

DATA PRIVACY

SELECTED LEGAL AND REGULATORY DEVELOPMENTS IN DATA PRIVACY

QUICK LINKS

EDITORIAL

LEGAL UPDATES

CASE LAW UPDATE

REGULATOR GUIDANCE

ICO ENFORCEMENT OVERVIEW

EU GDPR ENFORCEMENT OVERVIEW

VIEWS FROM... East and southern AFRICA

THE LENS

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

This summer edition of our newsletter is going out shortly after the UK's [Data \(Use and Access\) Act 2025](#) (DUA Act) became law. This is welcome news on a number of levels. Like many of your teams, we have been monitoring the progress of the UK's data reforms for years now and are relieved that the hours spent engaging with the proposals, in our team and across the economy, have resulted in a moderate piece of legislation entering the statute books. While not an earthquake, the DUA Act does contain some useful data protection relaxations and will undoubtedly provide new opportunities for innovation and growth - particularly in those sectors that will now see the development of smart data regimes.

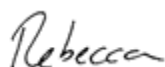
The other reason we are pleased to see the DUA Act reach fruition is that it signifies a maturing of government and regulatory perspectives on data protection - best demonstrated by the introduction of a new pro-innovation duty the Information Commissioner will now need to balance with their obligations to ensure that personal data is protected. It is significant that these UK reforms are taking place against a backdrop of similar conversations at EU level (discussed further in this [blog](#)).

In a similar vein, we were pleased to hear of the pro-innovation collaboration and information sharing that is ongoing between the Information Commissioner's Office and the Financial Conduct Authority, as part of efforts to support financial services organisations' uptake of AI in the UK (discussed further [here](#)).

The ICO's publication of its [AI and biometric strategy](#) in June marks another milestone in the regulator's efforts to walk the line between promoting innovation and protecting individuals. For those organisations either exploring or in early-phase AI uptake, the strategy provides reassurance that the regulator is committed to producing refreshed and easier-to-get-across AI guidance in the form of a statutory code. The strategy is also a timely reminder that despite the ICO's pro-innovation positioning, enforcement action for AI may still follow where compliance with the General Data Protection Regulation (GDPR) is lacking and there are real risks for individuals, with AI in recruitment and developers of AI models seemingly in frame.

My team is looking forward to catching up with many of you across the summer conference season, but for those we don't catch - do get in touch if you would like to discuss any of these issues.

Wishing you very happy holidays as and when you get there,



Rebecca Cousin, Head of Data Privacy

LEGAL UPDATES

Data (Use and Access) Act 2025

The UK's data law reform efforts came to fruition on 19 June when the DUA Act became law. The passage of the DUA Act was delayed following protracted to-ing and fro-ing between the Houses of Parliament on provisions aiming to address concerns about the use of copyright works to train generative AI models. This ultimately ended in a compromise, discussed further [here](#). Key aspects of the DUA Act include:

- the introduction of primary legislation to enable the development of sector-specific 'smart data' data sharing schemes;
- amendments to UK data protection law, including relaxations of the current rules around cookies and automated decision making and the introduction of new requirements relating to complaints procedures; and
- changes to the UK's data protection regulator, the Information Commissioner's Office (ICO), which will become the Information Commission and gain new powers, including to issue higher (GDPR level) penalties for marketing and cookie infringements. We discuss these changes in more detail in this [blog](#).

The DUA Act's changes do not all take effect immediately but are expected to be brought into force by the Government over the next year. The ICO has launched a [new set of guidance](#) on the DUA Act to support organisations with the changes.

UK's EU adequacy decisions to be extended by six months

The European Commission has confirmed an [extension](#) to the EU's adequacy decisions for the UK (under the GDPR and the Law Enforcement Directive), which underpin the free-flow of personal data between the territories. The existing EU decisions were scheduled to expire on the 27 June but will now run until 27 December 2025 to enable the Commission to assess the impact of the DUA Act. While still worth monitoring, significant concerns about the impact of the UK's data reforms on EU adequacy have subsided, given the DUA Act's more light-touch reforms (compared with the previous government's draft legislation, see [here](#)) and Government assurances of extensive dialogue with the EU in relation to the changes.

EU GDPR reform proposals

The EU is also considering GDPR reforms to [enhance competitiveness](#), with the European Commission publishing a [proposal](#) to simplify the EU GDPR's record keeping requirements for small businesses (discussed further in this [blog](#)).

