

# DATA PRIVACY

## SELECTED LEGAL AND REGULATORY DEVELOPMENTS IN DATA PRIVACY

### QUICK LINKS

[LEGAL UPDATES](#)

[CASE LAW UPDATE](#)

[UPDATES FROM THE ICO](#)

[UPDATE FROM THE EDPB](#)

[ICO ENFORCEMENT OVERVIEW](#)

[EU GDPR ENFORCEMENT OVERVIEW](#)

[VIEW FROM... BRAZIL 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 our first newsletter of 2024. It's been a busy (and exciting) few months for us, as I am sure it will have been for you given the continuing pace of developments in our field.

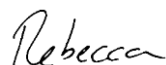
Given these developments, we are also delighted, as a privacy team, to have become part of the firm's new Tech, Digital, Data and IP group. While we have always worked closely with our colleagues, this move enables us to combine expertise in an even more integrated, efficient and seamless way across the increasing digital water-front, for example on topics such as AI and cookies.

Additionally, we held our first Data Privacy Forum Academy in late November. Although similar to our previous Forums in scale, rather than invite senior privacy decision makers, we asked them to nominate people in their team who would like to increase their privacy knowledge. We had fantastic attendance and lots of dynamic sessions and discussion on 'hot topics', including data commercialisation, employee monitoring and incident management. Many thanks to all of you that attended and participated. The Academy will be back later this year.

In reviewing content for this newsletter, the ICO's focus on innovative processing and technology is clear. Their second annual [Tech Horizon report](#) spells out the ICO's 'stitch-in time perspective', i.e. giving guidance on innovative processing early so organisations can build-in privacy from the start. They are also keen to engage with industry on challenging areas, as can be seen with their consultation on the first two generative AI and data protection chapters. The regulator is also seeking to lead by example and has recently published its own [Enterprise Data Strategy](#) setting out how the ICO will use its own data to drive efficiencies.

Looking beyond the UK, the EU's progress on its digital agenda has been gathering pace, with political agreement on the [EU AI Act](#) at the end of last year. It is clear from our discussions with many of you over the last few months, as well as from the EDPB's [report](#) following the coordinated enforcement action on DPOs, that collaboration between teams and taking the opportunity to proactively upskill in these developing areas is going to be vital in the coming months and years – and we will be here to support, so do please get in touch.

Rebecca Cousin, Partner



## LEGAL UPDATES

### Government announces response to AI White Paper consultation

On 6 February, the UK government published the [response](#) to its [AI White Paper](#) consultation. While confirming that the UK will retain its sector specific approach, supported by cross-sectoral principles, the government indicated that it may ultimately introduce binding rules for the most advanced general purpose AI systems. We cover the response in more detail in our [blog](#). In line with its [ICO25 plan](#), the ICO [has launched](#) a consultation series on generative AI and data protection, which we discuss further [below](#).

### EU Commission concludes review into pre-GDPR adequacy decisions

On 15 January, the EU Commission [announced](#) the conclusion of its review into the pre-GDPR adequacy decisions for Andorra, Argentina, Canada, Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay, finding that all 11 jurisdictions continue to provide an adequate level of protection for data transferred from the European Union. This confirmation follows an “intense period of dialogue” between the countries and the EU Commission, which resulted in many of them modernising and strengthening their privacy frameworks. We discuss the review in more detail in our [blog](#).

## CASE LAW UPDATE

### Privacy claims update

There are some limited ‘green shoots’ appearing in relation to data privacy claims in the UK, with claimants and funders continuing to explore ways to progress these claims post-Lloyd. For example, on 23 February, the High Court issued its decision in the [Equiniti](#) case, in which police officers’ pension benefit statements were mistakenly sent to their previous addresses. The claimants brought actions on the grounds of both misuse of private information and a breach of data protection legislation. All but 14 of the 474 claims were struck out by the judge, on the basis that the claimants did not have positive evidence the letters had been opened and without such evidence there was no viable claim via either route. Potentially significantly however, the judge did not decide on whether the damage suffered by the remaining 14 claimants met any ‘threshold of seriousness’ for data protection claims in the UK, as he recognised the “potential importance” of the issue (it has been a significant focus in the EU, as discussed below) and left it to be resolved at trial.

In addition, the opt-out claim brought by Andrew Prismall against Google and its subsidiary DeepMind for misuse of private information in relation to its data sharing agreement with the Royal Free Hospital London has now been granted permission to appeal to the Court of Appeal, following the High Court’s decision to dismiss the claim following the reasoning in Lloyd (as discussed in our [July newsletter](#)).

