SLAUGHTER AND MAY/

DATA PRIVACY NEWSLETTER

NOVEMBER 2025
ISSUE 29

DATA PRIVACY

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

As we edge toward Christmas, we reflect on a busy year (with still more developments expected!) and start looking ahead at what 2026 is likely to bring. The Information Commissioner's enforcement action against Capita—arriving on the back of a broader run of cyber and data security penalties—serves as timely confirmation that the regulator's pragmatic and pro innovation stance does not dilute its expectations around security. There are some valuable learnings for organisations here, not least a reminder that the most harmful incidents very often arise from well-known, preventable weaknesses.

In parallel, there continues to be a much-needed focus on AI, with regulators in the UK, the EU and beyond continuing to refine their approaches to the interaction between AI and data privacy. Across consultations, guidance and supervisory coordination, the trend line is becoming clear: AI deployments—especially those using personal data with sensitive attributes or in high stakes contexts such as employment, credit and public services—will be scrutinised for lawful bases, fairness, explainability and meaningful human oversight. Having said that, we know from our discussions with you that there are still many challenges with the deployment and continued use of AI tools within your businesses (and now with agentic AI on the near horizon) so the need for consistent and practical guidance across sectors remains.

Looking beyond AI, the EU is doubling down on digital regulation with increasing focus both on enforcement (e.g. under the Digital Markets Act, as discussed in this blog) and simplification, even as the bloc's regulatory plans for data continue to reach fruition (the landmark Data Act became applicable in September, see this blog). From a data privacy perspective, there has been a focus on practical interoperability, with a number of joint consultations and regulatory guidance on the interplay between the various digital laws and the EU GDPR (as we discuss below).

The pathway to 2026 is also coming into focus. We are still waiting for the finalised provisions simplifying the EU GDPR, though the changes are limited. In the UK, more provisions of the Data (Use and Access) Act (DUA Act) are scheduled to come into force, and it is expected that we will see consultations and developments around 'smart' data sharing schemes in sectors across the economy, using powers from the DUA Act. We will also be watching whether 2026 brings a step up in AI and data privacy fines – there is certainly an argument that targeted enforcement will be critical to keep privacy risks in focus, including at board level.

We look forward to catching up with many of you in the run up to the holidays. For those we may miss, do keep in touch and let us know if we can help in any way.

Rebecca

Rebecca Cousin, Head of Data Privacy

LEGAL UPDATES

Data (Use and Access) Act 2025

Certain provisions of the Data (Use and Access) Act (DUA Act) have been brought into force under three statutory instruments made on 21st July, and 2nd and 4th September 2025. Current Government guidance indicates we can expect the remaining provisions to be brought into force next year, with two further sets of commencement regulations expected in or around January 2026 and June 2026. In relation to some of the key aspects of the DUA Act (which we discussed in our podcast):

- provisions which enable the development of sector-specific 'smart data' data sharing schemes came into force on 20 August 2025 (to the extent they were not already brought into force when the DUA Act was passed);
- the relaxation of the rules around the use of automated decision making and cookies is expected to come into force in January 2026;
- the increase in the enforcement powers of the Information Commissioners Office (ICO), which will enable it to issue higher (GDPR level) penalties for cookie and marketing infringements, is expected to come into force in January 2026; and
- new requirements relating to complaints procedures are expected to come into force in June 2026.

CASE LAW UPDATE

Upper Tribunal upholds ICO fine against facial-recognition database provider Clearview AI Inc

The Upper Tribunal (UT) has handed down its judgement in the ICO v Clearview case, upholding the ICO's appeal against the First Tier Tribunal (FTT) decision. In May 2022, the ICO fined Clearview £7.55 million for its use of images of UK residents collected from the internet to create a global online database that could be used for facial recognition. In October 2023, the FTT ruled that the ICO did not have jurisdiction over Clearview since its services were only used by non-UK/EU governments and their contractors, whose processing activities fall outside the scope of the EU and UK GDPRs (both the EU and UK GDPR were relevant as the processing in question overlapped the UK's EU exit). The UT held that the FTT had misapplied the law, finding that Clearview's processing of personal information is within the material and territorial scope of the EU and UK GDPRs (confirming a broad understanding of the 'behavioural monitoring' aspect of the GDPR's extraterritorial reach). The substantive issues of the appeal are still to be determined by the FTT and in any event the decision may yet be appealed, as we discuss in our recent blog.

Court of Appeal clarifies how individuals can claim for non-material damage following data breaches

In Farley & Ors v Paymaster, the Court of Appeal (CoA) clarified some important points on when and how individuals can claim for non-material damage. In particular, the CoA held that:

- the disclosure of personal data is not an essential ingredient of an infringement under DP Law. The High Court was therefore wrong to strike out the data protection claims on the basis that the misaddressed letters sent by the defendant had not been opened or read;
- as a point of principle, compensation for emotional responses other than distress can be recoverable under data protection law; and
- there is no threshold for "seriousness" under the UK GDPR and DPA.

