SLAUGHTER AND MAY/

DATA PRIVACY NEWSLETTER
MARCH 2025
ISSUE 27

DATA PRIVACY

SELECED LEGAL AND REGULATORY DEVELOPMENTS IN DATA PRIVACY

QUICK LINKS

EDITORIAL

Writing this newsletter in the spring sunshine, I have been reflecting on the fact that we have seen a welcome increase in regulatory collaboration and alignment since our last edition.

While global leaders have been struggling to reach a collective position on some high-stakes issues in recent months, the privacy community seems to be having more success. For example, to coincide with the AI Action Summit in Paris the data protection authorities (DPAs) from the UK, France, Australia, South Korea and Ireland signed a joint statement committing to collaborate and share best practice to build a trustworthy data governance framework for AI (discussed further in this blog).

We are also seeing welcome signs of increasing collaboration between digital regulators across the economy, with the Information Commissioner's Office (ICO) entering into a memorandum of understanding with the UK Competition and Markets Authority on the operation of the Digital Markets, Competition and Consumers Act (discussed in this blog) and offering to spearhead an expansion of the existing cross-regulatory Innovation Advice service in its letter setting out pro-growth plans to Government (discussed here).

There are also encouraging signs that data privacy regulators are seeking to develop their guidance and regulatory positions in closer collaboration with industry. For example, when the ICO published the response to its generative AI consultation in December, it outlined the input received from stakeholders and reflected how those views had shaped its policy positions (see this blog). Similarly, the French DPA, the CNIL, reflected that it had worked with industry in developing its latest AI guidance on transparency and data subjects' rights (discussed here).

While organisations and practitioners will welcome regulatory collaboration as facilitating more effective and consistent regulation, we should also note that in some cases, thinking of the recent announcement of the European Data Protection Board (EDPB) AI enforcement task force and 'fast response team', it may result in the pooling of resources and sharper regulatory focus on non-compliance.

It is also worth acknowledging that data privacy does not exist in a vacuum with headwinds from the US political change starting to blow over Europe, causing perennial questions around US data transfers and the viability of the EU-US Privacy Framework to start reappearing like the daffodils in my garden. Our team has been considering the impact of these issues and reflecting on them in our recent webinar on the Tech Regulation Landscape (available here).

Do let us know if you have any questions on these issues or any others in the newsletter.

Regards,

Rebecca

Rebecca Cousin, Partner

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

LEGAL UPDATES

Data (Use and Access) Bill progresses

The Data (Use and Access) Bill (Data Bill) is continuing its passage through Parliament and is expected to received Royal Assent by the summer. The Information Commissioner has issued an updated response to the Data Bill, reflecting discussion and amendments made during the Bill's passage through the House of Lords (where it was introduced). For example, the Information Commissioner supports the inclusion of a new provision to allow charities to rely on the soft opt-in (as an alternative to explicit consent) for sending digital marketing and welcomes the Government's commitment to require the ICO to produce two new codes of practice on automated decision making and AI, and on ed-tech. See also our November 2024 newsletter for further background on the Data Bill.

CASE LAW UPDATE

High Court finds against Sky Betting and Gaming and emphasises consent standard

The High Court has found that Bonne Terre Ltd trading as Sky Betting and Gaming (SBG) breached data protection law by sending personalised advertising to a vulnerable individual, who was a problem gambler. The High Court found that SBG lacked a lawful basis for the processing of the claimant's personal data, including the use of cookies and detailed profiling to facilitate personalised advertising. The High Court held that because of his vulnerabilities, the claimant was unable to give valid consent as his autonomy was compromised. However, the judge emphasised that the decision was made on the specific facts of the case and that subsequent cases may find different outcomes. We discuss this case further, including its impact on organisations' consent procedures, in this blog.

Court of Appeal rejects Doorstep Dispensaree appeal against ICO penalty

The Court of Appeal has rejected the appeal filed by Doorstep Dispensaree Limited (DDL) in November 2023, in relation to the ICO's 2019 penalty (discussed in our previous newsletter and client briefing). The Court of Appeal judgment clarifies that the First-tier Tribunal (FTT) was correct to consider the views of the Information Commissioner as an expert, alongside making its own primary findings. The judgment also confirms that the burden of proof in an appeal against an ICO penalty notice lies with the appellant, rather than the ICO as the claimant contested.

