DATA PRIVACY NEWSLETTER

SELECTED LEGAL AND REGULATORY DEVELOPMENTS IN DATA PRIVACY

QUICK LINKS

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

EDITORIAL

Welcome to the March edition of our Data Privacy Newsletter.

I am writing this editorial after a particularly rainy few weeks in the UK but the sun is now shining, and the brighter evenings are a sign that spring is almost here. The data privacy landscape is also seeing renewal, with the EU looking to make significant changes to the EU GDPR regime with its Digital Omnibus simplification proposals. The Omnibus may be seen as timely pruning of a digital regime that has rapidly expanded, but the main structure of the GDPR rules will largely remain intact (see this blog). Concerns about the proposals, particularly on changes to the definition of personal data, are growing in volume so there is no guarantee the exact proposals introduced by the Commission will make it through the EU legislative process to become law. We discuss the EDPB/EDPS response below. The UK's DP refresh is further along, with the main data protection changes in the Data (Use and Access) Act 2025 now in effect.

At our DP Forum client event in December, we asked our audience of privacy professionals what approach they were taking to these legislative updates. Over half are looking to track mandatory changes only at this stage. Legislators will be hoping that organisations go further and take advantage of the relaxations to innovate, and 21% of our attendees suggested their organisations will be looking to do so.

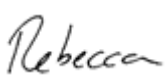
Another key theme from the last few months is regulatory overlap. The data protection regime and the work of data protection regulators is increasingly intertwining with others operating in the same neck of the woods. For example, the ICO has launched an investigation into X and Grok AI's personal data use, with Ofcom also looking at the platform from the online safety perspective. Meanwhile, the Russmedia case in the CJEU (discussed below) has confirmed the obligations of online platforms to take down content under the GDPR's rules.

We are also seeing regulators' focus on children's data crystalise, with the ICO issuing fines totalling nearly £15 million for children's data failings in February. Meanwhile, Ofcom has confirmed that it may fine more for infringements of children's data than other failings under the Online Safety Act (see this blog).

Against this backdrop, we are delighted to be working closely with Slaughter and May's new dedicated Digital Regulation practice to offer joined-up pragmatic advice across these evolving areas.

If you have any questions on these developments (or others), we would be delighted to discuss over coffee.

Regards,



Rebecca Cousin, Head of Data Privacy

LEGAL UPDATES

Data (Use and Access) Act 2025

Three new statutory instruments have been made (on 15 December 2025, 15 January and 29 January), which have brought into force nearly all the remaining provisions of the Data (Use and Access) Act 2025 (DUA Act). Changes brought into force include the majority of the DUA Act's data protection changes, including the relaxation of rules around automated decision making and cookies, and the increase in the Information Commissioner's Office's (ICO) enforcement powers (discussed further in this blog). Notably, the requirement for controllers to introduce a complaints procedure has not yet been brought into force. This requirement is expected to come into force in June 2026, one year after the DUA Act became law.

EU GDPR reform ongoing

The European Commission's Digital Omnibus Package, launched on 19 November 2025, included a number of proposals which aim to "harmonise, clarify and simplify GDPR provisions, without affecting the core principles". The proposed liberalisations include relaxations to the current data breach notification regime, amendments to the definition of personal data, a new exemption to data subject access requests (DSARs), and a clarification to allow legitimate interest to be relied on for processing personal data in the context of AI development and operation. For further analysis, see this blog.

In November, the Council of the European Union also adopted the GDPR Procedural Regulation rules to improve the efficiency of GDPR enforcement in cross-border cases (as discussed in our previous newsletter). The new rules will apply from 2 April 2027.

EU adequacy update

In December 2025, the European Commission renewed the two EU adequacy decisions for the UK (under the GDPR and the Law Enforcement Directive) which underpin the free-flow of personal data between the two territories. The Commission had previously extended the decisions on a six-month basis to 27 December 2025 in order to assess the DUA Act's impact. The renewed decisions will run until 27 December 2031, with the possibility for further renewal then.

