

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](#)

[VIEWS FROM THE MIDDLE EAST](#)

[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

Developments in the data privacy world have continued apace in the last few months. While we covered some of them at our Data Privacy Forum in December, there has been a raft of significant announcements since.

There has been some welcome recent progress on international transfers from the EU and UK, although significant complexity and uncertainty remains. In particular, the recent announcement of a US-EU transatlantic deal to replace the Privacy Shield will be a huge relief for businesses given the current difficulties with transfers to the US. It is hoped that the UK will soon follow suit with an equivalent agreement. In the meantime, the ICO has provided us with further certainty with the finalised International Data Transfer Agreement (IDTA) and the [Addendum](#) to the EU SCCs (discussed further below), although the ICO's final guidance on TRAs is still awaited.

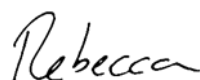
Change is potentially afoot at the ICO as well, with the newly appointed Information Commissioner, John Edwards, [opening](#) a major 'listening exercise' to receive feedback from organisations and individuals about their experiences of engaging with the regulator. On enforcement approach, John Edwards said, at a recent IAPP conference, that the ICO will adopt a surgical and targeted approach to fines, focussing on the greatest harm. This builds on the current enforcement trends seen in the enforcement action we discuss later in this newsletter.

At an EU level, we are seeing fines on a wide range of areas of privacy compliance, from cookies in France to accountability and legal bases for processing in Ireland, among (many) others. Some regulators are enforcing the rules on international transfers, with the Austrian and French DPAs acting on transfers made via Google Analytics, with other DPAs lined up to follow suit, after the issue was brought to their collective attention by privacy campaign group NOYB.

At a global level, there continues to be a steady increase in the countries passing or amending DP laws. One example is in the Middle East, as we discuss in our 'Views from...' section.

In terms of scanning the direction of travel for data privacy law, we await the UK Government's response to the DCMS' 'Data: a new direction' consultation which was initially promised for Spring of this year. The UK Government has also, perhaps optimistically, promised us a number of adequacy regulations by the end of 2022. We are also expecting some developments in the field of AI, with a White Paper planned from the government, and the ICO due to report back on the beta version of its AI toolkit.

I look forward to discussing these developments and catching up with you in the coming months.



Rebecca Cousin, Partner

LEGAL UPDATES

Spotlight on adequacy

On 25 March, the EU and the US announced an agreement in principle for the successor to the US Privacy Shield that was invalidated by the 2020 Schrems II case, with the new arrangement to be known as the “Trans-Atlantic Data Privacy Framework”. Although much of the detail of the new arrangement remains to be finalised/publicised, the progress towards a partial EU-US adequacy decision that would remove the need for the use of standard contractual clauses and the practically challenging ‘transfer impact assessments’ for transatlantic data transfers has been widely welcomed. We discuss the agreement in more detail in [this blog](#).

Meanwhile, the UK Government has confirmed that its own separate negotiations for an adequacy assessment for the US are ‘progressing well’. It has also announced that it hopes to have finalised the adequacy assessments for its ‘priority countries’ of Australia, Colombia, Dubai, Republic of Korea, Singapore and the US (discussed in our [November newsletter](#)) by the end of 2022.

We discuss more international data transfer developments from the UK and EU in the Regulator Guidance section below.

CASE LAW UPDATE

Post-Lloyd Developments

The Lloyd v Google decision, which we discuss in detail in our [blog post](#), was expected to stem the flow of representative actions (i.e. ‘opt-out’ actions) for data privacy breaches. However, it may not be the complete end to such actions as the group [claim against TikTok](#), brought by the ex-Children’s Commissioner Anne Longfield, has recently been successful in dealing with the first procedural hurdle, with the claimant being granted permission to serve proceedings on defendants outside the jurisdiction. The claimant argued that the claim differed from Lloyd v Google as this action had better chances of avoiding the need for assessment of each individual case, better prospects of getting over the de minimis threshold (even on lowest common denominator basis), is concerned with a different class of claimants, and involved a different and more intrusive type of data processing. The Defendants have applied for summary judgement in the case, with a hearing expected later this year.