In further good news for the regulator, the Upper Tribunal has granted the Information Commissioner permission to appeal the FTT's 2023 judgment that overturned the ICO's £7.55 million penalty against Clearview (discussed in this blog). A date for the hearing is yet to be set.

Data privacy mass claim update: Prismall action defeated in the Court of Appeal

Confirming the position in Lloyd v Google and the significant hurdles for UK mass data claims (discussed here), Andrew Prismall's representative claim against Google and DeepMind on the basis of misuse of private information (MOPI) has suffered defeat in the Court of Appeal. The High Court previously rejected the claim on the basis that on a "lowest common denominator" analysis not every member of the class held a viable claim (discussed in our July 2023 newsletter). The Court of Appeal agreed with the High Court and suggested that representative claims for MOPI would always be "very difficult to bring", as it is necessary to consider the facts of each individual claimant's circumstances to determine whether they have a 'reasonable expectation of privacy', as required for all the members of the class to meet the 'same interest' requirement under CPR 19.8.

Spotlight on DSARs

There have been a suite of recent legal developments in relation to data subject access requests (DSARs) across the UK and the EU:

- in Ashley v HMRC, the High Court found that HMRC's approach to defining personal data in a DSAR response was too narrow and determined that just because the DSAR was directed to specific individuals in a particular part of HMRC, the request's scope was not limited to those people or that part of the organisation; and
- in the EU, the EDPB has published the results of its Coordinated Enforcement Framework action on the right of access that took place throughout 2024 and involved coordinated investigations into DSAR compliance by 30 DPAs, as well as a case digest on DSAR cases that have been decided under the EU GDPR's one-stop-shop mechanism.

We discuss these recent DSAR developments in more detail alongside key learnings for organisations in this blog.

Update from the CJEU

Recent months have seen some significant cases from the CJEU on data privacy:

- Case T-354/22 has placed fresh emphasis on international data transfers and non-material damages under the GDPR, with the CJEU finding the EU Commission liable to pay a German citizen €400 for transferring his personal data to the United States without putting adequate safeguards in place, in the period between the invalidation of the EU-US Privacy Shield and the instigation of the new EU-US Data Privacy Framework (DPF). This case is attracting focus, particularly as concerns about the viability of the DPF surface following the recent removal of Democratic board members from the Privacy and Civil Liberties Oversight Board, which plays an important role under the DPF.
- In case C-394/24, the CJEU has confirmed that it is not necessary to collect the prefix of a customer (Mr, Mrs, Miss etc.) in relation to the purchase of train tickets. The decision arose after the French DPA received a complaint that rail provider SNCF was requiring customers to provide such prefixes when buying tickets. The CJEU found the processing of the prefix data was contrary to the principle of data minimisation and that neither the contract nor legitimate interests lawful basis could be relied upon for the processing, as the information was neither “objectively indispensable" as required for the contractual basis nor necessary, as required for legitimate interests.
- The CJEU has also issued guidance on the calculation of GDPR fines against subsidiaries. In case C-383/23 the court confirmed that group turnover should be used in line with the definition of an “undertaking” found in competition law, in determining both the maximum potential fine level and the actual amount of the fine for the specific infringement. We consider the decision in more detail in this blog.

REGULATOR GUIDANCE

KEY REGULATOR GUIDANCE	
ICO	
Tech Horizons Report 2025	February 2025
Employment practices and data protection: keeping employment records (final version)	February 2025
Guidance on consent or pay (final version)	January 2025
ICO consultation on the draft updated guidance on storage and access technologies (consultation closes on 14 March 2025)	December 2024
ICO response to the consultation series on generative AI	December 2024
ICO consultation on the revised approach to public sector regulation (consultation closed on 31 January 2025)	December 2024
Guidance on sharing personal information when preventing, detecting and investigating scams and frauds	November 2024
EDPB	
Statement 1/2025 on Age Assurance	February 2025
Guidelines 01/2025 on Pseudonymisation (consultation closed on 28 February 2025)	January 2025
Position paper on interplay between data protection and competition law	January 2025
Coordinated Enforcement Action, implementation of the right of access by controllers	January 2025

EDPB (continued)	
AI: Complex Algorithms and effective Data Protection Supervision (project)	January 2025
Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models	December 2024

UPDATES FROM THE ICO

ICO issues new guidance on consent or pay

Following its call for views last year, in January the ICO issued finalised guidance on consent or pay models (these are models which give customers a choice between consenting to advertising cookies when accessing a product or service, paying to access it or walking away). The new guidance confirms that consent or pay models can be compliant with data protection laws provided they offer users with a genuine free choice. The guidance outlines four criteria organisations should consider when assessing whether consent is "freely given", which are (in summary): whether there is a power imbalance between the organisation and the individual; whether the fee is set at an appropriate level; whether the organisation offers a core product or service which is essentially the same across both options; and whether the organisation has complied with its privacy by design obligations. We discuss the guidance and each of these criteria in more detail in this blog.