### CJEU round-up

Clarification of a number of areas has been provided by a flurry of CJEU decisions on data protection over recent months, for example:

- In relation to availability of compensation (following a claim), the CJEU has ruled in a [Case C-340/21](#), from the Bulgarian supreme court, that a fear of misuse of personal data can qualify as a non-material damage for the purposes of the GDPR, but the burden of proof is on the data subject to demonstrate it does.
- The CJEU clarified, in [Case C-683/21](#) following referral from cases in Germany and Lithuania, the instances in which an EU data protection authority (DPA) can issue fines to controllers. The court found imposing a fine requires there be ‘wrongful conduct’ consisting of an intentional or negligent infringement. Helpfully, the case also confirmed that the occurrence of a cyber-attack or data breach does not necessarily mean that a controller’s security measures are inappropriate, that is for a court or tribunal to decide.
- Finally, the court’s position in the Schufa case, [Case C-634/21](#), has defined automated decision making (ADM) broadly to include instances where the ADM has a “determining role” in the decision making process. The facts involved a German credit reference agency (SCHUFA) scoring the individual, which ultimately contributed to the individual’s loan application being rejected by a third party (e.g. an upstream bank). The decision potentially brings more organisations into the scope of the ADM restrictions, with the relevance to AI systems, in particular, being [highlighted](#) by the Hamburg DPA among others.

## KEY REGULATOR GUIDANCE

### ICO

Tech Horizons report	February 2024
Generative AI consultation series: Purpose limitation in the generative AI lifecycle (consultation closes on 12 April 2024)	February 2024
Biometric data guidance: Biometric recognition (final version)	February 2024
Draft Enterprise Data Strategy (consultation closes on 12 March)	January 2024
Generative AI consultation series: The lawful basis for web scraping to train generative AI models (consultation closed on 1 March)	January 2024
Draft Employment practices guidance: keeping employment records (consultation closes on 5 March 2024)	December 2023
Draft Employment practices guidance: recruitment and selection (consultation closes on 5 March 2024)	December 2023
Completing a transfer risk assessment when transferring personal information to the US using an Article 46 transfer mechanism	December 2023
ICO consultation on the guidance and toolkits available to organisations on the topic of AI (consultation closed on 10 January 2024)	December 2023

### EDPB

Opinion 04/2024 on the notion of main establishment of a controller in the Union under Art. 4.16(a) GDPR	February 2024
EDPB responds to EU Commission's voluntary cookie pledge proposal	December 2023
Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive (consultation closed on 18 January 2024)	November 2023

## UPDATES FROM THE ICO

### ICO announces consultation series on generative AI and data protection

Over the last two months, the ICO has announced the first two chapters of a [consultation series](#) that seeks to gain feedback on the ways data protection law applies to generative AI (genAI) models. The [first consultation](#) covers the availability of lawful bases for web-scraping data in connection with training AI models. The consultation document identifies legitimate interests as the most likely legal basis for this processing but raises a number of questions in relation to its use in this context. We discuss this in more detail in our recent [blog](#).

The [second chapter](#) looks at the application of the purpose limitation principle to the genAI lifecycle and outlines a policy position for consultation. The chapter discusses the importance of distinguishing separate purposes for the different phases of genAI development and considers how purposes should be defined in that context. The guidance advocates for a 'clearly defined purpose' and cautions that framing purposes too widely can make it difficult to comply with other GDPR obligations, for example, to explain the specific processing activities covered by the purpose. However, the ICO recognises that narrowly defining purposes is more challenging at the earlier stage of the genAI lifecycle. This second consultation closes on 12 April 2024.

### ICO issues two pieces of guidance for consultation on employment practices

The ICO has continued to develop its guidance for employers by publishing two pieces of guidance for consultation on the topics of [keeping employment records](#) and the duties of organisations during the [recruitment and selection](#) process. It follows the introduction of [guidance on monitoring in the workplace](#) (discussed in our [November 2023](#) newsletter). Both latest pieces of guidance reaffirm the application of key GDPR requirements to the specific employment context but also provide some new insights, for example, the keeping employment records guidance covers how an employer may be permitted to use their records, including in the context of M&A transactions and TUPE transfers. In addition, the recruitment and selection guidance provides additional clarity on the use of AI tools (and automated decision making) within the recruitment process.