In the meantime, attempts to streamline EU GDPR enforcement are progressing. The EU Council and EU Parliament have [announced](#) a provisional agreement on the GDPR Procedural Regulation, which seeks to improve cooperation between European data protection authorities (DPAs) in cross-border cases (discussed in our previous newsletter [here](#)). Final confirmation and adoption of their positions is now awaited by both institutions before the Regulation can become law.

CASE LAW UPDATE

Meta sees developments in Irish DPC fine appeal proceedings

As discussed in our previous [newsletter](#), Meta is pursuing a number of avenues to challenge the significant fines it has received from the Irish DPA. Progress in these actions is shedding fresh light on GDPR enforcement mechanisms as well as raising questions around the procedural management of concurrent GDPR appeals. For example, recently:

- Advocate General (AG) Tamara Ćapeta of the Court of Justice of the European Union (CJEU) issued her [opinion](#) in relation to the appeal by WhatsApp Ireland Limited (WhatsApp) against the binding decision of the European Data Protection Board (EDPB) that resulted in the Irish DPA increasing its penalty against WhatsApp to €225 million. The fine related to transparency failings on the messaging service (discussed in our previous [newsletter](#)). The EU's first tier General Court had previously held that WhatsApp's appeal against the EDPB decision was inadmissible, as WhatsApp was not directly concerned by the decision. However, the AG's non-binding opinion suggests the General Court erred in this finding. If the CJEU follows the AG's opinion, WhatsApp could progress its appeal against the EDPB's decision, potentially marking a new era of scrutiny for EDPB decision making.
- In March, the Irish Court of Appeal [determined](#) that Meta's appeal against the Irish DPA's €265 million [fine](#) (for data scraping on its Facebook and Instagram platforms) should proceed without further delay. The appeal had been [adjourned](#) by the Irish High Court last year pending the determination of the CJEU WhatsApp case

(discussed above). However, the Irish Court of Appeal found that any further delay would be harmful to the economic and timely determination of the issues, so the appeal should proceed. The decision suggests the Court is taking pragmatic action to reduce the length of the GDPR appeals process, while acknowledging that further references to the CJEU are likely in this case.

Tribunals hear ICO enforcement appeals

While not at the judgment stage yet, recent months have seen significant developments in relation to the ongoing appeals against major ICO enforcement actions:

- The ICO's appeal against the overturning of its £7.5 million penalty against Clearview AI Inc was heard in the Upper Tribunal (UT) on 9-11 June. The ICO is appealing against the decision of the First-tier Tribunal (FTT) (discussed [here](#)) that Clearview's data processing was outside the scope of the UK GDPR and the ICO's jurisdiction, on the basis that its services were used for law enforcement and national security functions. In the UT, the ICO reasoned that whilst the clients of Clearview were involved in national security, and therefore out of scope of the GDPR, Clearview itself was operating as a commercial entity and should be regulated as such.
- TikTok's appeal against the ICO's £12.7 million penalty in 2023 (discussed [here](#)) was before the FTT this quarter, with a preliminary reference hearing taking place in May. Submissions centred on TikTok's presentation of itself as a 'free expression service', arguing that the ICO exceeded its powers in issuing the penalty as TikTok's processing should fall under a Data Protection Act 2018 exemption relating to the processing of personal data for artistic purposes.
- The ICO has also been granted [permission](#) to pursue its appeal against the findings of the UT in the DSG case (discussed in our [November](#) newsletter) in the Court of Appeal. The fact that the ICO is seeking to pursue this case further indicates that the case has important implications for the definition of personal data and pseudonymised data under UK law. No date has currently been set for the hearing.

These developments serve as an important reminder that UK data protection law is still developing via the courts, as well as through legislative changes.