However, the claimants still have to prove their factual allegations and so each of their cases (and any allegations of abuse of process) must now be assessed by the High Court (and potentially the County Court). Overall, this judgement should inform controllers' data privacy risk-assessments, especially when considering the possibility of a mass-scale breach. We discuss the judgement in this blog.

TikTok unsuccessful in its initial challenge of ICO fine for misusing children's data

In July 2025, the FTT ruled against TikTok in its preliminary appeal of the ICO's £12.7 million fine for data misuse, including for unlawfully processing children's data (the ICO's original 2023 fine against TikTok is discussed in this blog). The FTT rejected TikTok's argument that it was processing personal data for artistic purposes, which is one of

the "special purposes" where the ICO is required to seek the court's permission to take enforcement action. The FTT held that even if TikTok did process children's data for artistic purposes, it did not follow that its processing of the same data for other purposes, such as targeted advertising, fell within the remit of special purposes. TikTok now await a hearing at the UT, who have granted TikTok permission to appeal the FTT's judgement.

UPDATES FROM THE CJEU

In case C-413/23, the Court of Justice of the European Union (CJEU) found that pseudonymised data under Regulation (EU) 2018/1725, which sets the legal framework for the protection of personal data processed by European Union institutions (the Regulation), will not always constitute personal data. The Regulation is similar to, and therefore of interest in relation to the interpretation of, the EU GDPR. The European Data Protection Supervisor had previously found that the Single Resolution Board (SRB) had breached its obligations under the Regulation, when it transferred pseudonymised consultation responses to Deloitte. The General Court had annulled that decision in 2023 but on appeal, the CJEU confirmed that the relevant test was whether the data was 'reasonably likely' to enable Deloitte to identify the data subjects and concluded that it would not necessarily be personal data from Deloitte's perspective (we discuss the impact on the meaning of 'personal data' in the EU, in this blog). However, because it was personal data from SRB's perspective, the CJEU found that the SRB had breached its GDPR obligations by failing to provide transparency information about its data sharing with Deloitte, reinforcing the importance of privacy notices.

Pseudonymisation was also relevant in case T-384/20, where the General Court awarded a Greek Scientist damages after the European Anti-Fraud Office published her personal data in a press release that made it possible for readers to identify her. These recent EU judgements show the court taking an increasingly risk-based approach to considering whether pseudonymised data is personal data.

In case T-553/23, the General Court upheld the EU-US data privacy framework, dismissing the action for annulment brought by Phillipe Latombe, a French MP. Latombe had challenged the EU Commission's 2023 decision that the US offered an adequate level of protection for personal data, creating a framework for personal data to flow from the EU to the US without additional safeguards. Latombe has since confirmed he is appealing the decision. The Commission has also issued its provisional adequacy decision for the UK, which would see the renewal of its assessment of the UK as an adequate country for a further 6 years. The current UK-EU adequacy decision is due to expire on 27 December 2025.

In a non-binding opinion, a CJEU Advocate-General said controllers can refuse a data access request for being 'excessive' if they can demonstrate that the individuals making the request have abusive intentions. However, the burden of proof will be on data controllers to demonstrate that requests are 'excessive'. The frequency of the requests will not be sufficient to demonstrate the requisite intent. However, if, for example, an individual made a request for the sole purpose of 'provoking' an infringement of the GDPR and making a claim for damages, then this could demonstrate abusive intentions.

REGULATOR GUIDANCE

KEY REGULATOR GUIDANCE	
ICO	
Call for views on enforcement procedural guidance (consultation ends on 23 January 2026)	31 October 2025
Guidance on consent or pay (updated on 20 October 2025)	20 October 2025
Consultation on new electronic mail marketing rules for charities (consultation ends on 27 November 2025)	16 October 2025
Encryption guidance	2 September 2025

Consultation on draft guidance on Distributed Ledger Technologies (consultation ends on 7 November 2025)	28 August 2025
Consultation on draft complaints guidance for organisations (consultation ended on 19 October 2025)	21 August 2025
Consultation on recognised legitimate interest guidance (consultation ended on 30 October 2025)	13 August 2025
Consultation on guidance on profiling tools for online safety (consultation ended on 31 October 2025)	30 July 2025
Consultation on a new chapter within the draft updated guidance on storage and access technologies (consultation ended on 26 September 2025)	7 July 2025
Call for views on ICO's approach to regulating online advertising (consultation ended on 7 September 2025)	7 July 2025
EDPB / EDPS	
Guidance on Generative AI, strengthening data protection in a rapidly changing digital era	28 October 2025
Draft UK adequacy decisions: EDPB adopts opinions	16 October 2025
Coordinated Enforcement Framework: EDPB selects topic for 2026	14 October 2025
Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation (consultation ends on 4 December 2025)	9 October 2025
Human Oversight of Automated Decision-Making	23 September 2025
Guidelines 3/2025 on the interplay between the DSA and the GDPR (consultation ended on 31 October 2025)	12 September 2025
The Helsinki Statement on enhanced clarity, support and engagement	3 July 2025

