

DATA PRIVACY

SELECTED LEGAL AND REGULATORY DEVELOPMENTS IN DATA PRIVACY

QUICK LINKS

[LEGAL UPDATES](#)[CASE LAW UPDATE](#)[REGULATOR GUIDANCE](#)[ICO ENFORCEMENT
OVERVIEW](#)[EU GDPR ENFORCEMENT
OVERVIEW](#)[VIEW FROM... NIGERIA
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

Welcome to the summer edition of our newsletter. There certainly has been a season change in the political and legal landscape since our last edition, perhaps more so than in the British weather. The Data Protection and Digital Information Bill's long-promised update to the UK data protection regime fell away ahead of the 4 July election and it is currently unclear whether the new Labour government will look to take forward any aspects of it (as we discuss further below). The new era is also being ushered in by the EU's headline Artificial Intelligence Act, which entered the Official Journal on Friday and will come into force 20 days later on 1 August (also discussed below and in [this briefing](#)).

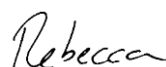
Against this backdrop of change, it has been great to catch up with so many of you to exchange views and share experiences over recent months. We were delighted to host our latest roundtable on the topic of AI and data protection in June. We enjoyed frank discussions over two mornings (and two delicious breakfasts) around the challenges and opportunities posed by AI for DP teams and how they are being navigated in practice. We have subsequently written a briefing for the Privacy Laws & Business UK report on this topic, which we look forward to sharing with you in the coming days.

We also caught up with a number of you in Cambridge at the PL&B International Conference at the start of this month. I had the opportunity to chair one of the conference panels on the important issue of women's privacy, alongside panellists from the ICO and US DOJ. It was a sobering session but valuable to be able to focus on the real-world impact of privacy infringements on people's lives.

Privacy infringements causing serious harm to individuals have continued to be an area of enforcement focus for the ICO, with its latest fine against the Police Service of Northern Ireland (see below). The regulator's fining approach appears to have crystallised in recent months, including through publication of its latest fining guidance. It will be interesting to see the extent to which this approach evolves in light of the new government's priorities.

As always, we will be watching closely to ascertain the direction of travel for data protection, digital and AI. We are already planning events over the autumn, including roundtables and the return of our Forum Academy so we will have plenty of opportunity to keep you updated.

Before then, I wish you warm and sunny summer - or at least happy holidays!



Rebecca

LEGAL UPDATES

EU Artificial Intelligence Act passes into law

The EU's AI Act will come into force on 1 August and will apply from 2 August 2026, with some provisions coming into effect sooner. Cited by the European Commission as the 'world's first comprehensive AI law', the AI Act has caught the attention of organisations across the globe with its focus on responsible innovation, wide extra-territorial reach, high fines and prohibition on certain types of AI which pose an unacceptable risk. Our Digital Regulation team has partnered with US law firm Cravath Swaine & Moore LLP to draft a detailed briefing which highlights some of the key aspects of the AI Act, focussing on ten key questions. The team also look at what practical steps organisations can take now to comply with the AI Act, and how the AI Act compares with the approach to AI regulation being taken in other jurisdictions like the UK and US. Follow [this link](#) to read the full briefing.

Data Protection and Digital Information Bill dropped ahead of UK general election

The [Data Protection and Digital Information Bill](#) (the DPDI Bill) failed to pass in the wash-up period ahead of the prorogation and dissolution of Parliament before the UK general election on 4 July. A number of trade and industry groups are calling for the new Labour government to progress a slimmed down version of the Bill, including [TechUK](#) and the [Data & Marketing Association](#), but it remains to be seen whether they will do so.

