to withhold or limit the information they supply when responding to a SAR. We discuss this guidance in more detail in our [Lens blog](#). The EDPB has also issued the final version of its DSAR guidance, discussed below.

### Data privacy mass claim update

In another attempt to circumvent the restrictions placed on data claims by [Lloyd v Google](#), a class action case against [Google and DeepMind Technologies](#) (in relation to the data sharing between Deepmind and the Royal Free London NHS Trust) brought by Andrew Prismall on the basis of misuse of private information, has been rejected by the High Court. In rejecting the claim, the Court performed a “lowest common denominator” analysis in which it found not every member of the class had a viable claim, in a similar result to seen in [Lloyd v Google](#). The case further limits the chances of success for data privacy related class actions as it stands, however, Andrew Prismall has applied for permission to appeal. In another recent development, Equifax and a group of claimants have [requested](#) the use of a preliminary issues trial to decide the value of the case relating to Equifax’s 2017 data breach, instead of seeking a group litigation order. The aim of this is to decide either the entirety of the claim, or a significant portion, which would increase the likelihood of settlement and reduce costs of the main action. The case is proceeding to a case management conference in the autumn, but the judge has not yet been persuaded by the parties’ approach.

### Data protection / competition law overlap clarified by CJEU

The CJEU has allowed the German competition authority to rely on GDPR violations in order to establish an abuse of a dominant position by Meta. In issuing the [judgment](#) the Court referred to [advocate-general Rantos’ opinion](#), in that a dominant company’s GDPR violations may provide an important clue to whether their behaviour is anti-competitive. Furthermore, the judgment emphasised that competition authorities were not a replacement for data protection authorities and must cooperate with them. This decision is discussed in more detail in our latest [Competition & Regulatory newsletter](#).

## REGULATOR GUIDANCE

KEY REGULATOR GUIDANCE	
ICO	
<a href="#">Privacy-enhancing technologies (PETs) (final version)</a>	June 2023
<a href="#">ICO tech futures report on neurotechnology</a>	June 2023
<a href="#">DSARs Q&amp;A for employers</a>	May 2023
<a href="#">ICO consultation on the draft guidance for ‘Likely to be accessed’ in the context of the Children’s code</a>	May 2023
<a href="#">The Information Commissioner’s response to the Government’s AI White Paper</a>	April 2023

## KEY REGULATOR GUIDANCE

## EDPB

<a href="#">Guidelines 04/2022 on the calculation of administrative fines under the GDPR (final version)</a>	May 2023
<a href="#">Guidelines 03/2021 on the application of Article 65(1)(a) GDPR (final version)</a>	May 2023
<a href="#">Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority (final version)</a>	May 2023
<a href="#">Guidelines 01/2022 on data subject rights - Right of access (final version)</a>	April 2023
<a href="#">Guidelines 9/2022 on personal data breach notification under GDPR (final version)</a>	April 2023

## UPDATES FROM THE ICO

[ICO issues privacy enhancing technologies guidance](#)

The ICO has issued new detailed guidance on [privacy enhancing technologies](#) (PETs) with a specific focus on those using large data sets in the finance, healthcare, research and governmental sectors. The ICO initially [published](#) draft guidance on PETs in September 2022 (discussed in our previous [newsletter](#)). In the press release announcing the latest guidance, the Information Commissioner encouraged organisations that process large quantities of data to begin using PETs over the next five years and we heard the ICO's Group Manager for Anonymisation & Encryption suggest at the PL&B conference in July that the ICO will now be moving to the enforcement phase in relation to PETs.

[ICO maintains focus on emerging technologies, including AI](#)

As mentioned in the editorial, understanding and responding to emerging technologies, including AI, remains one of the ICO's priorities (in accordance with the regulator's [ICO25](#) strategy) and this is seen in a number of its recent publications. In April, the ICO issued its [response](#) to the Government's long-awaited AI white paper, which outlined the Government's plans for the regulation of AI in the UK to maintain the current sector-specific approach (see our [blog](#)). While expressing support for the Government's approach, the ICO made a number of recommendations, including that the Government should engage with sector regulators through the Digital Cooperation Regulatory Forum and to encourage close collaboration with the ICO to ensure the new AI white paper principles are interpreted in a way that is compatible with the existing data privacy principles.

The ICO has also issued its own [guidance on generative AI](#) and large language models, in a blog from Stephen Almond, the ICO's Executive Director of Regulatory Risk at the beginning of April. The blog advises that "while the technology is novel, the principles of data protection law remain the same". It emphasises the importance of data privacy by design and lists eight questions developers or users of generative AI should ask themselves, reflecting key GDPR compliance obligations (such as lawful basis, controller/processor roles, DPIAs, transparency and security). We discuss the interaction between AI and Data Privacy in more detail in this [briefing](#). As part of its work on emerging technologies, the ICO has also recently published a 'tech futures' report on neurotechnology (following on from its previous [Tech Horizons Report](#) discussed in our [March newsletter](#)) which explores likely scenarios and use cases for neurodata, including in health, employment and education, and seeks to examine the critical challenges they raise for privacy.

