SLAUGHTER AND MAY

July 2026

Data Privacy Newsletter

Issue: 31

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 summer issue of our Data Privacy Newsletter. Following the recent heatwave we have been left with no doubt that summer is really here. The last few weeks have also seen the regulatory temperature rising - for social media companies in particular. The announcement of the UK's social media ban for under-16s has been welcomed by many but leaves significant questions unanswered (as we discuss here). What is clear though, is that age assurance is going to be a cornerstone of any new ban, with even more focus set to fall on the privacy obligations that brings. Those are not the only privacy aspects of age assurance however, and we will shortly be publishing an article (and a podcast) focusing in on why age assurance may be needed for GDPR compliance even where the DSA/OSA doesn't apply, so do watch out for that.

Alongside action around age assurance (discussed further below), the ICO has continued to focus on children's privacy in recent months. This has included publishing new materials to support families with online privacy and a report on the ICO's engagement work with major edtech providers. This is interesting reading for anyone, like me, who has daily kitchen-table debates about their children's app-based maths homework... The ICO's own homework on children's privacy is continuing to be marked by the courts, with the Upper Tribunal hearing an appeal against the regulator's 2022 fine against TikTok on 11-12 May (we discussed the First Tier Tribunal's findings last year, here).

Cyber breaches have also been keeping our team busy over the last few months, as major incidents have seen significant fines issued in both the UK and EU (as we discuss below). Cyber risks are continuing to evolve, with regulators flagging the risks posed by AI-driven attacks (see the ICO's blog of advice on this) and internal AI vulnerabilities, and with the EDPS publishing new guidance on the risks posed by shadow-AI. We discuss the latest on the cyber landscape in this blog.

Next week, I am going to be in Cambridge for PL&B's annual conference to chair a session with Carolina Foglia from the EDPB. A number of our privacy and cyber team will also be attending and we are really looking forward to the event as an opportunity to catch up on all these topical issues with our fantastic privacy community. We hope to catch up with a number of you there.

If you have any questions on the developments we cover in this newsletter (or others), we would be delighted to discuss over coffee.

Rebecca Cousin, Head of Data Privacy

Legal updates

New complaints process requirements come into force

On 19 June 2026, new requirements for data protection complaints processes came into force from the Data (Use and Access) Act 2025 (DUA Act). Every controller is now required to have a process in place to facilitate data protection complaints, including to acknowledge any complaint made within 30 days and to investigate complaints without undue delay. We discuss the practical steps organisations need to take in light of this new requirement in this blog.

Case law updates

Court of Appeal overturns High Court decision in RTM v Bonne Terre

The Court of Appeal has confirmed, in RTM v Bonne Terre Limited, that consent to personalised marketing and data processing should be judged objectively. The Court of Appeal overturned the High Court's decision, which had endorsed a more subjective test for consent requiring consideration of the actual state of mind of the individual providing the consent. The High Court had determined that marketing consents provided by a gambling addict were not valid. Citing workability and legal certainty concerns, the Court of Appeal rejected this subjective test, stating that whilst knowledge of a data subject's particular vulnerability may be relevant to other compliance obligations such as fairness, it is not relevant to the consent test itself. This case has now been remitted to the High Court. We discuss the case further in this blog.

CJEU rules on abusive data subject access requests

In case C-526/24 (Brillen Rottler), the EU Court of Justice (CJEU) acknowledged the relevance of an individual's intention in relation to the validity of their data subject access request (DSAR). In particular, a first request by an individual for access to their personal data may be regarded as excessive and abusive under the GDPR, where the request is made with the intention of "artificially creating the conditions laid down for obtaining compensation under the GDPR". This case related to a DSAR from an individual that had systematically subscribed to the newsletters of various companies before making DSARs and claiming compensation. The controller was aware of this pattern of behaviour and had refused to comply with the individual's DSAR on the basis it was abusive. The CJEU decided that the data subject's history of submitting multiple DSARs to different controllers with a view to obtaining compensation was relevant in establishing such an abusive intention.