CASE LAW UPDATE

High Court issues ruling on DSARs

The High Court has provided useful clarification on a number of aspects of the UK data subject access request (DSAR) regime, in the recent case of [Harrison v Cameron and another](#). The claim in question related to recordings of a heated telephone conversation between the chief executive of a real estate company, Mr Harrison, and a landscape gardener, Mr Cameron. In the course of the conversation, threats were made by Mr Harrison, and Mr Cameron subsequently shared the call recordings and transcripts with 15 people. The claim centred on whether the identities of those 15 people should be provided in response to Mr Harrison's DSAR. The judgment analyses the third-party data exception to the requirement to provide information in response to a DSARs (in paragraph 16 of Schedule 2, Data Protection Act 2018) and relevant case law. It confirms controllers have a 'wide margin of discretion' in undertaking the balancing exercise between the rights of the data subject and those of the third parties. Whilst on the facts of the case, the data subject's right of access to the identities of the 15 recipients was dismissed (as their rights outweighed the data subject's), the judge provided important analysis of the meaning of Article 15(1)(c) UK GDPR. Mrs Justice Styne confirmed that unless it is impossible or manifestly excessive to do so, controllers should provide a specific list of 'recipients' in response to a DSAR, if requested to do so by the data subject, rather than a list just outlining 'categories of recipients'. This follows the interpretation of the CJEU in the Austrian Post case (discussed in our previous [newsletter](#)) which, Mrs Justice Styne confirmed, should be applied in determining the meaning of Article 15(1)(c) of the UK GDPR.

Further rulings on non-material damages

Following on from the non-material damages cases discussed in our [November](#) and [March](#) Newsletters, the CJEU has provided further guidance in the recent [Scalable Capital](#) case (C-182/22). Alongside other issues, the decision confirms that the concept of 'identity theft', cited in GDPR recitals as an example of non-material damage, requires personal data to be actually misused by a third party (rather than just taken). The decision also recognises however, that such situations are not the only instances in which data theft can result in compensation. Following the reasoning in the Austrian Post case, data theft can potentially give rise to compensation wherever an individual suffers damage which is caused by processing carried out in breach of GDPR (as we discuss further in our previous [newsletter](#)).

Upper Tribunal dismisses the ICO's appeal in Experian case

The [Upper Tribunal](#) has rejected all five grounds of the Information Commissioner's appeal against the findings of the [First-tier tribunal](#) (FTT) on the ICO's 2020 [enforcement notice](#) against Experian (discussed in our previous [newsletter](#)). Experian had challenged the ICO's enforcement notice and, in particular, the regulator's conclusions on the company's approach to transparency and use of legitimate interests in relation to its offline marketing business. Although the Upper Tribunal criticised certain aspects of the FTT's decision and reasoning, the FTT's business-friendly interpretation of legitimate interests and relatively pragmatic view of the GDPR's transparency obligations stand. The ICO has [confirmed](#) it will not be seeking permission to appeal the Experian case further with Deputy Commissioner, Stephen Bonner, confirming the importance of the tribunal's scrutiny in clarifying "several key points".

REGULATOR GUIDANCE

KEY REGULATOR GUIDANCE	
ICO	
Generative AI fourth call for evidence: engineering individual rights into generative AI models (consultation closed on 10 June 2024)	May 2024
Learning from the mistakes of others (cyber)	May 2024
Guidance on special category data (updated)	April 2024
Call for views on “consent or pay” business models (consultation closed on 17 April 2024)	April 2024
Generative AI third call for evidence: accuracy of training data and model outputs (consultation closed on 10 May 2024)	April 2024
Data Protection Fining Guidance (final version, updated after consultation)	March 2024
EDPB	
Guidelines on generative AI: embracing opportunities, protecting people	June 2024
Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms	April 2024

ICO progresses consultation series on generative AI (genAI)

The ICO has continued to develop its consultation series on the interaction between genAI and data protection, calling for views on the [accuracy principle](#) and [data subjects rights](#) in this context. These latest chapters build on the work of the first two, on the [lawful basis for web-scraping](#) and [purpose limitation in the generative AI lifecycle](#), discussed in our [previous](#) newsletter. The ICO explains that accuracy under the GDPR is different to statistical accuracy, meaning the outputs of a model do not need to be 100% statistically accurate to comply with the GDPR. Nevertheless, ensuring the accuracy of training data is key, and organisations should carefully consider how inaccurate data used during the training process could impact the accuracy of outputs (see our [blog](#) on this chapter for further discussion). On individuals’ rights, the ICO outlines that organisations must have processes in place to ensure these rights are respected throughout the entire genAI lifecycle and notes that the cost of implementing these procedures should be considered in business decisions from the outset. We consider this latest chapter in more detail in this [blog](#).