### ICO issues pragmatic guidance on TRAs for US transfers

The new [guidance](#) issued by the ICO confirms that organisations transferring personal data to an importer in the US who is not certified under the UK-US data bridge, i.e. using SCCs or another of the safeguards, can rely on the analysis conducted by the UK government's Department for Science, Innovation and Technology when completing their transfer risk assessment. This means that rather than carrying out their own detailed analysis, organisations can rely on the analysis done by the UK Government in preparing their partial adequacy assessment for the US. However, it must be remembered that this new approach is currently only available for US transfers under the UK GDPR, with full assessments still required ahead of other transfers using the SCCs, including those under the EU GDPR.

## UPDATE FROM THE EDPB

### Clarification on the scope of 'main establishment' for One-Stop-Shop

On 14 February, the EDPB published an [Opinion](#) (04/2024) clarifying the concept of 'main establishment' for the purposes of the One-Stop-Shop (OSS) and limiting the application of the OSS for some organisations based outside the EU. The EDPB stated that the "place of central administration" of a controller can only be considered a main establishment if it is making the decisions on the purpose and means of processing and has the power to have those decisions implemented. Therefore, in instances where the processing decisions are made outside of the EU (e.g. where an organisation is taking operational decisions in the UK), there cannot be a main establishment within the EU and, as such, the OSS will not apply.

### EDPB publishes report following coordinated enforcement action on role of data protection officers

The EDPB has published the [results](#) of its second coordinated enforcement action, which focused on data protection officers (DPOs). The extensive action, following the EDPB's [Coordinated Enforcement Framework](#), involved 25 DPAs launching coordinated investigations and resulted in over 17,000 survey responses being received. The EDPB's final report highlights challenges facing DPOs including that a lack of resources and knowledge could be limiting DPO's ability to carry out their role. The report also lists recommendations, including that organisations ensure DPOs have sufficient opportunities and resources to learn about the latest developments and that DPAs develop additional guidelines on conflicts of interest in light of the developing EU digital legislation and the new roles some DPOs are taking in relation to them. The EDPB has recently [announced](#) that its 2024 coordinated enforcement action will focus on the implementation of the right of access across the EU, with 31 DPAs taking part.

## ICO ENFORCEMENT OVERVIEW

### ICO focuses on cookie compliance

The ICO are taking proactive steps to improve organisations' cookie compliance. In November 2023, the regulator published a [statement](#) confirming that it had issued warnings to 53 top 100 UK websites requiring them to address their non-compliant cookie practices within 30 days (see our [January blog](#)). Following up on their initial warning, the ICO [confirmed](#) in January that they had received an 'overwhelmingly positive response' to their letters with the vast majority of companies contacted bringing their cookie banners into compliance as a result, but that this was only the beginning and that they are "already preparing to write to the next 100 - and the 100 after that". We discuss this action and its wider ramifications in our recent [blog](#).

### Enforcement action against Serco for employee monitoring

Leisure providers, Serco Leisure, Serco Jersey and seven associated community trusts have been [issued](#) with an enforcement notice by the ICO ordering them to stop using facial recognition technology and fingerprint scanning to monitor employee attendance. The ICO's investigation found that Serco and the trusts have been unlawfully processing

the biometric data of more than 2,000 employees at 38 leisure facilities for the purpose of monitoring attendance. The enforcement action announcement coincided with the publication of the final version of the ICO’s [biometric recognition guidance](#) (we discussed the draft guidance in our [previous newsletter](#)), demonstrating the ICO’s ongoing focus in this area and comes ahead of the publication of a second phase of the ICO’s biometric guidance, on biometric classification and data protection, which is expected during 2024.

Other recent ICO enforcement action includes both public reprimands and fines. Recent reprimands have been issued against a number of public sector entities (such as [Derby and Burton NHS Foundation Trust](#) for lost and delayed patient referrals affecting nearly 5000 patients) and those in the private sector, including the [Bank of Ireland](#), for incorrectly reporting customers’ default loan status to credit reference agencies, continuing the ICO’s approach of the last year or so (as discussed in our [previous newsletter](#)). Fines continue to be issued for marketing infringements (as we discuss in our recent [blog](#) on the £140,000 fine against HelloFresh). The ICO has also recently issued a financial penalty to the [Ministry of Defence](#) for a data breach relating to high-risk data of individuals seeking relocation from Afghanistan to the UK, resulting in a £350,000 penalty. This is a reminder that the regulator will still issues fines for the most serious infringements.