The CJEU also determined that an individual is only entitled to compensation if they can show that the alleged infringement of the GDPR has caused them damage, which will not be the case if the data subject's own conduct is the determining cause of the damage.

In the UK, the ICO has produced new guidance on AI-generated Freedom of Information Act (FOIA) requests. While the guidance is aimed at those organisations within scope of the FOIA regime, it has helpful read-across relevance for organisations' approach to AI-driven DSARs, which we examine in this blog.

Regulator guidance

ICO	
Guidance for consumer Internet of Things products and services (final version)	11 June 2026
New guidance to support public authorities dealing with AI-generated FOI requests	6 May 2026
Online tracking strategy update – April 2026	29 April 2026
Guidance on direct marketing using electronic mail (updated guidance)	28 April 2026
Guidance on the use of storage and access technologies (final version)	20 April 2026
Draft updated guidance on automated decision-making, including profiling (consultation closed on 29 May 2026)	31 March 2026
Guidance on the recognised legitimate interest lawful basis (final version)	23 March 2026
Guidance on purpose limitation (updated guidance)	23 March 2026
EDPB / EDPS	
EDPS blog: Managing shadow AI's hidden data breach risk	15 June 2026
EDPB personal data breach notification template (consultation ends on 5 August 2026)	10 June 2026
EDPS Annual Report 2025	7 May 2026
Guidelines 1/2026 on processing of personal data for scientific research purposes (consultation closed on 25 June 2026)	16 April 2026
EDPB DPIA template (consultation closed on 9 June 2026)	14 April 2026
EDPB Annual Report 2025	9 April 2026
CEF 2026: EDPB launches coordinated enforcement action on transparency and information obligations under the GDPR	19 March 2026

Updates from the ICO

ICO focuses on children's online privacy

Following on from the ICO's enforcement actions against Reddit and Imgur at the start of the year (discussed in our March newsletter), the ICO has continued to focus its efforts on promoting children's online safety in recent months. In March, the ICO issued a joint statement with Ofcom outlining the regulators' joint expectations in relation to age assurance (discussed in this blog) and also issued an open letter to social media platforms calling on them to strengthen their approach to age assurance. Since then, the ICO has reported that the responses it received from TikTok, Snapchat, Facebook, Instagram, YouTube and X show that, while some services are taking additional steps to protect children, more needs to be done. The ICO has said that it is now considering "next steps" and stands ready to use its "full range of regulatory powers" (discussed further in this blog).

ICO consultation on draft automated decision-making guidance

The ICO has published an updated version of its guidance on automated decision-making (ADM) and profiling for consultation. The guidance reflects the changes made to the UK GDPR's ADM regime by the DUA Act and developing policy positions from the ICO. Key updates to the guidance include more analysis on what amounts to a 'decision' and 'significance', for the purposes of determining whether the ADM rules apply. Notably, the new guidance appears to pave the way for a broader set of decisions and market sectors to fall within the rules (as we discuss in this blog). We expect the ICO's policy positions in the updated ADM guidance to feed through to the regulator's AI and ADM statutory code of practice that is expected later this year. Regulations requiring the ICO to produce this code were laid before Parliament in April and came into force on 12 May.

ICO online tracking updates

The ICO has continued progressing its online tracking strategy, to give people meaningful choice over how they are tracked online. Recent months have seen:

- the ICO publish the final version of its guidance on the use of storage and access technologies, following two consultations. The latest version largely retains earlier policy positions but with a few new clarifications. See our blog for further information.
- the ICO publish an update to its online tracking strategy, outlining the impact of its compliance focus and industry engagement efforts to date, with 99% of the UK's top 1000 websites having now passed the ICO's compliance checks and positive changes having been made by both consent management and data management platforms (see our blog).
- the ICO publish finalised guidance on consumer Internet of Things (IoT) products and services, following its consultation last year. This includes detailed guidance on the application of the Privacy and Electronic Communications Regulations 2003 (PECR) online tracking and marketing rules to IoT devices, such as how the consent rules apply.
- the ICO provide advice to the Government (outlined in this blog) on how the PECR rules could be amended to support contextual advertising.