New cookies guidance published by ICO for consultation

The ICO has published new cookie guidance which it has renamed guidance on the use of "storage and access technologies" to emphasise its broad application to all tracking technologies. The guidance clarifies the application of the PECR rules to non-cookie tracking technologies (including fingerprinting, scripts, tags and link decoration), and offers new guidance on some issues, including how consent mechanisms should be presented and operated. The new guidance forms part of the ICO's online tracking strategy, announced in January, which confirms the ICO will be expanding its recent cookie enforcement focus to consider the compliance of the UK's top 1000 websites. Our recent blog discusses the guidance in more detail, as well as the ICO's approach to enforcement in this area. We will shortly be publishing a full briefing on these developments and the outlook for digital marketing compliance in 2025.

Data sharing to detect fraud/scams

In November, the ICO published new guidance aimed at private firms that share personal data to support efforts to reduce fraud and scams, such as in financial services and telecommunications. The guidance reiterates that neither the UK GDPR nor the Data Protection Act 2018 prevents the sharing of information where it is to limit harm, but that it is important to ensure this is done responsibly and in compliance with the data protection principles.

UPDATES FROM THE EDPB

New guidance on pseudonymisation published for consultation

The draft guidance on pseudonymisation published by the EDPB in January addresses the question of what information amounts to personal data. The guidance confirms that pseudonymised data which is shared with a third party is still personal data if someone else, including the original controller, has the ability to reidentify it. Interestingly though, a subsequent CJEU Advocate General decision (in EDPS v Single Resolution Board C-413/23 (SRB)) has called this position into question (as discussed in our recent blog). It is clear the law in this area is still developing, with a final decision in the SRB case and a final version of the pseudonymisation guidance yet to come. The EDPB's new guidance on anonymisation is also expected this year, according to the EDPB's 2024-2025 work plan. We examine the new pseudonymisation guidance in this blog.

EDPB publishes opinion on certain aspects of processing personal data in AI models

Responding to a request by the Irish DPA, the EDPB has published Opinion 28/2024 addressing certain questions relating to the processing of personal data in AI models. The Opinion clarifies that not all models trained on personal data are considered to be anonymous and suggests how DPAs should determine if they are truly anonymous, including by assessing how likely it is for the data to be extracted and the means reasonably likely to be used for doing so. The Opinion also covers the use of legitimate interests in the context of AI model training, as well as the ripple effects unlawful use of personal data can have on model deployment. We discuss the Opinion in more detail in this blog.

ICO ENFORCEMENT OVERVIEW

While the last four months have not seen any GDPR fines from the ICO, the regulator has made a number of public statements on its enforcement approach:

- The ICO has announced it will continue with the public sector approach it has trialled over the last two years, which has seen the regulator focus on using non-fining powers (such as warnings and reprimands) and reduce the level of fines issued to public sector organisations "so victims of a data breach are not being punished twice in the form of reduced budgets for vital public services".
- As part of its online tracking strategy, the ICO has said that it is in the process of investigating potential non-compliance in the data management platforms that connect online advertisers and publishers.
- The ICO has also confirmed that it has been working with social media platforms to bring about changes to how they process the personal data of children and has now launched formal investigations into TikTok, Reddit and Imgur in this context.

EU GDPR ENFORCEMENT OVERVIEW

The table below sets out a selection of the most substantial EU GDPR fines brought by European data protection supervisory authorities (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
DPC (Ireland)	Meta	€251 million	19 December 2024	Data security
Garante (Italy)	OpenAI	€15 million	20 December 2024	Data security
AP (Netherlands)	Netflix	€4.75 million	26 November 2024	Individuals' rights
Garante (Italy)	Foodinho (in Italian)	€5 million	22 November 2024	Lawful basis
Tietosuojavaltuutetun toimisto (Finland)	Posti	€91 million	13 November 2024	Individuals' rights

Irish DPA fines Meta €251 million following 2018 data breach

The Irish DPA has announced the final decisions from two investigations resulting from a data breach in 2018 that impacted 29 million Facebook accounts globally. Meta Platforms Ireland Limited (Meta) received the €251 million fine after the DPA faced no objections from other concerned EU DPAs. The first decision addresses Meta's failure to provide sufficient information in its breach notification, with the second decision focusing on infringements of the GDPR's data protection by design and default requirements. The full decision notices are awaited. Meta is expected to appeal.

