

DATA PRIVACY

SELECTED LEGAL AND REGULATORY DEVELOPMENTS IN DATA PRIVACY

QUICK LINKS

[LEGAL UPDATES](#)[CASE LAW UPDATE](#)[REGULATOR GUIDANCE](#)[UPDATES FROM THE ICO](#)[UPDATES FROM THE EDPB](#)[ICO ENFORCEMENT OVERVIEW](#)[EU GDPR ENFORCEMENT OVERVIEW](#)[VIEWS FROM ... SOUTH EAST ASIA](#)[THE LENS
DATA PRIVACY AT
SLAUGHTER AND MAY](#)

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

It was fantastic to see so many of you again in person at our Data Privacy Forum in December. We greatly enjoyed sharing experiences and insights with you, as well as hearing from Claudia Berg, the ICO's GC, talking about DP enforcement. That said, it feels like the Forum was a long-time ago, with the days now lengthening and Spring showing signs of arrival, and on the DP front there has been substantial movement on many of the Forum topics - there is never a quiet time in the world of data privacy as you all know!

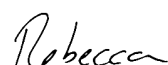
A key development is that the Government has brought the Data Protection and Digital Information Bill back to Parliament. While this version brings some business-friendly changes, it doesn't go as far as we had hoped to address challenges with the current GDPR, but we don't have any real hope of any material improvements.

International transfers continue to be a challenge, as ever, and whilst the ICO's new guidance on Transfer Risk Assessments and its updated international transfers guide shows a pragmatic approach, there continues to be divergence in interpretation with the EU DPAs, with the Norwegian DPA stating that Google Analytics is non-compliant with the GDPR's transfer rules and the Portuguese DPA [citing](#) international transfers as one of the breaches that led to it imposing a €4.3 million fine on the country's National Statistics Institute. This divergence in approach continues to produce challenges but also opportunities, with some organisations saying that they will follow the ICO approach for their EU transfers: given that strict compliance with the EU approach is near on impossible for many, they see the ICO interpretation as a sensible risk-based interpretation.

We are also starting to see the impact of John Edwards having taken the helm at the ICO at the start of last year, in particular with a move towards transparency and a shift in the ICO's enforcement approach and focus. This was clear when John Edwards spoke at the recent IAPP Data Protection Intensive event in London where he emphasised that he was regulating for outcomes. It is also clear that he is looking to improve their enforcement process more generally to avoid the lengthy process and now inevitable appeals. We get the impression that he is going to bring some rigour to the ICO's approach which should aid greater certainty in its findings.

I couldn't conclude without mentioning the enforcement actions against Meta. These decisions have importance beyond the 'Big Tech' field and emphasise the differences in enforcement approach between the various EU DPAs and wider challenges with the EU GDPR's 'One-Stop-Shop'.

We look forward to catching up soon to discuss these and other developments.



Rebecca Cousin, Partner

LEGAL UPDATES

UK data privacy reform progresses

On Wednesday 8 March, the Government [introduced](#) the [Data Protection and Digital Information \(No. 2\) Bill](#) to Parliament, containing the Government's latest data protection reform proposals. This ended months of uncertainty after the original proposals were paused in September last year. The new proposals replace the previous version of the legislation (and restart the Parliamentary process at first reading stage again). While the new Bill mostly mirrors the previous version, it does contain some amendments including loosening the requirements for records of processing activities and in relation to automated decision making, amongst others. We understand that the Government expects the Bill to receive Royal Assent in no more than a year, and, they believe, with minimal amendment. We discuss the proposals in more detail in our [blog](#).

UK's first data adequacy regulation comes into effect

The UK [announced](#) a data adequacy regulation for South Korea on 23 November 2022, marking the UK's first independent adequacy assessment since leaving the EU. The regulation has since come into effect (on 19 December), facilitating data flows between the UK and South Korea. The UK's announcement follows the EU's adoption of an [adequacy decision](#) for South Korea in December 2021. However, the scope of the UK's adequacy regulation for South Korea is broader than the EU's decision, particularly in relation to the sharing of credit information, so warrants separate consideration.