UPDATES FROM THE ICO

ICO consults on draft guidance on Distributed Ledger Technologies

The ICO has published draft guidance for developers and users of distributed ledger technologies (DLTs). DLTs, such as blockchain, are technologies used to store, synchronise and maintain digital records across a network of computing centres. The guidance sets out good practice for those using DLTs, clarifying how GDPR principles apply, and the protection measures organisations are expected to implement when designing or using a blockchain solution. The consultation closes on 7 November 2025. Read more about this draft guidance in our blog.

ICO consults on draft complaints guidance for organisations

The ICO has published draft guidance for organisations handling data protection complaints. The guidance explains how organisations should comply with the new requirements introduced by the DUA Act to:

- give people a way of making data protection complaints;
- acknowledge receipt of complaints within 30 days of receiving them;

- without undue delay, take appropriate steps to respond to complaints, including making appropriate enquiries, and keep people informed; and
- without undue delay, tell people the outcome of their complaints.

These requirements are expected to come into force in June 2026. The consultation closed on 19 October 2025.

ICO consults on recognised legitimate interest guidance

The ICO has published draft guidance on the new lawful basis of "recognised legitimate interest" introduced under the DUA Act. A "*recognised legitimate interest*" is a specified purpose for handling personal information that is in the public interest. It is different and separate from the 'legitimate interests' lawful basis and includes five pre-approved purposes for processing personal data: for public task disclosures, defence reasons, emergency situations, stopping crime and safeguarding. The consultation closed on 30 October 2025.

UPDATES FROM THE EUROPEAN DATA PROTECTION BOARD (EDPB)

EDPB consults on guidelines on the interplay between DSA and GDPR

The EDPB has issued guidelines on the interplay between the Digital Services Act (DSA) and the GDPR. The DSA creates obligations for intermediary service providers to tackle illegal content, protect privacy rights and increase transparency on their online platforms. Many activities regulated by the DSA are also regulated by the GDPR as they involve the processing of personal data. For example, the DSA makes references to 'profiling' and 'special categories of data' as defined in the GDPR. The advice offers clarity around compliance with both sets of regulations and makes it clear that DSA wording should not be construed to override the principles of the GDPR. The consultation closed on 31 October 2025.

EDPB and European Commission issue joint guidelines for consultation on the interplay between the DMA and GDPR

These are the first joint guidelines published by the EDPB and the European Commission. As with the DSA guidelines discussed above, these guidelines aim to provide legal certainty where activities regulated by the Digital Markets Act (DMA) are also regulated by the GDPR, for example, around the meaning of consent. The consultation closes on 4th December 2025.

EDPB's Helsinki Statement

In July, the EDPB issued a statement on their plan to make GDPR compliance easier and strengthen consistency across guidelines. These initiatives focus on enhancing the GDPR's clarity and offering more support to, and engagement with, organisations. They include producing templates for organisations to use, harmonising EDPB and national application and enforcement guidance to promote consistency across EU data protection authorities and preparing joint guidelines with other regulators.

ICO ENFORCEMENT OVERVIEW

ICO fines Capita £14 million for data breach that affected over 6 million people

The ICO has fined Capita £14 million for failing to ensure the security of millions of individuals' personal data following a cyber-attack in March 2023. The attack resulted in hackers stealing the personal data of 6.6 million people, including staff and customers of organisations Capita supports. For some, this included sensitive information such as their criminal records, financial data and special category data. The ICO found that Capita had failed to adopt appropriate technical and organisational measures to effectively respond to the attack.

ICO fines care home director for ignoring a resident's subject access request

In September, the ICO prosecuted a care home director in Yorkshire for refusing to respond to a request for a resident's personal information in April 2023. The request was made by the resident's daughter who had the authority to make the request under a power of attorney. The Magistrates Court ordered the director to pay a £1,100 fine and additional costs of £5,440. For more insight into complying with DSARs, see our blog post here.

ICO issues a statement on the ongoing Imgur investigation

On 30 September, the ICO issued a statement in response to Imgur's decision to block access to UK users after the ICO issued a notice of intent to impose a fine on MediaLab, Imgur's parent company. In March 2025, the ICO announced that it was investigating the image hosting website for how it used UK children's personal information and implemented age assurance measures. The ICO clarified that the decision to restrict access in the UK does not mean Imgur can avoid responsibility for a previous breach and that the investigation remains ongoing. This investigation forms part of a wider intervention effort by the ICO as part of its Children's code strategy to assess how social media and video sharing platform's use children's data, including TikTok and Reddit.