REGULATOR GUIDANCE

KEY REGULATOR GUIDANCE	
ICO	
ICO call for views on existing guidance on international transfers (call for views closes 7 August 2025)	June 2025
ICO consultation on draft guidance on consumer Internet of Things products and services (consultation ends 7 September 2025)	June 2025
ICO consultation on the draft updated guidance on encryption (consultation ended on 24 June 2025)	May 2025
ICO guidance on anonymisation	March 2025
EDPB	
Guidelines 02/2024 on Article 48 GDPR (on transfers of personal data to third country authorities)	June 2025
Guidelines 02/2025 on processing of personal data through blockchain technologies (consultation ended on 9 June 2025)	April 2025

UPDATES FROM THE ICO

ICO launches call for views on existing international transfers guidance

The ICO has launched a six week [call for views](#) on its current international transfers guidance. It is seeking to understand which elements of the guidance are helpful, and whether there are any tools which would make international transfers easier for organisations. The ICO had committed to issuing new and updated guidance on international transfers in a letter to the Prime Minister, the Chancellor and the Business Secretary published earlier this year. The letter was in response to a request to the Information Commissioner for proposals to boost business confidence, improve the investment climate, and foster sustainable economic growth. The call for views will close on 7 August 2025.

ICO consults on draft guidance for consumer Internet of Things products and services

The ICO has published [draft guidance](#) for consultation on Internet of Things (IoT) products and services targeted at consumers, such as smart appliances and fitness trackers. The guidance seeks to ensure IoT providers are aware of their GDPR and Privacy and Electronic Communications Regulations 2003 (PECR) obligations, and how the two sets of rules interact. Against concerns that users do not fully understand how their data is being processed by IoT devices and lack control in relation to the processing (reflected in [ICO workshops](#)), the guidance highlights requirements around user consent and transparency, data protection by design and data minimisation, and in relation to individual rights amongst others. The consultation closes on 7 September 2025.

ICO issues updated guidance on encryption

To reflect developments in technology, the ICO has issued an updated version of its [encryption guidance](#) for consultation. As a reminder, encryption is a security measure that organisations can apply to personal data to protect it, but encrypted data remains personal data. The draft guidance adopts the regulator's latest 'must', 'should', 'could' approach to guidance (which distinguishes legal requirements which organisations 'must' follow from other ICO recommendations) and covers what encryption is and how encryption relates to data protection law. It also examines in more detail encryption in relation to stored data and data in transit. The ICO is particularly prescriptive in relation to the type of encryption that must be used for in-transit data, aligning with National Cyber Security Centre guidance (e.g. in calling for organisations to use HTTPS as an encryption method across all website pages). The updated guidance also includes new worked encryption scenarios, covering for example, encryption and the cloud. The consultation closed on 24 June 2025.

ICO issues long-awaited anonymisation guidance

The ICO has published new [guidance on anonymisation and pseudonymisation](#). The guidance largely retains the ICO's previous position that information can be personal data in the hands of one controller but anonymous (and therefore no longer personal data and so outside the GDPR regime) in the hands of a third party. However, the guidance is a bit less clear on this point than we may have hoped and introduces new nuances to the analysis. It suggests, for example, that pseudonymised information that would be anonymous in the hands of a third party would amount to personal data in the hands of the controller's own processor or their joint controller. The guidance also retains the 'motivated intruder' test to assist with determining whether information is anonymous or personal data, confirming the high standard for UK GDPR anonymisation persists. We discuss these concepts and the new guidance in more detail [here](#).

UPDATE FROM THE EDPB

EDPB consults on blockchain guidance

The EDPB has issued draft guidance on data protection and blockchain. It provides an overview of blockchain technology and the distinct types of blockchain architecture (e.g. permissioned vs unpermissioned, public vs private) alongside their implications for data protection. The guidance examines the challenges that certain features of blockchain pose for GDPR compliance (such as the distribution of information across a network and the often immutable nature of information recorded), recognising that some risks can be mitigated upfront whereas others can pose ongoing challenge. The guidance puts forward recommendations for organisations, including via a helpful checklist at Annex 1, with data protection by design being key. We discuss the guidance in more detail in this [blog](#) and our publication: [When decentralisation meets regulation: how blockchain and GDPR can coexist](#).

