

## 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](#)[VIEW FROM ...  
AUSTRALIA](#)[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 past few months have been turbulent ones with political and economic upheaval bringing uncertainty for individuals and businesses. From a data privacy perspective, this environment has affected the course of the long promised post-Brexit reforms to the UK's data privacy regime. The UK Government's Data Protection and Digital Information Bill (DPDI Bill) stalled in light of the Conservative leadership change in September. However, the latest indications from DCMS are that we may yet see progress (initially in the form of another consultation) before the end of the year.

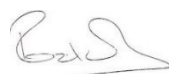
This autumn has also seen significant, and welcome, developments in relation to international data transfers. President Biden has signed an Executive Order laying the groundwork for a new EU-US data transfer framework (and an equivalent UK-US adequacy assessment). Meanwhile, the ICO has indicated that it will publish its final guidance on TRAs later this autumn, which will provide further clarity for organisations in this challenging area.

As a reminder of the GDPR's full force, European DPA's have continued to bring multimillion-Euro fines against tech giants this year - including Google, Meta and most recently, Instagram. Notably, Instagram was [fined €405m](#) by the Irish DPC for failing to protect children's privacy rights. This is also an area of focus for the UK's ICO, as evidenced by its [announcement](#) of a provisional fine of £27m for TikTok for possible infringements of children's privacy.

The UK and EU regulators have also brought a number of substantial enforcement actions against corporates for more basic GDPR compliance failings - for example, the ICO has [publicly reprimanded](#) organisations for non-compliance with DSARs and the Berlin DPA has issued a €525,000 penalty to a retailer for failures in connection with the GDPR's data protection officer requirements. While regulators are clearly looking far beyond data security in their enforcement, the recent [ICO enforcement](#) against Interserve following its cyber-attack is a reminder for organisations of the ongoing importance of maintaining focus on data security risks.

We will be considering these developments and the outlook for data privacy in more detail at our annual Data Privacy Forum, taking place on 6 December. We really hope you can join us but, if you have any questions before the Forum or you would like to discuss any current developments, please do give me a call.

On behalf of our Data Privacy team, I wish you a very happy festive season.



Rob Sumroy, Partner

## LEGAL UPDATES

### UK's data privacy reform - another consultation before the end of the year?

As mentioned above (and in [our blog post](#)), the government paused the second reading of the [DPDI Bill](#) on 5 September, to “allow ministers to further consider the legislation”. On 31 October, Owen Rowland, Deputy Director for domestic data protection policy at the Department for Digital, Culture, Media and Sport (DCMS), confirmed at a conference that a further consultation will be launched into the DPDI Bill “in the coming weeks”. He has also said that data adequacy with the EU is at the heart of the approach being taken going forward, which will be reassuring to many organisations.

### Progress on EU-US and UK-US data transfers

In a significant development towards restoring seamless transatlantic data flows, on 7 October US President Biden [signed](#) an Executive Order outlining the steps the US will take to implement its commitments under the EU-US data adequacy agreement in principle (the Data Privacy Framework or DPF) [announced in March](#). The Executive Order places additional “necessary and proportionate” limitations and layers of oversight on the US intelligence services’ access to personal data and establishes an impartial and independent redress mechanism (including a newly formed “Data Protection Review Court”) to investigate and resolve complaints regarding data access by those services. In light of the Executive Order, the EU Commission is now working on a draft adequacy decision for the US and launching its adoption procedure, in a process likely to take a few months.

Also on 7 October, the UK’s DCMS published an [explanatory note](#) reporting progress on the adequacy assessments between the UK and US - with the UK welcoming the US Executive Order and preparing for the laying of adequacy regulations, with respect to the US, before Parliament in early 2023. We discuss this further in our [blog post](#).

## CASE LAW UPDATE

### AG's opinion on non-material damages may limit GDPR claims in the EU

On the EU side, following a referral to the CJEU by the Austrian Supreme Court (in the *Österreichische Post* case mentioned in our [previous newsletter](#)) about the scope of the right to compensation under the EU GDPR, an [Attorney General's opinion](#) has endorsed a restrictive approach to non-material damages, resembling the decision in the UK’s *Lloyd v Google* case. The AG rejected the suggestion that the GDPR gives a right to compensation for any GDPR breach, such as one giving rise to a loss of control data, without damage actually being suffered by the data subject. He also suggested that compensation should only be available for genuine non-material damage and not for mere ‘annoyance or upset’ for the data subject, with the distinction between the two being left to Member States to decipher in light of prevailing social attitudes at the time. The CJEU may well adopt the position endorsed by the AG, potentially significantly narrowing the scope for data protection claims in Europe.