Despite the TikTok claim progressing, many class actions (both opt-in and representative actions) are settling out of court as the full impact of Lloyd v Google becomes apparent. For example, a representative claim against Google and Deepmind in relation to their 2015 data sharing agreement with the Royal Free hospital in London, under which Google obtained personal data of 1.6 million individuals without consent, has recently been settled; and Ticketmaster has reportedly settled a mass opt-in claim in relation to its 2018 breach, with no admission of liability. The company’s court appeal against its ICO’s fine (of £1.25 million in relation to the same breach) was stayed pending the outcome of the opt-in claim (as discussed in our [July 2021 newsletter](#)), but is likely to now progress.

ICO enforcement actions under scrutiny

The ICO’s decision-making and procedures are under increasing scrutiny with many recipients of UK GDPR penalties from the regulator choosing to appeal against them in court. For example, the First Tier Tribunal has recently heard the appeal of the credit reference agency Experian in relation to their 2020 [ICO enforcement notice](#). This enforcement action followed from the ICO’s investigation into direct marketing practices in the data broking sector. Experian’s counsel (Anya Proops QC of 11KBW) argued that the ICO’s enforcement action was “grossly disproportionate” and has also commented that ICO’s attitude towards transparency forces businesses to overload individuals with information that is needlessly detailed. Other ICO actions that are currently being appealed include those against Ticketmaster (discussed above) and the Cabinet Office (discussed below).

In light of the suite of recent appeals, it is notable that in February the [ICO announced](#) that it had reached a ‘pragmatic compromise’ with Somerset Bridge Insurance Services Limited (formerly Eldon Insurance Services Limited). The company had been appealing a fine, an enforcement notice and an assessment notice imposed against it by the ICO in 2019. Following discussions, Somerset Bridge agreed to withdraw its appeal against the monetary penalty and enforcement notices and pay the penalty sum of £60,000 without admission of liability, and to a consensual audit of its data protection practices, while the Information Commissioner, in turn, agreed to cancel its assessment notice.

Soriano v Forensic News LLC

In our [March 2021 article](#) we discussed the implications of the High Court decision in the Soriano case on GDPR's extraterritoriality. The [Court of Appeal](#) has now disagreed with High Court's findings on extraterritoriality and has put forward a broad interpretation of Article 3(1) and (2) of the GDPR, albeit in the context of an application to serve proceedings outside the jurisdiction (meaning the arguments were measured against the standard "of a real as opposed to a fanciful prospect of success in the claim"). Lord Justice Warby recognised that these issues needed further 'definitive consideration' and suggested the ICO should be invited to intervene in proceedings.

Despite the more limited context, a number of interesting arguments were put forward by Warby LJ, including:

- that the 'minimal' establishment standards (Art 3(1) GDPR) were met as 8.9% of the Forensic News readership was in the UK or EU, and some subscribers had paid in pounds or euros. The court also held that the subscriptions constituted a 'stable arrangement', because once a subscription is set, it tends to be maintained over a period of time. The judge's broad interpretation of Art 3(1) GDPR suggests that there may be no requirement for a business to have a physical presence in the UK to satisfy 3(1); and
- that the activities carried out by Forensic News, "assembling, analysing, sorting, and reconfiguring such data, and then publishing the result in articles" constitutes monitoring, which satisfies the requirements of Art 3(2)(b) on the extra-territorial application of the GDPR, and falls under the "behavioural analysis and profiling" concepts of EDPB guidance.

REGULATOR GUIDANCE

KEY REGULATOR GUIDANCE

ICO

Ransomware and data protection compliance (new guidance)	March 2022
Guidance on Video Surveillance (updated)	February 2022
ICO call for views: Anonymisation, pseudonymisation and privacy enhancing technologies guidance (draft - consultation closed on 16 September 2022)	February 2022
ICO publishes responses to its views on employment practice	January 2022
Regulatory Action Policy; Statutory Guidance on our Regulatory Action; and Statutory Guidance on our PECR powers (drafts - consultation closed on 8 March 2022)	December 2021

EDPB

Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them (draft - consultation closes on 2 May 2022)	March 2022
Launch of coordinated enforcement on use of cloud by public sector (15 February 2022)	February 2022
Guidelines 01/2021 on Examples regarding Personal Data Breach Notification (final version - adopted on 3 January 2022)	January 2022
Guidelines 01/2022 on data subject rights - Right of access (draft - consultation closed on 11 March 2022)	January 2022
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 (draft - consultation closed on 31 January 2022)	November 2021