EU Commission publishes draft US adequacy decision

As discussed above, the process to adopt a new partial adequacy decision to facilitate EU-US data flows has gained momentum since our last newsletter ([here](#)). The EU Commission [published](#) a draft adequacy decision for the US on 13 December 2022, launching the process towards its adoption. The European Data Protection Board (EDPB) has recently delivered its [opinion](#) on that draft decision, welcoming substantial improvements since the previous Privacy Shield version (that was invalidated by the Schrems II case in 2020, discussed in our [blog](#)) such as the introduction of new necessity and proportionality requirements for public agencies accessing personal data and new redress mechanisms for EU data subjects. However, the EDPB expressed some continuing concerns, including in relation to onward transfers of data and has called on the EU Commission to closely monitor the implementation of the new US legal framework that underpins the adequacy decision. The adoption process for the new EU-US adequacy decision is expected to be completed by the summer.

CASE LAW UPDATE

First-Tier Tribunal rules on Experian appeal against ICO

The First-Tier Tribunal (Information Rights) (FTT) [has issued](#) its judgement in Experian's appeal against the ICO's [October 2020 enforcement decision](#) that had required substantial changes to how the organisation handled personal data (covered in our [previous newsletter](#)). While the FTT endorsed the ICO's position on some issues, including in relation to the provision of privacy notices to individuals whose information was obtained from publicly available sources (and accordingly, supported a narrow reading of the Article 14(5) 'disproportionate exemption'), they sided with Experian in several important areas. For example, they disagreed with the ICO's findings in relation to the sufficiency of Experian's privacy notice and recognised, pragmatically, the challenges faced by organisations in drafting such notices, stating "there is a tension between providing large amounts of information on the one hand with the aim of improving transparency and accessibility of information and on the other the resultant information overload [...]". Significantly, the FTT also found in favour of Experian in relation to their legal basis for processing for direct marketing purposes, concluding they could rely on legitimate interests. In a [statement](#) following the decision, the ICO indicated that it was considering whether to appeal and the Information Commissioner has since indicated that the regulator will seek to do so.

CJEU issues significant ruling for DPOs

The Court of Justice of the European Union (CJEU) [has issued a decision](#) that considers the meaning of conflicts of interests in Article 38(6) GDPR. The data protection officer (DPO) in the case had also been the chairman of the company's work council. The court held that it falls to the controller/processor not to give the DPO other duties that could impair the execution of their DPO role and explained that there may be a conflict where a DPO is given other duties which result in them deciding the controller's objectives or methods for processing personal data. Whether there is a conflict should be determined on a case-by-case basis by national courts, in light of all relevant circumstances. This includes the organisational structure of the controller/processor and the policies they have in place. The case also considered the interaction of national laws (in EU Member States) and Article 38(3), on the dismissal of DPOs, finding that the GDPR does not preclude national laws in this area, as long as they do not undermine the GDPR's objectives.

REGULATOR GUIDANCE

KEY REGULATOR GUIDANCE	
ICO	
Tech Horizons Report	December 2022
Updated international transfers and transfer risk assessment guidance and tool	November 2022
EDPB	
Guidelines 07/2022 on certification as a tool for transfers	February 2023
Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them (final version)	February 2023
Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (final version)	February 2023
Report of the work undertaken by the Cookie Banner Taskforce	January 2023

UPDATES FROM THE ICO

ICO updates guidance on international data transfers

The ICO's long awaited guidance on Transfer Risk Assessments (TRAs) was [published](#) in November, alongside a final version of the ICO's TRA tool and further updates to the ICO's international transfers guidance. The ICO's TRA guidance and tool endorses a pragmatic, risk-based approach to risk assessments for international transfers from the UK, enabling organisations to alter the scope of their analysis in light of factors including the quantity and sensitivity of the data being transferred and the size and resources of the organisation making the transfer. The updated guidance also provides helpful clarification about where the responsibility lies for carrying out TRAs - with only the organisation 'initiating and agreeing' to the transfer needing to carry out the TRA (e.g. just the processor in a P2P transfer, rather than their controller too). While these changes may assist organisations (particularly SMEs) making transfers from the UK regime, many organisations operating across the UK and Europe will need to remain aligned with the EU GDPR regime. In recognition of this, the ICO has permitted the continued use of the EU's transfer impact assessment process (outlined in EDPB guidance [01/2020](#)) for UK transfers as an alternative to the UK's TRA approach. We discuss the new guidance in more detail in our November [blog](#).