Early this year, the European Commission also adopted mutual adequacy decisions with Brazil, allowing for the free exchange of data between the two. Meanwhile, the EU's adequacy finding for the US faces ongoing scrutiny, with the Court of Justice of the European Union (CJEU) recently accepting French MP Philippe Latombe's appeal against the dismissal of his challenge against the EU-US Data Privacy Framework (discussed in our November newsletter).

CASE LAW UPDATES

UK data protection claims update

Recent months have seen progress in two significant data protection claims in the UK courts, which indicate the landscape is continuing to gradually evolve post-Lloyd v Google:

- Permission to appeal to the Supreme Court has been granted in the Farley & Ors v Paymaster case (discussed in this blog), in relation to the issue of compensation. As such, the Supreme Court is set to reevaluate issues surrounding the test for non-material damage under the UK GDPR and Data Protection Act 2018.
- In February, a judgment was handed down in the Neil Spurgeon & Ors v Capita PLC mass claims, relating to Capita's 2022-2023 data breach, in which the court sided with the claimants and refused to strike out the claims as an abuse of process. At issue were the procedures used by the claimants' solicitors to gather and document evidence of the distress suffered by the individual claimants, with the defendants suggesting they exaggerated damage allegedly suffered by "putting words into the claimants' mouths". While calling for some aspects of the pleadings to be revisited, the court acknowledged there were good reasons for the approach deployed and recognised that claimants' legal representatives have a 'wide latitude' in formulating pleadings. This decision highlights the high bar for such strike-out actions but ultimately does not amount to any validation of the underlying claims.

Court of Appeal sides with the ICO in DSG Retail case

In the latest instalment of the long running case relating to the ICO's 2020 fine against DSG for data security failings in connection with a major cyber-attack, the Court of Appeal has allowed the ICO's appeal against the Upper Tribunal's judgment (discussed in our previous newsletter here). The Court of Appeal's judgment has confirmed that where information is personal data for a controller, they are required take appropriate security measures to protect that information from attack, regardless of whether the information would be identifiable in the hands of a third-party attacker. The case will now return to the First-Tier Tribunal to be decided following the clarification of this point of law.

Updates from the CJEU

Marketing in the spotlight

In case C-654/23 relating to Inteligo Media, the publisher of a legal news publication, the CJEU has considered how the ePrivacy Directive and the "soft opt-in" under Article 13(2) apply to organisations that provide free products or services and has also provided new guidance on the interaction of the e-Privacy Directive with the GDPR.

The court found the definition of "direct marketing" under the e-Privacy Directive applied to a free daily newsletter sent by Inteligio to their users, which included links to paid-for content. The court concluded that a newsletter having an informative purpose did not preclude it from being "marketing" and also that while the wording of the soft opt-in requires a "sale", this encompasses indirect payment (e.g. where a free service is provided to advertise a paid service). However, the CJEU emphasised that the soft opt-in must be interpreted strictly, so it is likely that not all free services will be able to benefit.

In a finding with wider relevance, the court determined that there is no need to establish a GDPR lawful basis for the sending of marketing where the soft opt-in is available under the e-Privacy Directive. It should be noted though, that this question was only dealt with briefly in the decision and may best be interpreted narrowly, i.e. as disapplying the requirement for a lawful basis for the sending of marketing only rather than for the wider processing of the data connected with it.

Clarification of platform obligations

What responsibilities does the GDPR place on online platforms for advertisements uploaded by third parties? This question was addressed by the recent Russmedia case C-492/23. Russmedia operates an online platform where third parties upload advertisements. At issue in the case was an advertisement falsely presenting the claimant as providing sexual services which included photographs and a phone number for her, used without her consent. The CJEU found that Russmedia was a joint controller of the personal data in the advertisement. Central to this decision was the fact that Russmedia's marketplace terms and conditions permitted the platform provider to use, distribute, modify, and remove published content at its own discretion, meaning it exerted the necessary influence over the processing of personal data for its own purposes.