Updates from the ICO

International data transfers

At the beginning of February the ICO laid final versions of the UK's own standard contractual clauses (SCCs), the International Data Transfer Agreement (IDTA) and the International data transfer addendum to the European Commission's standard contractual clauses for international data transfers (the EU Addendum), before Parliament. These came into force on 21 March and can now be used to facilitate international data transfers under the UK GDPR regime. The IDTA is a relatively standalone document while the EU Addendum is to be used alongside the latest EU SCCs to adapt them to provide for UK data transfers. Both sets of new clauses reflect the provisions of the UK GDPR, Brexit and the issues raised by the Schrems II case.

The ICO also updated part of its international transfers guidance to amend the definition of a 'restricted transfer' so it more closely reflects geographical transfers of data and moves away from the concept of the 'GDPR bubble' (incidentally, the position taken in this latest guidance mirrors that of the EDPB in their guidance on the interaction of EU GDPR Article 3 and Chapter V, discussed below). We discuss the new IDTA and EU Addendum and the new guidance in more detail in this [blog post](#).

We are still awaiting final guidance from the ICO on post-Schrems II transfer risk assessments (TRAs), the draft of which formed part of last autumn's consultation, as well as guidance on how organisations should complete the IDTA and EU Addendum. The ICO has indicated that it is still working on the TRA guidance and expects to publish it in the coming months.

ICO anonymisation guidance: Chapters 3 and 4

In accordance with the [ICO's plan](#) of March 2021 to publish its new anonymisation guidance chapter by chapter for consultation to maximise the opportunity for stakeholder comment (as we discussed in our [previous newsletter](#)), the ICO has now published the third and fourth chapters of this guidance:

- the [third chapter](#) focuses on pseudonymisation including what is meant by pseudonymisation, whether pseudonymised data is still personal data; the differences between pseudonymisation and anonymisation and the advantages of pseudonymisation for organisations as well as the offences that are connected to reversing pseudonymisation;
- the [fourth chapter](#) explores accountability and governance in the context of anonymising personal data, for example, it includes discussion of the use of DPIAs to identify disclosure risks as well as the need for the organisations to keep up to date with technical and legal developments in order to ensure anonymisation remains effective. The chapter goes on to offer guidance about related legislation to consider when disclosing anonymous information.

The consultation on these chapters is open until 16 September 2022. The ICO is now intending to publish further chapters before carrying out an additional full consultation on the final document.

ICO seeks feedback on how it uses its powers to investigate, regulate and enforce

In December 2021 the ICO launched a new consultation on its draft enforcement strategy, through the publication of a draft [Regulatory Action Policy](#), draft [Statutory Guidance on the ICO's Regulatory Action](#) and draft [Statutory Guidance on the ICO's PECR Powers](#). Through this consultation the ICO is seeking views on 'how the ICO aims to carry out its mission to uphold information rights for the UK public in the digital age'. The consultation on these documents closed on 24 March. For more detailed discussion of the consultation documents, see our blog post: [RAP \(feat. statutory guidance\): ICO releases draft enforcement strategy for consultation](#).

Updates from the EDPB

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

These [draft guidelines](#) seek to explain the interplay between Article 3 (on the scope and application of the EU GDPR) and the international provisions transfers in Chapter V. It aims to help controllers and processors in identifying whether a processing activity constitutes a transfer to a third country or an international organisation and, as a result, whether they have to comply with the provisions of Chapter V of the GDPR. It makes clear that the GDPR's Chapter V provisions will apply to transfers to non-EU based importers, even where the importer is subject to the EU GDPR due to its extra-territorial effect. Interestingly, the EDPB takes the opposite view where data is sent within an organisation and in that circumstance does not consider that Chapter V applies. As such, the EDPB's position appears to draw a hard distinction between transfers between legal entities in a corporate group and those between branches of the same organisation (although the guidance doesn't specifically reference the concept of branches at all).