## REGULATOR GUIDANCE

### KEY REGULATOR GUIDANCE

#### ICO

|  |                |
|--|----------------|
| <a href="#">ICO consultation on draft employment practices guidance: information about workers' health (consultation closes on 26 January 2023)</a>                  | October 2022   |
| <a href="#">ICO consultation on the draft employment practices: monitoring at work guidance and draft impact assessment (consultation closes on 11 January 2023)</a> | October 2022   |
| <a href="#">Guidance on direct marketing using electronic mail</a>   | October 2022   |
| <a href="#">Guidance on direct marketing using live calls</a>  | October 2022   |
| <a href="#">ICO call for views: Anonymisation, pseudonymisation and privacy enhancing technologies guidance (consultation closes on 31 December 2022)</a>            | September 2022 |

## KEY REGULATOR GUIDANCE

### European Data Protection Board (EDPB) / EU Commission

|  |                |
|--|----------------|
| <a href="#">Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority (consultation closes on 2 December 2022)</a> | October 2022   |
| <a href="#">Guidelines 9/2022 on personal data breach notification under GDPR (consultation closes on 29 November 2022)</a>                      | October 2022   |
| <a href="#">Open letter on EDPB budget proposal for 2023</a>   | September 2022 |

## UPDATES FROM THE ICO

### ICO finalises guidance on direct marketing

In October, the ICO published new detailed guidance on [direct marketing using live calls](#) and [direct marketing using electronic mail](#). This latest guidance follows the ICO's consultation on its [draft direct marketing code of practice](#) that took place in 2020 (discussed in our [January 2020 newsletter](#)). However, this latest guidance has not, so far, been given the status of a statutory code of practice under the Data Protection Act 2018 (despite indications from the ICO's [draft Annual Action Plan](#) that it intends to update its direct marketing statutory code this year) and has been published with little fanfare.

The new guidance on direct marketing using electronic mail retains much of the content (including examples) from the 2020 draft code of practice but now distinguishes between the different status of recommendations within the guidance. It specifies that 'must' is used to indicate a legal requirement, whereas 'should' indicates good practice recommendations that ought to be complied with unless there is a reason not to, with 'could' indicating options controllers may want to consider. Given the ICO is continuing to issue fines in relation to breaches of the rules on direct marketing (as discussed in our [briefing](#)), this user-friendly approach will be welcomed by organisations.

### ICO consultation on new draft employment guidance

The ICO is producing new topic-specific guidance on employment practices and data protection. The new guidance follows the ICO's [call for views](#) on the topic in 2021, with the responses informing the ICO's work in developing the new guidance. So far, the ICO has published new guidance on [monitoring at work](#) and an accompanying [impact assessment](#), and guidance covering [workers' health data](#). The ICO intends to add to these resources over time as it develops the new guidance further. The ICO's iterative approach to this topic is similar to the approach it is adopting in relation to its new anonymisation guidance (discussed below).

The ICO is also working on [new guidance](#) on the use of biometric technology, such as facial and fingerprint analysis, key stroke analysis and voice recognition (with relevance within the employment context and more widely) to be published in Spring 2023. The regulator has specifically warned that organisations should assess the risks of using emotion analysis technologies ahead of implementing such systems, given the risk of systemic bias and discrimination they pose and has published [two reports](#) to support businesses engaging with the use of biometrics.

### ICO publishes new PETs guidance

As discussed in our [previous newsletter](#), the ICO has been publishing its new anonymisation guidance a chapter at a time for consultation. As part of this approach, in September the regulator [published](#) draft guidance on privacy-enhancing technologies (PETs) that explains the benefits and different types of PETs currently available, as well as how they can help organisations to comply with data protection law. The PETs guidance was published ahead of a G7 meeting of data protection authorities in Bonn, Germany, with the ICO advocating for international agreement and support for the responsible and innovative use of PETs. The closing date for the whole [consultation](#) is now 31 December 2022. We discuss the PETs guidance in more detail in our [blog post](#).

## UPDATES FROM THE EDPB

### EDPB consults on updates to existing guidance on data breach notification and lead authorities

The EDPB [has opened](#) a consultation on the first post-GDPR update to its 2018 data breach notification guidelines (discussed in our [July 2018 newsletter](#)), relating to the data breach reporting obligations of non-EU established organisations. The consultation relates to a single paragraph change to the existing guidelines (helpfully highlighted in the consultation text) which outlines that the presence of an EU representative is not sufficient to trigger the one-stop-shop mechanism. The new guidelines require that the breach must be reported to the DPA in every Member State with affected data subjects. If confirmed in the final version, this change is likely to implement a more arduous breach reporting obligation for companies based outside the EU (including those in the UK) but caught by the GDPR.