The CJEU also ruled that such joint controllers must, before the publication of such advertisements, use appropriate technical and organisational measures to identify advertisements that contain sensitive data and then verify whether the advertiser is the person whose sensitive data appears in the advertisement. If not, the controller should refuse publication unless the advertiser can demonstrate explicit consent has been obtained. In addition, such controllers must implement appropriate security measures to prevent sensitive data being unlawfully copied to other websites. In an era of increasing online safety and platform regulation, this case is an important reminder of the continuing importance and operational impact of the GDPR.

REGULATOR GUIDANCE

KEY REGULATOR GUIDANCE	
ICO	
How to deal with data protection complaints (updated guidance)	12 February 2026
ICO updates data protection by design guidance	5 February 2026
ICO framework for handling data protection complaints	4 February 2026
ICO update to government on economic growth commitments	2 February 2026
Guidance on international transfers (updated guidance)	15 January 2026
ICO tech futures: Agentic AI	8 January 2026
Right of access (updated guidance)	8 December 2026
Children's Code Strategy progress update	1 December 2026
EDPB / EDPS	
EDPB-EDPS Joint opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus)	11 February 2026
Report on International Data Protection Enforcement Cooperation	2 February 2026
EU-US Data Privacy Framework FAQ for European individuals - version 2.0	23 January 2026
EDPB-EDPS Joint opinion 1/2026 on the Proposal for a Regulation as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)	21 January 2026
Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites (consultation ended on 12 February 2026)	4 December 2025
Guidance for Risk Management of Artificial Intelligence systems	11 November 2026

UPDATES FROM THE ICO

ICO updates guidance on international transfers and data subject access requests

In the last few months, the ICO has published updates to its detailed guidance on DSARs and international transfers. The DSAR guidance tracks changes brought in by the DUA Act which offer new operational flexibilities - for example, confirming that controllers can 'stop the clock' where clarification is reasonably required. However, the guidance also reflects recent case law in relation to increased transparency requirements, confirming that controllers must disclose specific recipients in supplemental information (as decided in Harrison v Cameron and ACL). We discuss the key takeaways in our blog.

The updated international transfers guidance has been timed to address changes made by the DUA Act, but also provides new content to clarify previous areas of uncertainty. For example, it clarifies rules around onwards transfers and offers substantial new guidance on complying with 'other' UK GDPR rules (outside Chapter V) in the context of transfers. We discuss the key aspects of this guidance in this blog.

ICO publishes its Tech Futures report on agentic AI

The ICO has published the latest report in its Tech Futures series on the topic of agentic AI. While not formal guidance, the report is a useful indication of the ICO's current thinking on this emerging technology. For example, it reflects on how agentic AI poses unique privacy risks, including in relation to determining controller and processor responsibilities, relying on automated decision-making and introducing new types of security risks. Whilst reminding organisations that they remain responsible for the compliance of agentic AI they develop or deploy, the ICO encourages a compliant exploration of these tools. Read more in our blog.

ICO cookie and innovation updates

The ICO has recently confirmed that its regulatory focus on cookie compliance has brought over 95% of the top 1,000 websites in the UK in line with compliance standards. Of the 979 websites who passed, 564 did so as a result of direct engagement with the ICO (we discuss ICO's cookie focus in more detail in this article).

The ICO is also committed to the promotion of innovation and competition (a duty now codified under the DUA Act), including in how it regulates cookies. The regulator recently updated the Government on its economic growth agenda, with the ICO continuing work to support a shift to privacy-preserving advertising via the introduction of new exceptions to the cookie consent requirements (discussed further in this blog).