ICO focuses in on Tech, with Tech Horizons Report and new guidance on AI

The ICO has published its first [Tech Horizons Report](#) examining technologies that present novel and significant implications for privacy in the next two to five years. It focuses on four technologies (consumer healthcare, next-generation Internet of Things, immersive technology and decentralised finance) and highlights areas of concern common to all of them. For example, all the technologies faced issues with transparency as they collect personal data within complex data ecosystems which makes it difficult for people to understand who is processing their information and how it is being processed. The report comes out of the [ICO25 strategy](#) to reduce burdens on businesses, support innovation and prevent harms (discussed in our [July newsletter](#)). The ICO has indicated the Tech Horizon Report will be followed by another report focused on neurotechnology later this spring.

The ICO has also [published](#) new tips outlining how organisations can use AI and personal data in an appropriate and lawful manner. The tips also demonstrate the way regulators are working to understand how to both regulate AI as well as how to use it themselves. We discuss this guidance in our [Lens blog](#).

UPDATES FROM THE EDPB

The EDPB has recently released its [Work Program for 2023-2024](#), setting out their key priorities for the next two years. The Work Program is divided into four pillars, which largely reflect the priorities already set out in its 2021-23 [Strategy](#): advancing harmonisation and facilitating compliance; supporting effective enforcement and efficient cooperation between national supervisory authorities; a fundamental rights approach to new technologies; and the global dimension. New significant pieces of guidance that are expected in 2023-24 include guidance on legitimate interests, anonymisation and pseudonymisation, blockchain and the interaction of the AI Act and GDPR. Final versions of current consultation drafts are also promised, including on the right of access.

One piece of EDPB draft guidance that has already been finalised this year is their [Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers](#). The final version includes a number of new examples and further clarification in some areas, including in relation to the role of processors in particular scenarios (e.g. where an EU processor is subject to a third country legal regime and receives an information access request from an overseas government). We wrote about the draft version of these guidelines in our [previous newsletter](#).

ICO ENFORCEMENT OVERVIEW

ICO's refocuses its approach to enforcement

In a November [speech](#), the Information Commissioner highlighted a new approach to “regulating for outcomes, not outputs”, placing greater emphasis on the ICO’s enforcement tools other than fines, including reprimands. He explained, “the number or quantum of fines is not the measure of our success or failure, nor of our impact. Getting better outcomes, and sharing those stories with the wider economy, can have a much greater effect on the lives and rights of the people of the UK than a fine might”. He confirmed the ICO would be publishing all reprimands issued from January 2022 onwards, unless there is a good reason not to (we considered this “naming and shaming” approach in relation to DSAR enforcement in our October [blog](#)). This approach was reiterated in the Commissioner’s [speech](#) to IAPP London, earlier this month (discussed above). We discuss these developments and trends in ICO enforcement over the last year in our January briefing: [The year in UK GDPR regulatory enforcement action](#).

In the same vein, the ICO [announced](#) in February that it would ease the reporting burden for communications service providers (CSPs), whose strict 24-hour personal data breach reporting deadline under the UK’s Privacy and Electronic Communications Regulations (PECR) will no longer be enforced in trivial cases (which are unlikely to result in a risk to individuals’ rights and freedoms), provided CSPs notify the regulator within 72 hours. We discuss this change in our [Lens blog](#).

EU GDPR ENFORCEMENT OVERVIEW

The table below sets out a selection of the most substantial EU GDPR fines brought by EU 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
Datatilsynet (Norway)	Sats	€900,000	6 February 2023	Legal basis, data subject rights
DPC (Ireland)	WhatsApp IE	€5.5 million	19 January 2023	Legal basis, fairness, transparency
DPC (Ireland)	Meta IE	€390 million (€210 million, Facebook, €180 million, Instagram)	4 January 2023	Legal basis, fairness, transparency
CNPD (Portugal)	The National Institute of Statistics	€4.3 million	12 December 2022	Special category data, international transfers, processor due diligence
Garante (Italy)	Clubhouse	€2 million	5 December 2022	Transparency, legal basis, data retention
DPC (Ireland)	Meta	€265 million	25 November 2022	Data protection by design