The ICO has also published an updated version of its guidance on electronic mail marketing, reflecting the DUA Act's extension of the 'soft opt-in' exemption to charities.

For further discussion of recent developments and key trends in marketing compliance across the UK, EU and US, see our article.

Updates from the EDPB

EDPB publishes DPIA and data breach notification templates

Last year, in its Helsinki Statement, the EDPB said it would make GDPR compliance easier, particularly for small organisations. In line with this aim, reiterated in its 2026–2027 work programme, the EDPB has published two new templates, one for data protection impact assessments (DPIAs) and one for data breach notifications, to support GDPR compliance. The DPIA template includes pre-defined fields that prompt structured responses. It provides for a granular description and compliance analysis of the processing (including, for example, in relation to legal bases, minimisation, necessity and proportionality) and includes a detailed risk assessment and management framework. It is accompanied by an explainer document to support its use. The template is now due to be finalised by the EDPB (following the consultation that

closed on 9 June). Ultimately, all national data protection authorities (DPAs) are expected to adopt the template or to align their own templates with it.

The personal data breach notification template is designed to be implemented by DPAs via an IT tool, with the EDPB to set a timeline for its implementation once the public consultation on the draft closes on 5 August.

ICO enforcement overview

ICO fines South Staffordshire Water and Police Scotland for security breaches

The ICO has issued two significant fines for data security failings:

- On 7 May 2026, the ICO fined South Staffordshire Plc and South Staffordshire Water Plc a total of £963,900 in connection with a cyber-attack that began in September 2020. The attack originated from a phishing campaign and went undetected for nearly two years, during which time the threat actor gained access to the companies' IT environment. The incident resulted in approximately 4.1 terabytes of data being exfiltrated and published on the dark web, including personal data of around 633,887 data subjects. The ICO highlighted failures relating to account access controls, security monitoring and logging, obsolete software, and vulnerability management. South Staffordshire reached a voluntary settlement with the ICO and received a 40% penalty discount. It has agreed not to appeal. See this blog for more information.

- In a fine issued in December 2025 but announced in March, the ICO issued Police Scotland with a £66,000 penalty and formal reprimand following the unlawful processing and unauthorised disclosure of personal data extracted from the mobile phone of someone reporting an alleged crime. During the investigation, Police Scotland conducted a bulk download of the data subject's mobile phone data, including over 10,000 pages of images and text conversations unrelated to the investigation. The data was subsequently disclosed without redaction to a third party that should not have received it. The penalty was reduced by 50% under the ICO's public sector approach.

These cases illustrate the ICO's continued willingness to deploy enforcement action across both the private and public sectors, with data breaches (cyber and non-cyber) remaining a key area of concern. We provide further analysis of recent ICO enforcement trends and on the outlook for future enforcement action in this podcast.

EU GDPR enforcement overview

The table below sets out a selection of the most substantial EU GDPR fines brought by European 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)	Amadeus	€9 million	6 June 2026	Lawful basis
CNIL (France)	IQVIA	€5 million	26 May 2026	Data security
AP (Dutch DPA)	Yango	€100 million	8 May 2026	International data transfers
Garante (Italy)	Poste Italiane and Postepay	€12.5 million	20 April 2026	Lawful basis
Garante (Italy)	Intesa Sanpaolo	€31.8 million	30 March 2026	Data security

Garante (Italy)	Intesa Sanpaolo	€17.6 million	12 March 2026	Lawful basis

Dutch DPA fines Yango €100 million

On 8 May 2026, the Dutch DPA fined MLU B.V., the operators of the Yango taxi app, €100 million for unlawful transfers of personal data to Russia. An investigation by the Dutch, Norwegian and Finnish DPAs found that the app collected and stored a significant volume of personal data on servers located in Russia. The data stored was highly sensitive, including scans of driving licences, precise location data, chat conversations and social security numbers.