## UPDATES FROM THE EDPB

The [new chair](#) of the EDPB, Anu Talus, said at the beginning of July that the EDPB's focus is shifting from providing guidance to "legal analysis of concrete cases", i.e. enforcement. As an example of its focus on enforcement, the EDPB has already adopted a [template complaint form](#) for the submission of complaints and the subsequent handling of complaints by DPAs in cross-border cases, and a [template acknowledgement](#). These aim to facilitate the cross-border

exchange of information regarding complaints between DPAs and will help DPAs save time and resolve cross-border cases more efficiently alongside the new GDPR Procedural Regulation, discussed above.

The EDPB has also recently published the final version of its [Guidelines](#) on the calculation of administrative fines, which provide a five-step methodology for DPAs setting administrative fines (including suggested percentage ranges for calculation starting-points). We discuss key takeaways from the guidelines in our recent [blog](#).

Finally, the EDPB has published the final version of its guidance on the [Right of access](#), following consultation on the draft last year. While these guidelines are not binding on organisations in the UK, they provide useful detailed guidance on the scope of the right of access and the notion of manifestly unfounded or excessive requests, with the EDPB confirming that “these concepts have to be interpreted narrowly, as the principles of transparency and cost-free data subjects rights must not be undermined”. In particular, the EDPB confirms that a request should not be considered excessive on the ground that “the data subject intends to use the data to file further claims against the controller”.

## ICO ENFORCEMENT OVERVIEW

### TikTok fined £12.7m for children’s privacy breaches

The ICO has issued its final [monetary penalty notice](#) against TikTok, with the £12.7 million penalty representing an over a 50% reduction from the £27 million fine proposed in the ICO’s September 2022 notice of intention. The ICO’s press release explains that this reduction was due (in part at least) to the ICO deciding not to pursue its provisional findings in relation to the platform’s unlawful processing of special category data. Instead, the ICO’s final penalty notice focuses on TikTok’s non-compliance with core GDPR compliance requirements of lawful basis, transparency and fairness. In particular, the ICO found that TikTok had provided its services to UK children under the age of 13 and processed their personal data without consent or authorisation from their parents or carers; failed to provide proper information to people using the platform about how their data is processed in a way that is easy to understand; and failed to ensure that the personal data belonging to its UK users was processed lawfully, fairly and in a transparent manner. TikTok have confirmed that they are appealing. We discuss useful learnings for organisations from the fine in our [blog](#).

### ICO penalties remain under scrutiny from appeals

In a continuation of the trend of major fines being almost inevitably being subject to appeal (as discussed in our previous newsletters), we have seen a number of high-profile ICO enforcement decisions being appealed, to both the First Tier Tribunal and higher courts. DSG Retail is seeking permission to bring a second appeal against the £250,000 fine received after their appeal in the First-Tier Tribunal (FTT) (covered in more detail in our [November 2022 article](#)). The company is arguing that the lower court made an error in defining personal data, and that as the individuals could not be identified by the breached data, it is out of scope of data protection legislation. Meanwhile, the ICO has [confirmed](#) it has gained permission to appeal against the decision of the FTT in relation to its fine against Experian (which we discussed in our March [newsletter](#)) which was mostly, but not wholly, overturned by the FTT. TikTok has also confirmed that it will appeal against the ICO’s penalty (discussed above).

In the context of an appeal process, in March, the ICO reached a settlement [agreement with Easylife](#) that was approved by the FTT. The ICO agreed to reduce the £1.35 million fine issued against the company in October 2022, for unlawful processing of special category data, to £250,000. In a press statement on the agreement, the Information Commissioner emphasised the ICO’s position as a “pragmatic and proportionate regulator” and explained that the reduction was appropriate given Easylife had stopped their unlawful processing of special category data. We examine the reasoning behind the ICO’s original penalty against Easylife this [blog](#).

## EU GDPR ENFORCEMENT OVERVIEW

The table below sets out a selection of the most substantial EU GDPR fines brought by EU 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
IMY (Sweden)	Tele2 and CDON	12.3 million SEK (€1.2 million)	30 June 2023	Data security, international transfers
CNIL (France)	Criteo	€40 million	15 June 2023	Legal basis, transparency, data subjects' rights
IMY (Sweden)	Spotify	58 million SEK (€4.9 million)	12 June 2023	Data subjects' rights
DPC (Ireland)	Meta IE	€1.2 billion	22 May 2023	International transfers
AZOP (Croatia)	B2 Kapital	€2.2 million	2 May 2023	Data security, transparency, processor terms
CNIL (France)	Clearview AI	€5.2 million	13 April 2023	Legal basis, transparency, data subjects' rights
Garante (Italy)	TIM	€7.6 million	13 April 2023	Direct marketing, data subjects' rights, transparency