ICO fines Birthlink £18,000 for destroying irreplaceable data

In July, the ICO fined Birthlink £18,000 after it destroyed approximately 4,800 personal records, up to ten percent of which may be irreplaceable. Birthlink, a Scottish charity who specialise in post-adoption support, destroyed physical documents including handwritten letters and photographs from birth parents without authorisation when faced with storage constraints in early 2021. Read more in our 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
AP (Dutch DPA)	Experian	€2.7million	16 October 2025	• Transparency • Lawful basis
Data Protection Ombudsman (Finland)	S-Bank	€1.8million	8 September 2025	• Data security
Andmekaitse Inspektsioon (Estonia)	Allium UPI	€3 million	5 September 2025	• Individual's rights • Lawful basis
Urzad Ochrony Danych Osobowych (Poland)	ING Bank Śląsk	€6.5 million	26 August 2025	• Lawful basis • Data minimisation

Dutch DPA fines Experian €2.7 million

The Dutch data protection authority (AP) has fined Experian €2.7 million for unlawfully processing personal data to generate credit reports without data subjects' consent. This involved collecting and selling information, including sensitive information, gleaned from public sources and purchased from telecom and energy companies. The AP found that such processing lacked a lawful basis, and that Experian had failed to comply with transparency requirements as people were unaware this data was being collected.

VIEW FROM… HONG KONG

Contributed by Jason Cheng (Counsel) and Kenny Lai (Associate), Slaughter and May, Hong Kong

Data protection in Hong Kong has long been governed by the Personal Data (Privacy) Ordinance (**PDPO**). For years, there was no dedicated legislation to address cybersecurity threats. In response to rising risks, particularly those fuelled by the rapid development of artificial intelligence, Hong Kong enacted its first cybersecurity law - the

Protection of Critical Infrastructures (Computer Systems) Ordinance (**PCICSO**) - on 19 March 2025. The PCICSO is set to come into effect on 1 January 2026.

The PCICSO aims to regulate designated Critical Infrastructure Operators (**CIOs**) in Hong Kong that operate essential infrastructure within one of the eight specified sectors[1], and/or any other infrastructure that plays a substantial role in maintaining critical societal or economic activities (such as major sports and performance venues).

The key obligations under the PCICSO for a CIO include, inter alia:

- maintaining a physical office in Hong Kong;
- notifying the regulating authority of any material changes to its critical infrastructure or computer system;
- establishing and maintaining a dedicated computer-system security management unit;
- developing and implementing a security management plan;
- conducting an annual computer-system security risk assessment;
- arranging for an independent computer-system security risk audit at least once every two years; and
- maintaining an emergency response plan for computer-system security incidents.

While the PCICSO primarily applies to designated CIOs and their computer systems, vendors, contractors and other service providers linked to CIOs may also be indirectly impacted, as CIOs are expected to uphold the same standards across their supply chain.

In recent years, data breaches have remained a key focus of investigations and enforcement by the Privacy Commissioner for Personal Data (**PCPD**)[2]. Although the PCPD has long advocated for a mandatory data breach notification regime, the PDPO currently imposes no statutory obligation to report such breaches. Notably, the PCICSO has introduced a mandatory notification requirement for computer-system security incidents. Once a CIO becomes aware of an incident affecting its critical infrastructure, it must notify the Commissioner as soon as practicable and within:

- 12 hours for any serious incident which has disrupted, is disrupting or is likely to disrupt the core function of the relevant critical infrastructure; or
- 48 hours for any other incident.

This new mandatory notification regime under the PCICSO may signal the potential introduction of similar requirements for data breaches under the PDPO in the foreseeable future.

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: Same Warnings. Same Threats. Bigger Consequences… Increase in highly and nationally significant cyber-attacks in 2025, NCSC announces; Can Brussels change? One year after Draghi – the EU's Digital Simplification Package; and UK and EU ramp up online safety enforcement: Ofcom issues first OSA fine as Commission probes child protection under DSA.

[1] The eight sectors are (1) energy, (2) information technology, (3) banking and financial services, (4) air transport, (5) land transport, (6) maritime transport, (7) healthcare services and (8) telecommunications and broadcasting services.

[2] All investigation reports published on the PCPD's website in 2025 are related to data breaches (see here).

CONTACT

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

REBECCA COUSIN
SENIOR CONSULTANT
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

JUSTIN CHAN (HONG KONG)
PARTNER
T: +852 2901 7208
E: justin.chan@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