Italian DPA focuses on financial institutions

Q1 2026 has seen the Italian DPA issue significant fines to the country's financial institutions, for a range of GDPR failures. In March, the DPA fined Intesa Sanpaolo S.p.A. €17.6 million for unlawfully profiling approximately 2.4 million customers in the context of their transfer to Isybank, a newly established digital bank within the same corporate group. This fine was followed by a separate €31.8 million fine, relating to a data breach that occurred between February 2022 and April 2024 and involved the unauthorised access to 3,573 customers' personal data by one of Intesa Sanpaolo's own employees.

Then in April, the DPA fined the Italian postal, logistics and financial services company, Poste Italiane S.p.A., €6.6 million and its subsidiary, Postepay S.p.A., €5.9 million, for unlawfully processing the personal data of millions of users of their financial services apps. The apps required users to authorise monitoring of data on their mobile devices, which the companies argued was for the purpose of detecting malicious software and fraud prevention. The DPA found that the methods adopted were excessive and not strictly necessary for fraud prevention purposes. Poste Italiane is appealing against the penalties.

View from... Canada

Contributed by Wendy Mee, Partner, Blake, Cassels & Graydon LLP, Toronto

The Canadian federal government recently introduced two new bills that, if enacted, will modernise Canada's digital regulatory framework. Bill C-34, the Safe Social Media Act, aims to address online safety, and Bill C-36, An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts, aims to reform Canada's private-sector privacy legislation. Both bills build on prior proposals introduced by the federal government, with some key changes.

Bill C-34: Digital Safety Act

Bill C-34 introduces the Digital Safety Act, which creates a new federal regulatory regime to govern online content. It applies broadly to operators of "regulated services," which would include regulated social media platforms, regulated chatbot services, and regulated online services. Whether such service will be considered "regulated" is to be prescribed by future regulation.

The Digital Safety Act imposes transparency obligations and a general duty to protect children for all operators of regulated services. Additionally, operators of regulated social media services will be required to implement age-verification measures to prevent children under the age of 16 from having an account. Regulated social media services and regulated chatbot services will also be subject to a "duty to act responsibly" which, among other things, will require operators to mitigate against the risk that users may be exposed to harmful content and provide tools to users to flag harmful content.

Bill C-36: Protecting Privacy and Consumer Data Act

If enacted, Bill C-36 will repeal the privacy provisions of the federal Personal Information Protection and Electronic Documents Act (PIPEDA) and replace them with the new Protecting Privacy and Consumer Data Act (PPCDA). The PPCDA carries forward many of PIPEDA's core obligations, including the obligation to obtain consent for any processing of personal information (with limited exceptions), but creates new exceptions from the consent requirement, imposes new obligations with respect to privacy management programs, introduces new data subject rights (including with respect to data portability and automated decision systems), and creates stronger enforcement powers. Of note, the PPCDA will introduce a new legitimate business interest exception that will (subject to certain conditions) allow for the processing of personal information without consent.

Enforcement and Penalties

A new regulator, the Digital Safety and Data Protection Commissioner of Canada, will be responsible for enforcing the Digital Safety Act and the PPCDA. As drafted, both acts contain potentially significant penalties for non-compliance. Under the Digital Safety Act, penalties can reach up to 5% of global revenue or C$20 million, whichever is greater. Under the PPCDA, fines may reach 3% of global revenue or C$10 million, whichever is greater.

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: A Look at the Annex 1 and 3 EU AI Act Guidelines on High-Risk Systems; Transparency of AI-Generated Content – EU Publishes Code of Practice; and European Commission Fines Temu €200 Million Under the DSA.

Contact

Rebecca Cousin
Head of Data 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

Henry Pelling
Associate
T: +44 (0)20 7090 5333
E: henry.pelling@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