

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...](#)[AUSTRALIA](#)[THE LENS](#)


EDITORIAL

Reflecting on the months since our summer newsletter, it does feel very much like we have started the first term of a new academic year in data privacy. The new Government has now delivered us their Data (Use and Access) (Data) Bill (discussed below and in this [blog](#)). While much of the Data Bill is familiar to us and takes forward elements of the previous Government's Data Protection and Digital Information (DPDI) Bill, some aspects of the old Bill have been dropped (notably the proposed governance changes and 'vexatious' test in connection with DSARs), and the focus changed. The Data Bill's public and private sector data sharing provisions are now very much the Government's emphasis - so our curriculum is certainly developing.

One of our key topics of focus this autumn has been on marketing and cookies, reflecting the ICO and EU regulators' continuing focus on this area (discussed below) and the escalating risk-profile of marketing given the uplift in penalties to GDPR levels coming in the new Data Bill. Over a series of roundtables earlier in the autumn, we shared experience and insights with clients from a large range of sectors on this topic. We were encouraged by the collaborative relationships and solutions some privacy teams are developing with marketing colleagues to deliver on the (sometimes-competing) objectives of both teams.

Data and cyber breaches have been continuing to keep our teams busy too. The ICO's latest [Annual Report](#) indicates that breach reports to the regulator have risen nearly a third (28%) on the previous year, so we certainly are not alone. In particular, we have been seeing first-hand the extensive impact of supply chain incidents and the importance of having appropriate contractual protections to address such risks. These issues are also becoming an increasing focus for regulators in the UK and EU - with the first provisional fine from the ICO against a processor (discussed below) and new guidance from the EDPB on controller's responsibilities in respect of their processors (see below).

We are now busy preparing for our annual Data Privacy Forum Academy and we certainly have plenty of material to discuss! We look forward to seeing many of you (or your teams) then. In the meantime, if you would like to discuss any of these developments or any other data privacy issues, do please get in touch.



Rebecca Cousin, Partner

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

LEGAL UPDATES

Data (Use and Access) Bill

On 23 October, the Government introduced the [Data \(Use and Access\) Bill](#) (Data Bill) to Parliament. As discussed above, the Data Bill takes forward a number of aspects of the DPDI Bill, including in relation to Smart Data and Digital ID schemes. The changes the Data Bill proposes to make to the UK data protection regime are more modest than its predecessor's, for example, the DPDI's changes to the GDPR's accountability regime and the introduction of a new 'vexatious' test for refusing or charging for DSARs have been dropped. However, provisions modernising the structure of the ICO and giving the regulator enhanced enforcement and fining powers are being taken forward. Notably these include aligning the fining regime under the Privacy of Electronic Communications Regulations (PECR) with the UK GDPR, so penalties for marketing infringements could attract fines of up to £17.5m / 4% annual turnover. We discuss the Data Bill in more detail in our [Lens blog](#).

Public consultation on new EU standard contractual clauses (SCCs)

The European Commission has [announced](#) its intention to hold a public consultation on proposals for a new set of SCCs to specifically cover data transfers to controllers and processors in third countries which are already subject to the EU GDPR via the regulation's extraterritorial scope. This new set of SCCs would complement the existing EU SCCs published in June 2021 (discussed in our [briefing](#)). The Commission is targeting the second quarter of 2025 for the adoption of the new SCCs. In the UK, the ICO has indicated, in its [newly published list](#) of upcoming guidance, that it plans to issue updates to its existing international transfers guidance in the winter of 2024.

CASE LAW UPDATE

High Court considers international transfer rules

The UK High Court has provided helpful guidance on the interpretation of the UK GDPR's international transfer provisions, in the recent case of [JSC Commercial Bank Privatbank v Kolomoisky & Ors](#). The decision concerns an application for permission to disclose UK court documents in response to a request from a Ukrainian court, in the context of an Ukrainian criminal investigation. In interpreting the UK GDPR's international transfer provisions, the High Court closely aligns its approach with ICO guidance. In particular, it suggests that organisations should first consider if appropriate safeguards can be used before relying on the Article 49 derogations. The court also helpfully examines what it means for a transfer to be 'necessary' in the context of Article 49, holding that to be necessary transfers must be a "targeted and proportionate way of achieving the specific purpose" rather than "absolutely essential". The decision also suggests it may be possible for private organisations to make use of the 'public interest' derogation, although avoids giving a final view on the matter.