EDPB publishes expert reports on AI

With DPAs across Europe focusing on AI, recent months have seen a suite of reports published under the umbrella of the EDPB's Support Pool of Experts initiative (SPE). The SPE was introduced to support DPAs' "capacity to enforce by developing common tools" with a particular focus on emerging technologies. Although papers by the SPE make clear that they do not reflect the opinion of the EDPB, they provide useful insight into emerging areas of focus for EU DPAs, as well as a useful source of reference for organisations. The SPE has recently published three reports on AI:

- [Fundamentals of Secure AI Systems with Personal Data](#) (June 2025) This five-part training curriculum is aimed at cybersecurity professionals, developers and deployers of AI systems and aims to fill the current skills gap around AI security and data protection.
- [Law & Compliance in AI Security and Data Protection](#) (June 2025) This training programme is aimed at data protection officers and aims to provide a comprehensive foundation on legal and compliance issues in AI security and personal data protection, with case studies covering the GDPR, the EU AI Act and the Data Act.
- [AI Privacy Risks & Mitigations Large Language Models \(LLMs\)](#) (April 2025) This paper puts forward a comprehensive risk management methodology for LLM systems and includes three case studies based on real-world scenarios.

ICO ENFORCEMENT OVERVIEW

ICO focuses on cyber enforcement

The ICO has issued a number of cyber breach related enforcement actions over recent months and has [called](#) on organisations to do more to combat the growing cyber threat. The ICO has fined:

- (A) DNA testing company 23andMe [£2.31 million](#) on 5 June, following the conclusion of a joint investigation with the Privacy Commissioner of Canada into a 2023 data breach. In announcing the fine the ICO reaffirmed that the UK GDPR still applies to 23andMe despite its bankruptcy declaration. Nevertheless, the ICO's final penalty for 23andMe is half the amount indicated in the ICO's provisional fine announcement in April (£4.59 million), in part reflecting the change to the company's financial position.
- (B) DPP Law Ltd [£60,000](#) on 17 April, after a cyber-attack against the law firm led to highly sensitive personal data being published on the dark web. Attackers exploited administrator accounts that lacked multi-factor authentication.
- (C) Advanced Computer Software Group Limited [£3.07 million](#) on 26 March, for processor security failings after a ransomware attack in 2022 exposed the personal data of 79,404 individuals including sensitive information, such as home entry details for 900 individuals receiving care from the NHS. We discuss this fine further in our recent [blog](#).

The ICO's focus on cyber extends beyond fines - for example the ICO recently issued a joint [statement](#) with the NCSC, responding to the recent spate of retail cyber incidents, confirming both regulators are working closely with impacted organisations. The heightened activity, both by threat actors and regulators, emphasises the importance of robust security measures and cyber preparedness. We discuss recent cyber trends and the importance of understanding cyber insurance coverage in our recent [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
BfDI (Germany)	Vodafone	€45 million	6 June 2025	<ul style="list-style-type: none">• Data security• Processors
DPC (Ireland)	TikTok	€530 million	2 May 2025	<ul style="list-style-type: none">• International transfers

DPA (Country)	Company	Amount	Date	Description
Garante (Italy)	Acea Energia (in Italian)	€3.8 million	7 May 2025	<ul style="list-style-type: none"> • Individuals' rights • Lawful basis
Garante (Italy)	Luka	€5 million	10 April 2025	<ul style="list-style-type: none"> • Lawful basis • Transparency
UODO (Poland)	Poczta Polska (Polish Post Office)	€6.5 million	17 March 2025	<ul style="list-style-type: none"> • Lawful basis

Irish DPC issues TikTok with €530 million fine for data transfers

In May, the Irish DPA issued TikTok with a €530 million [penalty](#) in connection with TikTok's transfers of EEA users' personal data to China. The Irish DPA held the transfers were made without the necessary GDPR safeguards (such as standard contractual clauses) or transparency information being put in place. The Irish DPA decided to proceed with the fine despite TikTok undertaking "Project Clover", a €12 billion European data security initiative. TikTok was also ordered to suspend data transfers to China within six months, although TikTok has been granted a stay on the suspension until early October, when its appeal against the Irish DPA's decision is due to take place.

Regulatory focus on AI

Regulators across the EU are focusing on AI but there are clear signs they are adopting diverging approaches to driving compliance. On one hand, fines remain a real risk - in April the Italian DPA issued a fine of €5 million against [Luka Inc.](#), in connection with its Replika AI "virtual companion" chatbot. This followed the DPA's €15 million fine against OpenAI in December (discussed in our previous [newsletter](#)). The Italian DPA's penalty against Luka, Inc, highlighted failings in connection with lawfulness and transparency, and around age verification for the use of Replika. On the other hand, some high profile regulators are seeking to drive data privacy compliance in AI development by engaging with key players before products are launched. Statements from both the Irish DPA and ICO indicate they are taking this approach - although this doesn't rule out fines from these regulators. We explore these trends in GDPR AI enforcement further in this [blog](#).