ICO ENFORCEMENT OVERVIEW

Royal Mail direct marketing enforcement

The ICO [has fined](#) Royal Mail £20,000 for sending direct marketing messages without individuals' consent following a human error. This was despite the fact that Royal Mail self-reported the incident to the ICO. Royal Mail mistakenly sent out a marketing campaign to 245,850 potential recipients, even though only 30,648 had provided existing and valid consent. Despite the company self-reporting the breach, the ICO held that a monetary penalty should be issued, in part to act as a deterrent for other organisations against non-compliance (and arguably also against voluntary reporting of non-compliance).

Provisional findings against Clearview AI

The ICO [has announced](#) a provisional intention to impose a penalty of just over £17 million on Clearview AI Inc (self-described as "the World's Largest Facial Network") for multiple significant breaches of UK data protection laws. In addition, the ICO has issued a provisional enforcement notice requiring the tech company to stop processing the personal data of UK individuals and to delete any data held about UK individuals. The announcement follows a [joint investigation by the ICO and the Office of the Australian Information Commissioner \(OAIC\)](#). We discussed this action in more detail in our December [blog](#).

Focus on security failings

The ICO [fined](#) the UK Cabinet Office £500,000 after the postal addresses of the 2020 New Year honours recipients were disclosed online. The Cabinet Office has appealed against this enforcement action. See our [blog post](#) for more details.

Criminal solicitors Tuckers LLP was also [fined](#) £98,000 for breaches of its security, and other obligations under the GDPR, which came to light following a ransomware attack. We discuss this action, the ICO's first ransomware fine, in this recent [blog post](#).

ICO's approach to DSARs

Recent ICO enforcement actions in relation to data subject access requests (DSARs) suggest that while the ICO may look to encourage compliance with DSARs it is not an area the regulator is currently focusing on for monetary penalties:

- in January, the ICO served the Ministry of Justice (MoJ) with an [enforcement notice](#) following the MoJ's failure to provide nearly 8,000 data subjects with a copy of their data. The enforcement notice required that the MoJ: (i) takes the required steps to comply with the legislation; and (ii) develops a recovery plan, containing details of how it intends to remedy the issue of the out-of-time subject access requests. No monetary penalty was issued.
- in March, the ICO issued an [enforcement notice](#) against an independent financial adviser, Smith, Law & Shepherds IFA Ltd, for their failure to comply with two DSARs over a nearly two year period, despite multiple interactions with the ICO on the matter. Again, no monetary penalty was issued.

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 (Facebook)	€17 million	15 March 2022	Accountability
Garante (Italy)	Clearview AI	€20 million	10 February 2022	Legal basis for data processing
CNIL (France)	Facebook	€60 Million	6 January 2022	Cookie infringements
CNIL (France)	Google	€150 Million	6 January 2022	Cookie infringements
Garante (Italy)	Enel Energia	€26.5 million	16 December 2021	Insufficient legal basis for data processing
Datatilsynet (Norway)	Grindr	€9.6 million	13 December 2021	Illegal data sharing

Irish DPC reaches agreement on Meta fine

The Irish Data Protection Commission (DPC) [has fined](#) Meta €17 million (£14 million) for multiple breaches of the GDPR's accountability principle (i.e. failing to have measures in place that would enable it to 'readily demonstrate' the security measures it implemented in practice to protect users' data). The Irish DPC reached a consensus on the decision with the other interested DPAs, without the need for the involvement of the EDPB to adjudicate (as happened in relation to last year's WhatsApp decision, discussed in our [previous newsletter](#)).

Cookies in focus

The CNIL, the French DPA, has recently fined [Google](#) a total of €150 million (£126 million) and Facebook €60 million (£50 million) for failing to obtain valid consent for cookies on their respective websites, as the process for users to reject cookies was not as easy as to accept them. The CNIL brought the actions under the French domestic data privacy laws (that implement the EU's ePrivacy Directive), circumventing the application of the EU GDPR's 'one-stop-shop' mechanism. We discuss this action in more detail in our [blog post](#).

VIEWS FROM... THE MIDDLE EAST

With input from Andrew Fawcett and Nick O'Connell, Partners, Al Tamimi & Company

There have been a number of legislative developments in the Middle East in the recent years in relation to data privacy. The influence of the GDPR can be seen in a number of these, alongside the intention of law-makers to support the growth of the digital economy in their territories. We provide a round-up of some of the latest developments below.