The EDPB has also published a [specific update](#) to its guidance on identifying a controller or processor's lead supervisory authority to clarify that joint controllers cannot designate a common main establishment for both joint controllers.

## ICO ENFORCEMENT OVERVIEW

### Interserve fined following cyber attack

On 24 October the ICO [announced](#) that it had fined construction company Interserve Group Limited £4.4 million for data security failings after a cyber-attack in spring 2020 enabled hackers to gain access to the records of 113,000 current and former employees. In a statement, the Information Commissioner suggested that “complacency” was to blame (although this was disputed by the company). The Commissioner warned other organisations to monitor systems for suspicious activity, act on warnings, update software and train staff or risk facing a similar fine. We outline important lessons from the decision on how the ICO expects organisations to handle cyber and data risk in [our briefing](#) and [our Lens blog](#).

### Action taken against organisations for data subject access failures

The ICO has [taken action](#) by issuing public reprimands to seven organisations, six public sector and one private, for failing to comply with data subject access requests (DSARs) in accordance with the UK GDPR. These public statements represent a new approach from the ICO to deter non-compliance with the GDPR, and especially in respect to DSARs. We discuss this action and the ICO's new approach further in our [Lens blog](#).

### Catalogue retailer EasyLife fined for “invisible processing”

EasyLife Limited has been [fined](#) £1.35 million by the ICO for using the purchase history of its customers to predict their medical conditions and then market health-related products to them based on those predicted conditions. The ICO concluded that EasyLife was profiling its customers and processing their special category data without a legal basis and without adequate transparency - which the ICO deemed “invisible processing”. We discuss this fine and its implications for controllers processing special category data in our [Lens Blog](#). EasyLife was also fined £130,000 for making over 1.3 million phone calls to those on the Telephone Preference Service in breach of direct marketing rules.

### Cabinet Office fine reduced by 90%

The ICO [has agreed](#) to reduce the £500,000 penalty it imposed on the Cabinet Office for the 2019 New Year Honours data breach (discussed in our [Lens blog](#)) to £50,000. The Information Commissioner has indicated that the reduction is in line with the ICO's [updated approach to public sector enforcement](#) (discussed in our [July newsletter](#)). The First Tier Tribunal has approved the settlement, with the planned appeal hearing on 4 November now vacated.

## EU GDPR ENFORCEMENT OVERVIEW

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

| DPA (Country) | Company                          | Amount                         | Date      | Description                                 |
|---------------|----------------------------------|--------------------------------|-----------|---|
| CNIL (France) | <a href="#">Clearview AI</a>     | €20 million                    | 20-Oct-22 | Lack of lawful basis, data subjects' rights |
| Berlin DPA    | <a href="#">Unknown retailer</a> | €525,000                       | 20-Sep-22 | Data protection officer requirements        |
| CNIL (France) | <a href="#">Infogreffe</a>       | £250,000                       | 13-Sep-22 | Retention periods and data security         |
| DPC (Ireland) | <a href="#">Instagram</a>        | €405 million                   | 02-Sep-22 | Children's privacy                          |
| CNIL (France) | <a href="#">Accor</a>            | £600,000                       | 17-Aug-22 | Data subjects' rights                       |
| CNIL (France) | <a href="#">Criteo</a>           | €60 million - provisional fine | 05-Aug-22 | Lack of lawful basis                        |

Recent EU DPA actions continue the trend of big-ticket fines for tech-giants but also include a number of substantial actions for a range of GDPR breaches by non-tech focused corporates:

- the Irish DPA has issued a **€405 million fine** against Instagram (owned by Meta) for breaching children's privacy rights, by enabling children to set up business accounts and setting children's accounts to 'public by default', in the second biggest GDPR fine to date. The fine followed the intervention of the EDPB after the other DPAs concerned failed to reach a consensus with the Irish DPA in relation to the enforcement action (we discussed the importance of the Article 65 procedure in our [November 2021 newsletter](#)). Meta had filed an appeal against the fine in the Irish High Court.
- the French DPA has ordered hotel chain Accor SA to pay a **€600,000 fine** for GDPR failures relating to the right of access and the right to object to processing for direct marketing. The fine amount was set following the involvement of the EDPB under the Article 65 procedure, with the EDPB determining that CNIL must increase its proposed fine from €100,000 to €600,000.
- The Berlin DPA has issued a **fine of €525,000** to the subsidiary of a Berlin-based retail group for non-compliance with the GDPR's DPO requirements. A conflict of interest was held to have arisen in breach of the EU GDPR's requirements, as the DPO had been responsible for the data processing activities of companies of which they were also the managing director.