ICO updates special category data guidance

The ICO has made a number of [updates](#) to its guidance on special category data (SCD). The most significant change is in relation to how the ICO treats inferences made by organisations. The requirement that an inference is made with “a reasonable degree of certainty” has been removed as a deciding factor in whether the information amounts to SCD. The guidance also includes new content on the processing of biometric data and new examples, including on social media platforms’ processing of SCD. The ICO’s statement accompanying the updated guidance confirms that its position on SCD has not altered but that it has amended its explanation for clarity.

ICO and EDPB consult on “consent or pay” business models

Against a backdrop of increasing focus on ad-funded online business models, the ICO and European Data Protection Board (EDPB) have both recently issued consultations on ‘consent or pay’ models. These business models give individuals the choice between consenting to their information being used for personalised advertising in exchange for free access to an online service or paying to access the service. The ICO’s [call for views](#) on the topic indicates that the UK regulator’s initial perspective is that data protection law does not prohibit ‘consent or pay’ models. However, the ICO cautions that

organisations need to ensure they are obtaining valid (e.g. freely given and informed) consent and that they are properly informing individuals about the processing. We discuss the ICO's approach in more detail in this [blog](#).

On 17 April (the same day the ICO's call for views closed), the EDPB issued its [opinion](#) on the topic. Focusing specifically on large online platforms, in response to a request from the Dutch, Norwegian and Hamburg data protection authorities (DPAs), it seeks to establish when consent will be freely given by users choosing between 'consent or pay'. At first glance, the EDPB's position appears to be more restrictive than the ICO's, as it suggests that in most cases 'consent or pay' models which only offer users this binary choice will not comply with the requirements of data protection law. The EDPB suggests that controllers should consider providing an additional alternative to payment for those who don't want to consent, such as an option with advertising using less personal data, or none. On further reflection though, it is likely that the ICO and the EDPB's views are not as far apart as the rhetoric might suggest. With the European Commission issuing [preliminary findings](#) of non-compliance against Meta in respect of its 'consent or pay' advertising model under the Digital Markets Act on 1 July, this is likely to be a continuing area of regulatory focus and development in the months to come.

EDPS provides EU institutions with guidance on genAI

The European Data Protection Supervisor (EDPS) published their [orientations](#) on genAI and its interaction with data protection, on 3 June. While directed at the EU institutions, the guidelines provide valuable practical advice as well as an insight into the EDPS's thinking on genAI. We discuss the key takeaways for organisations in our [blog](#).

EDPB publishes its strategy for 2024-2027

The EDPB has announced its [strategy for 2024-2027](#), promising among other things new guidance on legitimate interests and highlighting how the EDPB will cooperate with other regulators, including consumer protection authorities, competition authorities, and authorities competent under other legal acts such as the EU AI Act.

ICO ENFORCEMENT OVERVIEW

ICO publishes final decision following investigation into Snap

The ICO has closed its investigation into Snap's 'My AI' chatbot, with no enforcement action being taken against the company. The ICO's [preliminary enforcement notice](#), issued in October 2023, (discussed in this [blog](#)) had identified infringements relating to Snap's risk assessments for 'My AI' and had suggested the regulator may look to take enforcement action in relation to it. However, the ICO investigation subsequently resulted in Snap taking "significant steps" to improve its data protection impact assessment for My AI and to bolster its mitigations of the risks posed by the tool. Despite the ICO not pursuing enforcement action in this case, in a statement, Stephen Almond, the ICO Executive Director of Regulatory Risk, described the Snap decision as a "warning shot" and confirmed that the ICO will continue to use its full range of enforcement powers, including fines, in this area. We discuss the key insights for organisations from the ICO's decision in this [blog](#).