Upper Tribunal delivers judgment in DSG appeal

The Upper Tribunal has issued its [judgment](#) in the long-running DSG Retail (DSG) case, holding that the First-tier Tribunal (FTT) was incorrect in its interpretation of the meaning of personal data in the context of a data breach. The judgment stems from the ICO's [£500,000 fine](#) issued to DSG in 2020 in relation to a major data breach. The FTT reduced the fine to £250,000 on [appeal](#) in July 2022 (see our [article](#)), but DSG chose to further appeal that decision. Whereas the FTT had focused on whether the data was personal data in the hands of the controller, the Upper Tribunal held the focus should be on whether the data was personal data in the hands of the hackers. This decision could have significant implications for the definition of personal data and the status of pseudonymised (rather than anonymous) information, as it potentially reduces the scope of information that needs to be protected from security risks under the data protection regime. Following the Upper Tribunal's decision, the case is due to be remitted to the FTT to be re-decided. However, the ICO [has now confirmed](#) it has applied to the Upper Tribunal to further appeal the decision, given the significance of the case. The ICO has also recently applied to the Upper Tribunal to appeal against the FTT's decision in the Clearview case (discussed in our [blog](#)), following the FTT's rejection of the ICO's appeal request in September.

Update from the CJEU

In a non-binding opinion in [case C-203/22](#), an EU Advocate General has indicated that under the GDPR's right of access and rules on automated decision making, data subjects must be given concise and easy to understand information about automated decisions which enables them to exercise their rights under the GDPR. However, crucially, this does not require disclosure of the algorithm used, as it would be too complex for a normal person, without technical expertise, to understand. The opinion, whilst non-binding will be welcome news to those developing commercially sensitive algorithms.

In [case C-621/22](#) the CJEU has established that an organisation's pure commercial interest can be considered a valid basis for processing under the legitimate interests ground provided that a strict balancing test is met. This decision has been reflected by the EDPB in its new draft guidance on legitimate interests, discussed [below](#).

REGULATOR GUIDANCE

KEY REGULATOR GUIDANCE	
ICO	
Communicating with empathy after a data breach	October 2024
New data protection audit framework	October 2024
Generative AI consultation series: Allocating controllership across the generative AI supply chain (Consultation closed on 18 September 2024)	August 2024
EDPB	
Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive (Final version)	October 2024
Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (Consultation ends on 20 November 2024)	October 2024
Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s)	October 2024
EDPB to work together with European Commission to develop guidance on interplay between GDPR and DMA	September 2024

ICO announces call for views on genAI controllership

The ICO has issued its final [call for evidence](#) on generative AI (genAI), this time focusing on the topic of controllership within the genAI supply chain. The ICO accepts that understanding controllership in genAI supply chains can be difficult, as the controller / processor division does not always neatly map onto the roles of 'developers' and 'deployers'. Helpfully, the ICO includes several examples and options to help organisations determine what role they may be performing in different processing activities. We discuss this latest call for evidence further in our [blog](#).

EDPB issues new opinion on obligations relating to processors and sub-processors

Following a request from the Danish Data Protection Authority (DPA), the EDPB has issued an opinion ([22/2024](#)) on the duties of controllers that rely on processors. The opinion addresses eight questions on the scope of controllers' duties and places significant new obligations on both controllers and processors. For example, the opinion outlines that:

- controllers must retain information on the identity of all their processors and sub-processors, including name, address and contact person. Processors should provide and update this information.

- ultimate responsibility for engaging sub-processors remains with the controller, but processors should ensure they put forward sub-processors providing ‘sufficient guarantees’. Controllers can rely on information received from processors but may need to build on the information where it is lacking.
- controllers are always obliged to verify whether processors/sub-processors provide ‘sufficient guarantees’ but the extent of such verification can vary according to the risks posed. Similar obligations are placed on controllers in respect of international transfers by their processors.

The opinion also considers certain aspects of processing contracts, including wording governing processing required by law. While the EDPB’s one-size fits all approach may be difficult for many organisations to comply with in practice, certainly initially, these new recommendations are likely to influence market practice over time, in the EU and UK. For example, they may increase the depth and quality of information provided by processors to controllers for due diligence. We discuss the opinion further in this [blog](#). It should be noted however, that the EDPB’s power to issue such opinions (under GDPR Article 64(2)) is currently [being challenged](#) in the EU General Court by Meta, as part of the tech company’s response to the EDPB’s opinion on pay or consent models (discussed in our [previous newsletter](#)).