### EU enforcement focus on EU-US data transfers

Meta has been [fined](#) a record €1.2 billion by the Irish DPA for unlawful transfers of personal data to the US relating to its Facebook service. The Irish DPA's final enforcement decision reflected a binding decision from the EDPB, after the case was escalated to the EDPB via the GDPR's Article 65 dispute resolution procedure. Key aspects of the final decision are: (i) Meta was ordered to suspend its future transfers of personal data to the US, within a period of five months of the decision; (ii) Meta was ordered to pay a fine of €1.2 billion, with the fine level set with reference to the 'assessments and determinations included in the EDPB binding decision'; and (iii) Meta was ordered to bring its processing operations into line with the GDPR's transfer rules, by ceasing its unlawful processing in the US, including data storage, within 5 months of the decision. We published our initial thoughts on the Meta decision in this [blog](#). However, the impact of the Irish DPA's decision on Meta's business model has now been mitigated by the adoption of the DPF (discussed above and in our [blog here](#)).

The Swedish DPA has also recently brought enforcement action for unlawful international transfers as it [has fined](#) telecommunications company Tele2 12 million SEK (€1 million) and ecommerce site CDON 300,000 SEK (€25,357) for transfers made via Google Analytics. Two other companies, retailer Coop and newspaper Dagens Industri, were reprimanded. These are the first such monetary penalties to be imposed on companies following the series of 101 complaints about Google Analytics issued by NOYB (see this previous [newsletter issue](#)). As with Meta's transfers, this issue is likely to be rectified by reliance on the DPF going forward.

## VIEWS FROM... CHINA AND HONG KONG

### Regulatory developments on cross-border data transfers in the People's Republic of China and Hong Kong

*Contributed by Wynne Mok, Partner and Jason Cheng, Associate, Slaughter and May, Hong Kong*

#### People's Republic of China

The last 18 months have seen some major developments in the regulation of cross-border transfer of personal data in the People's Republic of China (PRC). Under the current legal framework<sup>1</sup>, data processors in the PRC (which have a role similar to data controllers under the UK GDPR) can only transfer personal data outside of China through one of three main routes:

<sup>1</sup> Regulated mainly by the Data Security Law (DSL) and Personal Information Protection Law (PIPL), both of which came into force in 2021.

- (i) undergo a certification process by a professional institution in accordance with the regulations of the Cyberspace Administration of China (CAC);
- (ii) obtain a CAC security assessment; or
- (iii) sign a standard contract with the overseas data recipient in the specified form published by the CAC.

The Chinese government has been gradually rolling out more guidelines for the implementation of the regulatory regime, setting out the detailed requirements of each of the three main routes. In particular, it has issued the Cybersecurity Practices Guideline relating to the Safety Certification Specification for Cross-Border Processing of Personal Information to govern the certification process and the Measures on State Security Assessment of Cross-Border Data Transfer in relation to the CAC's security assessment.

More recently, the CAC released the long-awaited final version of the *Standard Contract* for the third route, which is accompanied by two further guidelines in relation to its use - namely the *Measures for the Standard Contract for Outbound Cross-border Transfer of Personal Information* and the *Guidelines for the Filing of Standard Contracts for Cross-border Transfer of Personal Information*. It is now clear that the third route is not available if the data transferor is a critical information infrastructure operator which handles data in relation to important industries and fields (such as informational networks, infrastructure, natural resources, etc.) or if it processes personal data of more than 100,000 individuals or the sensitive personal data of more than 10,000 individuals<sup>2</sup>.

The guidelines also provide that a data processor which signs the Standard Contract must conduct a Personal Information Protection Impact Assessment (PIPIA) and file a PIPIA report and the Standard Contract with the local CAC office within 10 working days of signing the Standard Contract. In this regard, the Beijing CAC office has, on 2 June 2023, released an additional guidance to clarify how a companies should make filings in different situations. It is expected that other local CAC offices will release further guidelines on the formalities and procedures for the requisite filings.

### **Hong Kong**

As far as Hong Kong Special Administrative Region is concerned, whilst the proposed legislative provision on cross-border transfer of personal data (i.e. section 33 of the Personal Data (Privacy) Ordinance (PDPO)) has not yet come into force, the Privacy Commissioner for Personal Data (PCPD) considers it to be a best practice to comply with the provision. Indeed, it has recently issued a [Guidance Note on the Recommended Model Contractual Clauses for Cross-Border Transfers of Personal Data](#) introducing two sets of Recommended Model Contractual Clauses (RMCs) which can be incorporated in commercial agreements involving cross-border data transfers to comply with the requirements under section 33. The adoption of the RMCs is not a mandatory requirement. However, the PCPD would take into account any failure to comply with its best practice recommendations if the relevant data user is investigated for infringements of the PDPO, including in relation to the data protection principles.

## **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 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.

<sup>2</sup> Such a data processor will need to apply for a security assessment in order to transfer data out of the PRC.

## 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: [Is cookie enforcement crumbling? No, the ICO warns](#); [In for a penny: Data protection and privacy implications of the Bank of England's digital pound proposals](#); and [Generative AI - Three golden rules](#).

## 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)

582165458