UPDATES FROM THE EDPB/EDPS

EDPB and EDPS issue joint opinions on the European Commission's Omnibus proposals

Following the publication of the European Commission's Digital Omnibus regulatory simplification proposals in November (see this blog), which include amendments to the GDPR regime (discussed in this blog), the EDPB and EDPS have now issued a joint opinion on the proposed changes. They generally welcome the proposal's aim to simplify the digital rulebook, strengthen individuals' rights and boost EU competitiveness. However, they have mixed views on the changes proposed. For example, they welcome the suggested relaxations to the data breach reporting regime and the introduction of a new exception for processing special category data for biometric authentication. Conversely, they have significant concerns about the proposed narrowing of the definition of personal data, emphasising that this change goes 'far beyond a technical modification' and would adversely affect the fundamental right to data protection. In other cases, they support the underlying aim of the changes, but suggest modifications, including in relation the new exception for processing residual special category data for AI.

The regulators have also issued a joint opinion in response to the European Commission's Digital Omnibus on AI Regulation Proposal. Although the bodies express support for the Proposal's aim to reduce the administrative burden of the AI Act, they highlight elements that require further consideration and make recommendations to ensure individuals' rights are protected.

ICO ENFORCEMENT OVERVIEW

ICO maintains focus on cyber breaches

ICO enforcement activity towards the end of 2025 continued to focus on cyber security and shows that the ICO is willing to deploy the full range of its regulatory powers in this area:

- Password manager LastPass UK Ltd was fined £1.2 million, in connection with a data breach that impacted the personal data of up to 1.6 million UK users. Insufficient security measures were found to have allowed a threat actor to gain access to the company's backup database.
- Post Office Limited was issued a reprimand following a data breach that resulted in the names, addresses and postmaster status of 502 people who were part of a group litigation against the organisation being leaked. Had the public sector approach not been in place, the ICO would have issued a fine of £1.094 million in relation to the incident.
- The ICO announced the launch of a cross-border investigation into the Prospect data breach, that impacted 160,000 trade union members, in collaboration with the DPAs of Jersey, Guernsey, and the Isle of Man.

We will be exploring the key takeaways from the ICO's recent enforcement actions in an upcoming client publication.

ICO enforcement in the context of online safety

The ICO's long-running focus on children's privacy in an online context has come to fruition in the last month, with a suite of announcements:

- on 3 February, following a public statement in January, the ICO opened a formal investigation into X Internet Unlimited Company and X.AI LLC following reports of the Grok artificial intelligence system being used to generate non-consensual sexual imagery of individuals, including children;
- on 5 February, the ICO fined MediaLab.AI Inc, owner of image hosting platform Imgur, £247,590 for children's privacy failures; and
- on 24 February, the ICO announced a £14.47 million fine for Reddit, Inc, also for children's privacy failings. This is the ICO's highest fine in nearly three years. Reddit has already confirmed it is appealing against the penalty.

These fines form part of the ICO's work under its Children's code strategy to drive improvements in how digital platforms use children's personal data. Both fines focused on age assurance and data protection impact assessment failings, amongst others. We discuss these developments in more detail in this blog.

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

DPA (Country)	Company	Amount	Date	Description
AEPD (Spain)	Aena (country's main airport operator)	€10,043,00	6 November 2025	• Biometric data • DPIA
CNIL (France)	Free Mobile and Free	€42 million	13 January 2026	• Data security
CNIL (France)	Unnamed French company	€3.5 million	30 December 2025	• Lawful basis • Transparency • Data security
CNIL (France)	Nexpublica France	€1.7 million	22 December 2025	• Data security
CNIL (France)	Travail	€5 million	22 December 2025	• Data security
AZOP (Croatia)	Telecommunications operator	€4.5 million	14 November 2025	• International transfers • Lawful basis • Data processors

VIEW FROM… VIETNAM

With input from Jonathan Lin (Partner) and Tu Do (Senior Associate), Allen & Gledhill, Vietnam.