VIEWS FROM... EAST AND SOUTHERN AFRICA

Contributed by John Syeki, Partner, Bowmans (Nairobi)

The East and Southern Africa regions continue to see significant developments in data protection law and enforcement. From legislative reforms in Kenya to regulatory implementation in Zambia and South Africa, regulators are actively refining legal frameworks and strengthening oversight and enforcement mechanisms. Below is a snapshot of notable updates across key jurisdictions.

Kenya

In May 2025, the Office of the Data Protection Commissioner ("ODPC") released a series of sector-specific draft guidance notes to enhance effective implementation of the Data Protection Act, 2019 covering areas such as processing children's data, biometric data, and data used for research and journalistic purposes. Stakeholder feedback is currently under review by the ODPC.

A recent High Court decision in *Republic v Office of the Data Protection Commissioner Ex parte Hotel Waterbuck Ltd & Victor Siele* has clarified the proper legal pathway for challenging regulatory decisions under Kenya's data protection framework. The Court held that judicial review is not the appropriate remedy for contesting ODPC determinations, which must instead be appealed through the statutory process outlined in the Data Protection Act. This process is established under Section 64 of the Data Protection Act, which grants individuals the right to appeal administrative actions, including enforcement and penalty notices, directly to the High Court within 30 days of the date of receipt of the notice.

Tanzania

In Tanzania organizations were required under the Personal Data Protection Act (“PDPA”) to register as data controllers or processors by 30 April 2025 to ensure compliance. This will be necessary for organisations, both local and foreign, that operate within Tanzania and process personal data of individuals or entities in Tanzania. In addition to registration, the PDPA imposes ongoing compliance requirements, including the submission of quarterly compliance reports by registered entities. Furthermore, organisations seeking to transfer personal data outside Tanzania must obtain a permit from the Commission, reflecting the country’s commitment to safeguarding personal data in cross-border contexts.

Zambia

In March 2025, the Data Protection Commission commenced enforcement of the Data Protection Act, 2021, requiring all data controllers and processors to complete mandatory registration by 30 April 2025. The Data Protection Commission is yet to issue guidance on extension of the registration deadline. In parallel, the enactment of the Cyber Security Act, 2025 and the Cyber Crimes Act, 2025 has sparked debate among digital rights advocates. While these laws aim to strengthen the country’s cyber infrastructure and address online threats, concerns have been raised about their potential to infringe on privacy and civil liberties.

Mauritius

Mauritius has launched its Blueprint for Digital Transformation 2025-2029, outlining strategic priorities in cybersecurity, ethical artificial intelligence, and data protection. The Blueprint proposes comprehensive legal reforms, including updates to data protection laws to align with evolving international standards (such as the GDPR), amendments to the Cybercrime Act to address emerging threats like deepfakes and ransomware, and revisions to telecommunications legislation to support the rollout of 5G infrastructure and enhance regulatory oversight of digital service providers.

South Africa

In April 2025, the South Africa Information Regulator implemented amendments to the Regulations under the Protection of Personal Information Act, 2018 (“POPIA”) to include simplified and accessible procedures for data subjects to exercise their rights through various channels, including email, SMS and WhatsApp. In addition, organizations facing administrative fines may now negotiate payment by instalment, subject to assessment.

In conclusion, the developments across Africa reflect a clear regional momentum toward strengthening data protection regimes and promoting accountability in the handling of personal data.

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: [Cyber Update: New Software Security Code of Practice](#), [International transfers in the limelight again with Belgian decision on FATCA data transfers to the US](#) and [Commission updates Model Contractual Clauses for AI procurement](#).

CONTACT



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



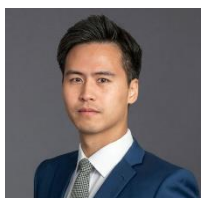
REBECCA COUSIN
PARTNER
T: +44 (0)20 7090 3049
E: rebecca.cousin@slaughterandmay.com



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



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

Published to provide general information and not as legal advice. © Slaughter and May, 2025.
For further information, please speak to your usual Slaughter and May contact.

www.slaughterandmay.com

590506539