PSNI facing £750,000 fine for data breach that exposed personal information of entire workforce

On 23 May the ICO [announced](#) its intention to fine the Police Service of Northern Ireland (PSNI) £750,000 after a data breach exposed the personal information of the entire PSNI workforce (i.e. over 10,000 officers and staff). The breach was caused when a hidden tab in a spreadsheet was included in a version published online in response to a freedom of information request. Recognising the incident as life-altering and potentially life-threatening, the ICO indicated that if its public-sector fine reduction approach was not in place, the fine would have been set at £5.6 million. The ICO has recently [announced](#) that it will be reviewing its approach to public sector enforcement, following a two year trial which has seen the ICO issue lower fines and focus on other elements in an attempt to avoid diverting money from public institutions. A decision on the approach is expected in the autumn.

The ICO has also recently issued the final version of its [fining guidance](#), which promises to usher in a new, more focused era of ICO enforcement, with quicker and clearer outcomes for organisations under investigation. We discuss the changes made to the guidance in its final version and the implications for organisations in this [blog](#).

Learning from the security mistakes of others

Leveraging its regulatory experience on data breaches, the ICO has provided a [report](#) into current trends and future developments across the five main causes of security breaches: phishing; brute force attacks; denial of service; errors and supply chain attacks. The report emphasises that criminals will continue to use new technologies to develop threats, and organisations need to respond by ensuring they keep pace with the changing threat landscape. The findings of the report are covered in more detail 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 DPAs in the last 4 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)/ LRV (Lithuania)	Vinted	€2.4 million	3 July 2024	Individuals' rights Accountability
Garante (Italy)	Eni Plenitude	€2.8 million	26 June 2024	Lawful basis Transparency
IMY (Sweden)	Avanza	SEK 15 million (c. €1.3 million)	25 June 2024	International data transfers
UOOU (The Czech Republic)	Avast	€13.9 million	10 April 2024	Lawful basis Transparency
Garante (Italy)	Unicredit	€2.8 million	7 March 2024	Data security

Intragroup sharing of pseudonymised data results in €13.9m fine

Avast Software has been fined €13.9 million by the Czech DPA for unlawfully sharing data relating to approximately 100 million users. The data shared included users pseudonymised internet history tied to a unique identifier and the subsidiary in question was suggested to be sharing the data with third parties for marketing purposes. The Czech DPA concluded that a user's browsing history constituted personal data even if it were incomplete, as it was possible some individuals could be re-identified from it. The DPA also found that Avast had misinformed data subjects about the transfers, as it claimed the data transferred was anonymised and used only for statistical trend analysis. This action is a useful reminder of the high bar for data being classified as anonymous under the GDPR.

Vinted fined by Lithuanian DPA for data subjects' rights failings

Vinted has been issued with a fine totalling nearly €2.4 million following complaints to the Lithuanian DPA, as the Lead Supervisory Authority, forwarded by the Polish and French DPAs. The complaints focused on the unwillingness of Vinted to comply with data erasure requests unless the data subject specified the Article 17(1) grounds for deletion. In reviewing the complaints, the DPA discovered that Vinted also invisibly processed the data of individuals that had broken the platform's terms to 'shadow block' them into not using the service. This was in violation of the GDPR's transparency and fairness principles. The investigation also identified accountability failings, with Vinted struggling to demonstrate it had taken action in relation to the right of access. The discovery of these additional failures highlights again the risk that when there is a breach of the GDPR it can lead to a regulator 'opening the bonnet' to uncover further breaches.

VIEW FROM... NIGERIA

Contributed by Jumoke Lambo (Partner), Babatunde Olayinka (Senior Associate), Chisom Okolie (Senior Associate), Opeyemi Adeshina (Associate) and Samuel Ngwu (Associate) at Udo Udoma & Belo-Osagie, Lagos

The increasing adoption of a digital economy and market globally has made data protection a critical issue across many jurisdictions including Nigeria. Consequently, Nigeria enacted its first principal data protection legislation, the Nigeria Data Protection Act ("NDPA") on 12 June 2023. The NDPA established the Nigeria Data Protection Commission ("NDPC") as the regulator for the sector. The NDPC has since its inception issued guidelines and regulations to provide additional clarification and guidance of the provisions of the NDPA. We provide below a summary of the significant developments in Nigeria's data protection landscape so far in 2024.