New guidance on legitimate interests published by EDPB for consultation

The EDPB has published [new guidance](#) on legitimate interests for consultation. The guidance emphasises and analyses the three elements that must all be fulfilled by a controller in order to rely on the legitimate interests legal basis. These are: (i) the controller or a third party must be pursuing a legitimate interest; (ii) the processing of personal data must be necessary for the purposes of pursuing the legitimate interest; and (iii) the interests or fundamental freedoms and rights of individuals do not take precedence over the legitimate interest(s) of the controller or the third party (balancing exercise). The guidance looks at each of these aspects in turn and emphasises the stringent nature of the assessment. It further explains how the assessment should be carried out in a number of specific contexts, including fraud prevention and direct marketing. The EDPB have also reflected, within the guidance, the recent CJEU ruling in Case C-621/22, discussed [above](#).

ICO ENFORCEMENT OVERVIEW

Advanced Computer Software handed £6 million provisional fine by ICO

The ICO has issued its first [provisional fine](#) for breaches of the GDPR by a data processor. Advanced Computer Software Group Ltd (Advanced) was given the £6 million provisional fine following an August 2022 data breach which impacted the NHS 111 service and the personal data of over 80,000 patients. The breach was caused after a malicious actor was able to access a customer account which was not protected by multi-factor authentication. We discuss the provisional fine and the key takeaways for organisations in our recent [blog](#).

ICO extends focus on cookies to adtech

The ICO is continuing to focus on cookie compliance (as we discussed in our [March newsletter](#)) and is now also looking at the adtech industry more broadly. In October, the regulator issued a public reprimand to Sky Betting and Gambling in connection with its cookie practices (discussed in our [blog](#)). In its [statement](#) publicising the reprimand, the ICO confirmed that it is currently investigating a number of data management platforms, as part of the regulator’s “strategy to ensure people’s rights are upheld in the online advertising industry”. At the recent ICO Data Protection Practitioners’ Conference, the Commissioner also said that adtech is one of the ICO’s top-three current areas of focus.

EU GDPR 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 three months, along with an indication of the principal areas of non-compliance addressed by each enforcement action.

DPA (Country)	Company	Amount	Date	Description
DPC (Ireland)	LinkedIn	€310 million	24 October 2024	Lawfulness, fairness, transparency
DPC (Ireland)	Meta	€91 million	27 September 2024	Data security
AP (Netherlands)	Clearview AI	€30.5 million	3 September 2024	Lawfulness, transparency, individuals' rights,
IMY (Sweden)	Apoteket AB	SEK37 million (€3.3 million)	29 August 2024	Data security
AP (Netherlands) and CNIL (France)	Uber	€290 million	22 July 2024	International transfers

LinkedIn issued €310 million fine by Irish DPA for personalised ads

On 22 October 2024, the Irish DPA issued a €310 million [fine](#) to LinkedIn Ireland Unlimited Company (LinkedIn) following an investigation into LinkedIn's advertising practices triggered by complaints received in 2018 from French non-profit La Quadrature Du Net. The Irish DPA found that LinkedIn's processing of personal data for behavioural analysis and targeted advertising was in breach of the principles of lawfulness, fairness and transparency. Microsoft, the owner of LinkedIn, is considering an appeal. In the meantime, LinkedIn is required to bring its data processing into compliance within three months.

Dutch DPA and CNIL announce joint fine of €290 million on Uber

The Dutch and French DPAs have issued Uber with a €290 million [fine](#) for failing to implement appropriate safeguards when transferring driver data, including special category data, to the United States over a two year period. The breach stemmed from complaints made to the French DPA by 170 drivers in France through a human rights organisation. The French DPA subsequently transferred the complaint to the Dutch DPA as lead supervisory authority, but the two authorities continued to collaborate. Uber's failure came in the period between the invalidation of the Privacy Shield and the implementation of the new EU-US Data Privacy Framework, during which they did not have applicable standard contractual clauses in place. Uber is expected to appeal the decision.

VIEW FROM... AUSTRALIA

Contributed by Cheng Lim, Partner, King & Wood Mallesons

Recent developments in privacy litigation in Australia

Against a backdrop of significant data breaches, the landscape for data privacy claims in Australia has been developing in recent years and upcoming regulatory changes may further facilitate individual and group claims.

Current position: class actions, representative complaints and regulatory action

Currently, individuals in Australia do not have a direct right of action for an interference with their privacy under the Privacy Act 1988 (Privacy Act). Instead, they must complain to the Office of the Australian Information Commissioner (OAIC) who can then order compensation for the interference. However, this order is only enforceable through the Federal Court which examines the privacy breach afresh, making this a potentially lengthy and cumbersome process.

Despite these regulatory hurdles, recent significant data breaches in Australia have given rise to a range of complex privacy enforcement actions and litigation. For example, following Medibank's 2022 data breach which impacted 9.7 million individuals in Australia, it is facing a number of actions including:

- for breach of contractual provisions on compliance with the Privacy Act, breach of consumer law and misuse of confidence;
- a class action by Medibank's shareholders in relation to the diminution of the company's share value; and

- a representative action before the OAIC, despite the challenges of enforcing an OAIC order as mentioned above.