New national/federal laws in force

In the UAE, Oman and Saudi Arabia, the first comprehensive standalone laws on data privacy have come into effect this year. In the UAE, the Federal Law on the Protection of Personal Data came into force on 2 January 2022. It introduces the requirement of consent for the lawful processing of a data subject's personal information, alongside controller and processor obligations related to data processing, and general principles including purpose specification and data minimisation. In Saudi Arabia, the Personal Data Protection Law, which regulates the collection and processing of personal information, may have come into force on 23 March 2022, although delays in issuance of the implementing regulations, and an eleventh hour press release announcing the 'postponement of full enforcement' of the new law until 17 March 2023, has created significant uncertainty. The law is the Kingdom's first attempt at a comprehensive, modern data protection regime. While it seems to be a step in the right direction, there are a variety of concerns, including what appear to be heavy restrictions on data transfers. Further movement can be expected in this space, as the

regulations are developed. In Oman, the Law on the Protection of Personal Data, was issued on 9 February 2022 and is expected to come into force in 2023.

Although the new laws in these territories have some similarities with the EU/UK GDPRs, there are also some differences. For example, they are much more focused on consent as a requirement for processing, whereas the EU/UK GDPRs permit processing on other grounds such as the 'legitimate interests' one. Some of the laws contain criminal as well as administrative penalties. The scope for very significant administrative fines, as are available under GDPR, does not feature.

Amendments to, and strengthening of, existing laws

The Israeli Parliament announced on 5 January 2022 that the Privacy Protection Bill, amending the Protection of Privacy Law, had been laid for its first reading. Key amendments would include the requirement of certain companies to appoint a DPO, the introduction of enforcement powers for the Privacy Protection Authority, and refined definitions for key terms to reflect technological developments, in line with the GDPR.

In Qatar, the new Financial Centre Data Protection Regulations were issued on 21 December 2021 to amend the 2005 Data Protection Regulations and Data Protection Legislation. The new Regulations (to come into effect on 21 May 2022) clarify existing provisions and introduce new provisions in line with global developments in data privacy law, including the establishment of: (i) a new Data Protection Office and Data Protection Commissioner; (ii) general principles such as purpose specification, data minimisation and storage limitation, clarifications of the requirement for consent; (iii) new data subjects' rights to data portability and effective judicial remedy against controllers and processors; and (iv) requirements on controllers to implement appropriate technical and organisational measures.

In Bahrain, following several months of public consultations, the Bahrain Personal Data Protection Authority issued ten decisions (essentially, regulations) supplementing and giving effect to several provisions under the Personal Data Protection Law 2018.

Draft laws proposed

A draft Personal Data Protection Law of 2021 is being proposed in Jordan, which would establish a regulatory framework for the maintaining and processing of personal data, as well as a legal framework balancing individuals' rights to personal data protection with technological advances. The draft law is still making its way through the legislative process and may yet be amended.

The data protection landscape in the Middle East is developing rapidly. In limited instances (such as in financial services free zones in the UAE and Qatar) there has been a conscious effort to emulate the GDPR. In other jurisdictions, while there have been efforts to address key concepts typically found in mature data protection legislation, this has not always been done in a manner consistent with what one might find in jurisdictions with sophisticated data protection regimes. Accordingly, it will not be enough to take the view that compliance with the high standards of GDPR will ensure compliance with the requirements in Middle East jurisdictions. We recommend continuing to monitor developments, and obtaining current, on-the-ground advice.

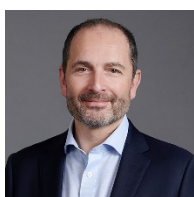
THE LENS

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: [Ransomware attacks: Are you ready? New ICO guidance can help](#); [Another one bites the dust: Further vicarious liability data breach claim fails](#); and [New AI standards hub launched in UK](#).

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.

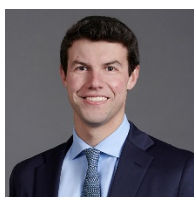
CONTACT



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
Senior PSL and Head of Knowledge -
Data Privacy
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

Document No

576223064