Italian DPA fines OpenAI €15 million for ChatGPT breaches

OpenAI has received a €15 million fine from the Italian DPA, for breaches of data protection law in connection with its ChatGPT tool. As well as identifying a failure to notify the DPA of a data breach in March 2023, the Italian DPA identified a number of infringements including a lack of legal bases for the training of ChatGPT and for violations of the GDPR's transparency principle. Alongside the financial penalty, OpenAI is required to carry out a six-month information campaign to raise public awareness around how their data will be used and ways they can oppose their data being used to train AI models. It follows an investigation which began in March 2023 and saw ChatGPT temporarily banned in Italy. The Italian DPA has also recently blocked access to the Chinese AI tool DeepSeek in the country (we discuss this further in this blog).

VIEW FROM … SWITZERLAND

Contributed by Clara-Ann Gordon, Partner, Niederer Kraft Frey, Switzerland

With the revision of the Swiss Federal Data Protection Act (FDPA), which came into force on September 1, 2023, the legislator has extended the protection of personal data, essentially aligning it with the level of protection provided by the EU GDPR and the UK GDPR. However, despite the FDPA's alignment with GDPR standards, a certain "Swiss finish" still remains in a few areas. Here are some of the key differences:

Topic	Revised FDPA	EU GDPR and UK GDPR
Scope of application	The FDPA has a broad territorial scope, as it even applies to all foreign controllers who process personal data abroad, as long as this processing has a relevant effect in Switzerland. It is even sufficient that only the server is operated in Switzerland or that the data subjects are located in Switzerland.	Applies to the processing of personal data of individuals within the EU/UK (as relevant under the EU GDPR or UK GDPR regime) where the controller/processor is established in the EU/UK or, if not, where the processing activities relate to the offering of goods or services to, or monitoring the activities of, data subjects within the EU/UK.
Data breach notification	Controllers are obliged to inform the Federal Data Protection and Information Commissioner (FDPIC) of a data breach "as soon as possible" when it is likely to result in a high risk to the data subject's personality or fundamental rights.	Data breach notifications must be made to the relevant supervisory authority without undue delay and within 72 hours where a breach is likely to pose a risk to the rights and freedoms of data subjects.
Obligation to appoint a data protection officer	No formal obligation to appoint a data protection officer for private controllers.	Duty to appoint a data protection officer in specific scenarios, including by private sector controllers.
Profiling	The FDPA does not stipulate that consent is required for profiling in general. Consent is only required in the case of "high-risk" profiling.	Data subjects have a right not to be subject to automated decisions, including those based on profiling, that have legal or other significant effects on them. Such decisions can only be taken with the explicit consent of the data subject, or where necessary to the contract between the data subject and controller or required by law.
Sanctions	Intentional violations of the FDPA by individuals acting on behalf of private controllers may result in criminal sanctions in the form of personal fines of up to CHF 250,000. This is the case e.g. if no data processing agreement is concluded or if the countries abroad are not made identifiable to the data subject, etc. The individuals, who are exposed to the fines are those, who committed the breach and those who had the obligation and the power to prevent the breach or at least mitigate its consequences but failed to do so. Only if the responsible persons within a company cannot be identified with reasonable effort and the expected fine does not exceed CHF 50,000, it is possible to impose a fine on the company instead.	Depending on the nature of the violation, sanctions include fines of up to €20 million (under the EU GDPR, £17.5 million under the UK regime) or 4% of annual global turnover, whichever is higher.

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: Excluding anticipated profits and savings: EE v Virgin Mobile, AI in recruitment: ICO publishes recommendations, Navigating Türkiye's updated international data transfer rules: What you need to know, Will you have to report paying a ransom? New UK rules proposed and New UK AI plans: Labour throws its hat into the AI ring.

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.
For further information, please speak to your usual Slaughter and May contact.

www.slaughterandmay.com