Vietnam's new Personal Data Protection Law No. 91/2025/QH15 was passed by the National Assembly on 26 June 2025 and entered into force on 1 January 2026 ("**PDPL**"). To provide further guidance on this Law, the Vietnam Government passed Decree 356/2025/ND-CP on 31 December 2025, which also entered into force on 1 January 2026 ("**PDPD**"). The

PDPL and PDPD unify data privacy regulations previously dispersed across different laws, most significantly in Decree No. 13/2023/ND-CP ("Decree 13"). While the new laws mostly maintain the approach taken to data protection under the previous legal regime, they introduce a number of important changes and clarifications:

Application to international organisations. While both Decree 13 and the PDPL apply broadly to Vietnamese and international agencies, organisations, and individuals engaged in personal data processing, the PDPL expressly captures those involved in processing data of both Vietnamese citizens and persons of Vietnamese origin whose nationality has not been determined but who reside in Vietnam and have been issued identity certifications.

Data de-identification, encryption, and decryption. The PDPL introduces the new concepts of "de-identification of personal data" and "encryption and decryption of personal data". Personal data de-identification refers to the process of altering or deleting information so as to produce data that cannot be used to identify, or assist in identifying, a specific individual. Personal data encryption refers to the process by which "data is converted into an unreadable format without decryption". In this regard, the PDPL provides that while de-identified personal data will no longer be regarded as personal data, encrypted personal data continues to be categorised as personal data, akin to the GDPR concept of pseudonymised data.

Consent. The PDPL maintains the consent-centric model utilised in Decree 13 but tightens it by providing that consent for the processing of personal data must be voluntary, informed, and specific to each processing purpose. It explicitly prohibits bundling unrelated services with consent. The PDPL introduces a new lawful basis for personal data processing without consent, stipulating that this is possible where it is necessary to protect the "the life, health, honour, dignity, and legitimate rights and benefits of the personal data subject" or to "respond to emergencies or threats to national security". Such thresholds appear to be considerably higher than the "legitimate interests" threshold under the EU GDPR which permits a broader balancing of organisational needs against data subject rights. The PDPD further prescribes requirements as to the method and manner in which consent is to be obtained. In particular, consent must be obtained in a manner that evidences the grant of consent by the data subject and the time at which such consent was granted.

Cross-border transfer impact assessment. A data overseas-transfer impact assessment (OTIA) must be prepared and submitted within 60 days of the initiation of the cross-border transfer. Similar to Decree 13, the requirement to prepare and submit the OTIA is separate and distinct from the requirement to prepare and submit a data protection impact assessment. However, certain exemptions to the OTIA requirement apply, such as where the transfer is initiated by the data subject or where employee data is stored in the cloud. The OTIA dossier must be prepared in the prescribed forms as set out under the PDPD.

Permitted data transfers. The PDPL specifies the circumstances in which the transfer of personal data is permitted. However, the PDPL expressly provides that the transfers of personal data in the prescribed circumstances will not be regarded as the sale and purchase of personal data, regardless of whether the transfers involve payments. The PDPD sets out further requirements for the transfer of personal data, including that the parties must enter into contract (with certain prescribed terms) for the transfer of personal data in certain prescribed cases and that the data must be de-identified before being transacted on data exchanges. There is a degree of ambiguity in these provisions, and it remains unclear whether the list of permitted transfers is intended to allow certain transfers (e.g. arising due to a merger) even where the consent of the data subject has not been obtained. The Vietnam Government is expected to provide further guidance on these provisions.

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 blog posts include: The EU Data Act in practice: Key recent developments; Commission makes preliminary finding that TikTok's "addictive design" breaches the DSA; and Lessons in online safety: Ofcom's £1 million fine against AVS and end of year review.

CONTACT

REBECCA COUSIN
HEAD OF PRIVACY
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

JASON CHENG (HONG KONG)
COUNSEL
T: +852 2901 7211
E: jason.cheng@slaughterandmay.com

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

BRYONY BACON
SENIOR KNOWLEDGE LAWYER
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