## EU GDPR ENFORCEMENT OVERVIEW

The table below sets out a selection of the most substantial EU GDPR fines brought by 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
UODO (Poland)	<a href="#">Morele.net</a>	3.8 million Polish Zloty (€879,000)	8 February 2024	Data security
CNIL (France)	<a href="#">Amazon France Logistique</a>	€32 million	27 December 2023	Data minimisation, lawful basis, transparency
AP / CNIL (Netherlands / France)	<a href="#">Uber B.V. and Uber Technologies Inc.</a>	€20 million	11 December 2023	Individuals’ rights, transparency
Datatilsynet (Norway)	<a href="#">SATS</a>	NOK10 million (€873,989)	11 December 2023	Individuals’ rights, lawful basis

### Amazon France Logistique receives employee monitoring penalty from the French DPA

Amazon has received a [penalty](#) of €32 million from the French DPA following an investigation into employee monitoring practices in their warehouses. Employees were given scanners that track their performance of various tasks such as picking and packing items in real time. While acknowledging that Amazon would need some form of monitoring to manage its business in light of its high performance targets, the DPA found that the nature of this particular tracking was excessive (including, for example, the tracking of “idle time”) and was therefore in breach of the data minimisation requirements and lacked lawful basis (as the legitimate interests basis was not available as the company’s interests were outweighed). In addition, the DPA concluded that the system’s data retention was excessive and some employees were not provided with appropriate privacy information about the scanners. This action coincides with the ICO’s focus on employee monitoring ([discussed above](#)).

### Uber receives fine for illegal transfers of data outside the EU

In a joint action between the Dutch and French DPAs, Uber [has been fined](#) €10 million for transparency and individuals’ rights failings, after it failed to specify retention periods for drivers’ personal data or to which countries outside of the EEA the personal data would be sent. The regulators also found Uber hindered the ability for drivers to exercise their data rights by “making it unnecessarily complex” for drivers to do so, via an app-pathway.

## VIEW FROM... BRAZIL

*Contributed by Felipe Palhares, Partner, BMA, Brazil*

### Brazil's Data Protection Law: The State of Affairs in 2024

The Brazil General Data Protection Law (LGPD) became effective in September 2020. The LGPD shares the same structure as the GDPR and shares common features with it. At the same time, it also presents many differences that should be taken into account by organizations that already comply with the GDPR and believe this would be enough to also comply with the LGPD - in many cases, it would not. For instance, timelines for responding to data subjects' access requests (15 days from the date the request is made), obligations on reporting data breaches (which include the same threshold for notifying the Brazilian National Data Protection Authority (ANPD) and affected data subjects, meaning that all incidents that trigger the requirement must be communicated to both) and on appointing a data protection officer (except for small processing agents, all data controllers must appoint a DPO) are quite distinct.

Over the last 3 years, there have been a number of developments in relation to regulatory guidance and enforcement of the LGPD. Below are some examples of relevant work that has been carried out by the ANPD:

- the ANPD has issued several regulations and guidance materials, including on the use of cookies, on recommended security measures for small and medium enterprises, and on the legitimate interest legal basis. On this last topic, the ANPD stated it expects data controllers to prepare legitimate interest assessments before processing personal data based on this legal basis. According to the ANPD, the same assessment should be made before adopting the legal basis of fraud prevention (a legal ground provided by the LGPD for the processing of sensitive personal data). Failure to do so could be deemed an infringement of the law.
- the ANPD has imposed penalties on five data controllers for infringements of the LGPD (four from the public sector and one from the private sector). Although only one of those penalties was a fine - applied against a small businessman for processing personal data without a legal basis and for not cooperating with the ANPD during the sanctioning procedures. The fine related to the creation of a database of contact details (including names and phone numbers) that had been made available online by individuals. The details were then used by the businessman to send marketing messages on behalf of his clients, for a fee. It is expected that the DPA will be highly active in 2024 and may potentially impose larger fines throughout the year. There are three sanctioning procedures still ongoing and 13 oversight procedures ongoing. All of those could result in the imposition of penalties against the respective data controllers and data processors.

Furthermore, there are two relevant regulations that are anticipated by the market and that should be issued by the end of 2024: (i) a regulation on the communication of security incidents (including specific deadlines, which are expected to be set as 3 business days from the date the data controller becomes aware of the incident, and obligations for data controllers, such as creating a technical report on the incident response); and (ii) a regulation on international data transfers, which will include the first set of Brazilian Standard Contractual Clauses.

## 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: [EU AI Act agreed as UK says it won't legislate until timing is right](#), [Changes in Cyber Governance](#), [Cautionary tales for privacy compliance from Hong Kong's Privacy Commissioner](#), [Fake reviews and 'hidden' online fees to be banned under new digital markets and consumer protection rules](#).

## CONTACT



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



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



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



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



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



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



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