## VIEW FROM... AUSTRALIA

*Australia's first significant data breach triggers rapid legislative response, contributed by Melissa Fai (Partner) and Dal Lim (Lawyer), Gilbert + Tobin*

### Background

In September 2022, Australia's second-largest telecommunications provider, Optus, revealed that it had been affected by a data breach compromising the information of around 9.8 million current and former customers (to put in context, that comprises approximately 38% of Australia's population). As Australia's largest (known) data breach to date, the data breach has been heavily scrutinised, triggering widespread public debate about how data, privacy and cybersecurity are handled in Australia, and the ability of the Privacy Act 1988 (Cth) (Privacy Act) in its current form to adequately protect individuals. This has prompted the (recently elected) Australian Federal Government to hastily amend telecommunications regulations and expedite some long-awaited reforms to the penalty regime of the Privacy Act. Further regulatory reforms to Australia's privacy regime are likely to follow (albeit already on the cards as part of a larger reform process initiated more than two years ago).

Described by Optus as a cyberattack, a threat actor was able to access an improperly secured Optus system and steal substantial amounts of personal information, including names, addresses, dates of birth, and government identifiers such as driver licence numbers and passport numbers. Widespread public concern and questions were raised over Optus' (and all businesses in general) data collection and retention policies - many questioned why Optus was holding government identifiers for years, even for former customers. The data breach has also highlighted that individuals currently have no ability to bring actions (including class actions) directly against entities that have breached the Australian Privacy Principles under the Privacy Act, nor is there any clearly recognised tort of invasion of privacy or similar remedy available under the common law.

### **Regulatory reforms: key aspects**

Responding directly to the Optus attack and the large-scale threat of identity theft, fraud and scams, the Government amended the Telecommunications Regulation 2021 on 12 October 2022 to allow telecommunications companies to temporarily share customer information with third parties. A remedial measure intended to be in place for 12 months, this amendment allows Optus to coordinate with financial institutions and government agencies to detect and prevent the fraudulent use of their data. Although necessary to protect Optus customers, this temporary reform has limited long term impact on Australia's data privacy regime.

The Optus attack also took place against the backdrop of the ongoing general review and potential reform of the Privacy Act. The review, which was announced in 2019, aimed to investigate the effectiveness of Australia's current data protection regime (the Review). In response to the Optus data breach, the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (the Bill) was tabled in Parliament on 26 October 2022 and is the first legislation that has been tabled in Parliament in connection with the Review.

### **The Bill covers four key objectives:**

- to significantly increase penalties for serious or repeated breaches of the Australian Privacy Principles, raising the penalties for body corporates from a maximum of AU\$2.22 million to the greater of: (i) AU\$50 million; and (ii) three times the value of the benefit obtained from the contravention or, if the value of the benefit cannot be ascertained, 30% of the adjusted turnover in the relevant period;
- to give the Office of the Australian Information Commissioner (OAIC) enhanced powers to request information and conduct compliance assessments of the notifiable data breach regime;
- to give the OAIC new enforcement powers, including allowing the OAIC to require entities to conduct external reviews of their internal procedures and to publish notices about specific privacy breaches to affected individuals; and
- to introduce new information sharing powers for the OAIC and the Australian Communications and Media Authority (ACMA) (the regulator that oversees telecommunications providers).

Additionally, the Privacy Act's extraterritorial application will be broadened if the Bill is passed. The Bill requires entities who are established outside of Australia to meet the obligations of the Privacy Act if they "carry on business" in Australia (as is currently the case), however, it proposes to remove the current requirement in the Privacy Act for such entities to collect or hold personal information in Australia in order for the Privacy Act to apply.

### **Implications for businesses and consumers**

The Optus data breach is clearly a catalyst for major scrutiny and reform of Australia's privacy regime, and the Bill is likely just the beginning of ongoing and anticipated reform. However, given that the OAIC has, to date, only sought to impose a penalty under the Privacy Act on one occasion (in relation to the Cambridge Analytica breach, with the relevant proceedings still ongoing), and in the context of the OAIC's relatively small budget and the fact that it is required to pursue any penalties through the Federal Court, it remains to be seen what difference increased penalties will actually make in preventing data breaches and protecting consumers from the consequences. As a result of the Optus data breach, it is likely that tougher legislative requirements will be imposed on how long data may be retained and how much data an entity may collect, as well as potentially more prescriptive requirements in relation to security, as part of broader reforms to the Privacy Act.

## 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 Data Privacy Knowledge  
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)