The Irish DPA has brought a series of actions against Meta in recent months for breaches associated with its various products:

- in November, it imposed €265 million penalty against Meta, following an enquiry triggered by complaints that collated Facebook user data was publicly available on the internet. The enquiry centred on how Meta had complied with the GDPR's data protection by design obligations. All of the other DPAs agreed with the Irish DPA's final decision. For more information, see the Irish DPA's [press release](#).
- on 4 January, it issued [final decisions](#) against Meta Ireland in respect of its Instagram and Facebook services, centring on transparency and on the choice of legal basis to support its personalised advertising models - it was fined €210 million relating to Facebook, and €180 million with respect to Instagram. Under the EU GDPR's One-Stop-Shop mechanism, there were 47 'Concerned Supervisor Authorities' (CSAs) in this case. All of them broadly agreed with the Irish DPA on Meta's transparency failings, but 10 disagreed with the Irish DPA's view that Meta should be permitted to rely on the 'necessary for contract' legal basis for personalised advertising (as part of its broader services). The dispute was escalated to the EDPB, which ruled that Meta was not permitted to rely on the 'contract' legal basis for that processing. The Irish DPA also increased the level of fine to reflect the EDPB's binding determinations. Meta has confirmed that it intends to appeal against this decision. The EDPB called for a fresh investigation by the Irish DPA into Facebook and Instagram's processing of special category data, which the [Irish DPA has stated](#) it intends to challenge in the CJEU as an overreach by the EDPB (for more information, see the Irish DPA's [press release](#)).
- in a separate judgment, on 19 January, it fined WhatsApp IE €5.5 million for GDPR failings in relation to its transparency and lawful basis for processing. As with the previous Meta fine, the Irish DPA could not agree with other CSAs about whether WhatsApp could rely on the 'necessary for contract' basis. As before, the dispute was escalated to the EDPB, who held that WhatsApp was not permitted to rely on the contract basis. The EDPB again

called for the Irish DPA to investigate WhatsApp's processing of special category data, which the Irish DPA intends to challenge. For more information, see the Irish DPA's [press release](#).

[The CNIL issues fines against Apple, Microsoft, and TikTok for cookies infringement](#)

At the end of 2022 the French DPA, the CNIL, issued three major fines for breaches involving failures to gain consent from users for advertising cookies, using fining powers available to the regulator under French e-privacy laws (outside the remit of the GDPR's OSS). [Microsoft](#) was fined €60 million with a potential further potential penalty of €60,000 a day, if it failed to collect consent from all French users of 'bing.com' within three months. Smaller fines were also issued against [Apple](#) (€8 million), as well as [TikTok](#) (€5 million). The CNIL was one of the DPAs that formed the EDPB's Cookie Banner Task Force, following hundreds of complains being lodged with 18 DPAs by the campaign group NOYB. The Cookie Banner Task Force has now adopted a [report](#) on the work carried out by the grouping.

VIEWS FROM... SOUTH EAST ASIA

Contributed by Alexander Yap, Partner, Eugene Ho, Partner, Oene J. Marseille, Partner, Aris Budi Prasetyo, Partner, Oh Hsiu Hau, Partner and Tran Thi Thanh Truc of Allen & Gledhill.

[Singapore allows data protection claims for emotional distress](#)

The right of private action under Singapore's comprehensive data protection law, the Personal Data Protection Act 2012 ("PDPA") is available to claimants who have suffered pecuniary losses and other heads of loss recognised at common law. In addition, following a recent case in Singapore's highest court, the Court of Appeal, *Michael Reed and Alex Bellingham and Attorney-General (Intervener)*, a claimant who suffers emotional distress directly due to a PDPA breach may now also be able to obtain damages and/or an injunction.

However, the data protection risk profile for organisations in Singapore has likely not materially increased. The test for emotional distress is nuanced, allowing consideration of a multitude of factors, merely suffering emotional distress may not result in liability. In the case, the defendant unreasonably refused to furnish an undertaking not to further misuse personal data, and behaved in a dismissive manner in relation to data protection concerns made explicit by the claimant.