In addition, the OAIC has instigated enforcement proceedings against Medibank, with the company facing a potential penalty of up to \$2.2 trillion. While questions remain around OAIC's approach to this action, it demonstrates a new zeal from the regulator and coincides with an increase in its regulatory investigations into data breaches (for example against [HWL Ebsworth](#) and [Optus](#)) and its civil penalty claims (including against [Meta](#) and [Australian Clinical Labs](#)).

Outlook: legislative reform

Two areas of proposed legislative reform look to expand the ability of individuals to bring privacy claims against organisations and may therefore lead to an increase in claims.

New tort for serious invasions of privacy

In September, the Australian Government introduced the long-awaited Privacy Bill amending the Privacy Act. While the Bill does not go as far as some had hoped, it did propose a new tort for serious invasions of privacy. The tort is not limited to data privacy and regulates a broad range of privacy harms, including physical intrusions into an individual's private space. To successfully prove a serious invasion of their privacy - and gain access to a broad range of remedies - plaintiffs must show that:

- there was a privacy invasion;
- there was a reasonable expectation of privacy when the invasion occurred;
- the invasion was serious; and
- the invasion was intentional or reckless.

The requirement for intent or recklessness may exclude many claims relating to data breaches or cyber-attacks involving third parties as it is unlikely organisations will intentionally leave their systems vulnerable. However, claims for other 'invasions' such as monitoring or surveillance or otherwise using personal data without transparency and permission could potentially be made under the new tort. Successful claimants will be able to seek a range of remedies including damages, injunctions and apology orders.

A new direct right of action

The creation of a direct right of action has been agreed in principle by the Australian Government but not included in the recent Privacy Bill. If included in future legislation it would allow individuals that have suffered loss or damage resulting from an interference with their privacy to bring a claim directly in court. This would likely result in a further increase in the popularity of class action cases relating to both cyber incidents and breaches of privacy law more broadly. It is yet to be seen whether this right, though agreed to in principle, will be in fact be introduced.

Conclusion

The new tort introduced in the Privacy Bill is expected to become law in the first half of 2025, whilst the timing of the proposed direct right of action is somewhat more uncertain given it is not included in the Bill. The progress of the various actions against Medibank are also worth monitoring given the potential precedents they will set in privacy litigation regardless of the proposed reforms mentioned above. Everything therefore points towards a future increase in privacy litigation in Australia, and so organisations should reassess their privacy risks against this backdrop.

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: [Are you ready for NIS2 - new EU cyber law applies from 18 October](#); [The EU Data Act - one year to go: what you need to know to prepare](#); [Revolutionising Regulation: The UK's New Innovation Office Takes Centre Stage](#)

CONTACT



ROB SUMROY
PARTNER
T: +44 (0)20 7090 4032
E: rob.sumroy@slaughterandmay.com



REBECCA COUSIN
PARTNER
T: +44 (0)20 7090 3049
E: rebecca.cousin@slaughterandmay.com



RICHARD JEENS
PARTNER
T: +44 (0)20 7090 5281
E: richard.jeens@slaughterandmay.com



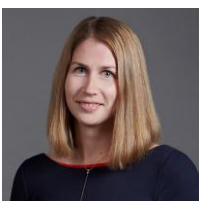
DUNCAN BLAIKIE
PARTNER
T: +44 (0)20 7090 4275
E: duncan.blaikie@slaughterandmay.com



JORDAN ELLISON (BRUSSELS)
PARTNER
T: +32 (0)2 737 9414
E: jordan.ellison@slaughterandmay.com



WYNNE MOK (HONG KONG)
PARTNER
T: +852 2901 7201
E: wynne.mok@slaughterandmay.com



CINDY KNOTT
PSL COUNSEL AND HEAD OF DATA PRIVACY
KNOWLEDGE
T: +44 (0)20 7090 5168
E: cindy.knott@slaughterandmay.com



BRYONY BACON
SENIOR PSL, DATA PRIVACY
T: +44 (0)20 7090 3512
E: bryony.bacon@slaughterandmay.com

London
T +44 (0)20 7600 1200
F +44 (0)20 7090 5000

Brussels
T +32 (0)2 737 94 00
F +32 (0)2 737 94 01

Hong Kong
T +852 2521 0551
F +852 2845 2125

Beijing
T +86 10 5965 0600
F +86 10 5965 0650

Published to provide general information and not as legal advice. © Slaughter and May, 2023.
For further information, please speak to your usual Slaughter and May contact.

www.slaughterandmay.com