Registration of Data Controllers or Processors of Major Importance

Further to section 5(d) and 65 of the NDPA, in February the NDPC issued a Guidance Notice ("Notice") requiring Data Controllers and Processors of Major Importance ("DCPMI") to register with it before 30 June 2024. This deadline has

been extended to 30 September 2024. The classification of data controllers and processors as DCPMIs or non-DCPMI's was introduced by the NDPA. The Notice defined DCPMIs to mean data controllers or processors who:

- process the personal data of more than 200 data subjects in 6 months, or
- provide ICT services on any digital device that has storage capacity and belongs to another individual; or
- operate in sectors such as finance, communication, health, insurance, export and import, aviation, tourism, oil and gas, electric power.

In addition, DCPMIs are entities which are in a fiduciary relationship with data subjects by virtue of which they are expected to keep confidential information on behalf of the data subjects in view of the significant harm that may be done to data subjects if the data controllers or processors are not under the obligations imposed on DCPMIs by law. The Notice classified DCPMIs into 3 categories namely: (a) major data processing ultra high level; (b) major data processing extra high level, and (c) major data processing ordinary high level.

Any DCPMI that fails to register with the NDPC on or before the deadline will be deemed to be in breach of the NDPA and liable to the penalties imposed for non-compliance under NDPA. The monetary penalty stipulated under the NDPA for any DCPMI that fails to comply with the NDPA is a fine up to NGN10,000,000 (Ten Million Naira) or 2% of its annual gross revenue from the preceding financial year, whichever is greater. Data controllers and processors that process the personal data of residents of Nigeria and fall within the definition of DCPMIs continue to register with the NDPC ahead of the new deadline.

Draft Nigeria Data Protection General Application and Implementation Directive (NDP GAID)

In June 2024, the NDPC released a draft NDP GAID for implementation of the NDPA for public consultation. The NDP GAID seeks to guide data controllers and processors on ensuring their compliance with the applicable data protection obligations and to clarify key terms in the NDPA. For instance, Article 1 of the NDP GAID seeks to expand the scope of application of the NDPA to include the processing of personal data of: (a) data subjects whose personal data has been transferred to Nigeria; (b) data subjects whose personal data is in transit through Nigeria; and (c) Nigerian citizens who are not in Nigeria. In addition, Article 7 now provides for the designation of Associate DPOs /Privacy Champions by DCPMIs (as data controllers or processors) to support the DPO where the processing or interfacing with data subjects occurs on multiple platforms and places. It also adds a requirement to prepare and keep semi-annual data protection reports containing detailed analysis of data processing activities over the last six months, and amends the date for filing annual data protection reports.

The NDPC is still receiving comments on the draft document, particularly on the areas that seem to be unclear to data controllers, processors and other stakeholders. For instance, the NDP GAID allows for the data subject to give implied or constructive consent in certain situations such as where a data subject is participating in public event photo and the images taken in that event are used for reporting on the event. This provision contradicts sections 25(1) (2) of the NDPA which provides that data processing shall be lawful, where the data subject has given and not withdrawn consent for the specific purpose or purposes for which personal data is to be processed, and as such requires additional clarification. It is expected that after receiving comments, the NDPC will finalise and issue the document. We are unable to determine the timing of the issuance of the final document at this time.

The NDPC's activities so far in 2024 reflect its determination to ensure that data protection practices in Nigeria continue to align with global standards. In some cases, such as the establishment of the DCPMIs and the requirement for such entities to be registered with the NDPC, a higher degree of protection of data and duty of care is imposed on data controllers and data processors than global practice stipulates.

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: [What do the Pope, the Republic of Korea and the Labour manifesto have in common?](#); [Are you ready for new data sharing rules ?](#); [Cyber threats evolving as a result of new technologies, warns ICO](#); [Tech companies to see digital regulation come to the UK](#).

CONTACT



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



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



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



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



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



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



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



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

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

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

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

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

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

www.slaughterandmay.com