[Financial penalties enhanced in Singapore](#)

For breaches of PDPA data protection obligations which occur from 1 October 2022, the maximum financial penalty which the Singapore Personal Data Protection Commission can impose has increased from the previous S\$1 million (roughly £615,000) to 10% of an organisation's annual turnover in Singapore if the organisation's annual turnover in Singapore exceeds S\$10 million (equivalent to around £6 million).

[Indonesia's comprehensive personal data protection law enacted](#)

Law No.27 of 2022 on Personal Data Protection ("PDP Law") was effective from 17 October 2022 and is Indonesia's first comprehensive law on personal data protection.

Some key provisions:

- the PDP Law applies to every organisation that carries out acts regulated under the PDP Law which are carried out within Indonesia or which are carried out outside Indonesia but which have legal consequences either within Indonesia and/or the data subjects are Indonesian citizens wherever they are located in the world;
- processing of specific personal data (e.g., health data, genetic data, and financial data) requires an additional risk assessment to be conducted by data controllers;
- there are six permitted legal bases for collecting and processing personal data, namely: (i) express consent from the data owner; (ii) obligations under contracts to which the data owner is party; (iii) legal obligations of the data owner under applicable regulations; (iv) protection of the data owner's vital interest; (v) duties in the

interest of public service or implementation of the authority of the data controller based on the applicable law; and (vi) other legitimate reasons;

- nine rights are granted to data subjects: the right to be informed, the right to rectification, the right to erasure, the right to access, the right to object, rights in relation to automated decision making and profiling, the right to revoke provided consent and the right to limit personal data processing; and
- the PDP Law also sets out requirements for data controllers on, among other things, data breaches, cross-border data transfers and data protection officers.

Whilst there is a two-year transitional period from 17 October 2022, it is likely that all provisions/obligations, to the extent possible, are immediately applicable and effective. The transitional period should therefore be interpreted as a period for the relevant data privacy actors to comply with and make necessary adjustments before the relevant authorities begin imposing serious sanctions and so organisations should start working towards compliance now.

Draft decree on personal data protection of Vietnam issued

In February 2021, the Ministry of Public Security in Vietnam issued a draft decree on protection of personal data (the “Draft DPDP”), intended to be Vietnam’s first comprehensive law on personal data protection. The Draft DPDP is still in a consultative stage.

Key provisions based on the current draft:

- it covers all Vietnamese citizens’ personal data regardless of whether it is processed onshore or offshore;
- there are separate definitions and requirements for “basic” versus “sensitive” personal data;
- prior consent from the data subjects is a basis for collection and processing of personal data. Consent is only effective if opt-in, voluntary and specified information is provided;
- exceptions apply, for example, use: (a) in accordance with applicable laws; (b) for national and public security; (c) for emergencies when the freedom and health of the data subjects or the general public is threatened; (d) for the investigation of any legal violations; (e) for research statistics collection; and (f) other circumstances as required by Vietnamese law and international treaties;
- rights of data subjects include rights to: (i) grant consent or object; (ii) be informed; (iii) access and rectification; (iv) revoke any provided consent; (v) limit processing; (vi) complain; and (vii) request compensation;
- before sensitive personal data is processed, those considered processors under the Draft DPDP must obtain consent from the data subjects and register such processing; and
- administrative sanctions may be applicable.

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: [How would you like to pay? Moving towards the digital pound](#) and [UK and US Governments crack down on ransomware criminals](#).

DATA PRIVACY AT SLAUGHTER AND MAY

We advise on all aspects of data privacy compliance across the world. This ranges from ad hoc GDPR compliance issues from UK, EU and non-EU businesses to complex global data risk strategic advice. We regularly advise on data breaches; data protection issues arising in commercial and M&A transactions, global investigations and pension scheme arrangements; the privacy implications for tech such as blockchain or AI; individuals' rights; and data sharing agreements, from simple processor agreements to more complex data pooling arrangements and large strategic sourcings. Our global data privacy team comprises six expert partners, supported by several associates and professional support lawyers who specialise in this area. As data privacy issues affect all areas of a business, we train all of our other lawyers to advise on these issues within their practice areas. For more complex or novel queries, our specialist cross practice data privacy team can provide the necessary expertise and support.

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
Data Privacy PSL
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, 2022.
For further information, please speak to your usual Slaughter and May contact.

www.slaughterandmay.com

580665402