

DATA PRIVACY NEWSLETTER

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 PRC AND HK

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

Last week's [Lloyd v Google LLC decision](#) marked the end of an era as the Supreme Court concluded the widely followed wrangle between the tech-giant and Richard Lloyd representing more than 4 million UK iPhone users. The court's judgement (discussed below and in our [blog](#)) is likely to significantly stem the flow of future opt-out representative actions in data protection claims, much to the relief of many organisations.

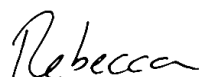
While the question of controllers' exposure to mass opt-out claims appears to have been settled by the courts, this autumn has seen significant new uncertainty arise on the regulatory side, with the [DCMS publishing its plans](#) for data protection regulatory reform in the UK (which we discuss below). The DCMS plans can be seen as outlining an evolution of the UK GDPR rather than a completely fresh start albeit that they do include a large number of substantial proposals that would significantly change the UK's regime as we know-it (and organisations have embedded within their policies and procedures).

Uncertainty also remains over international data transfers from the UK. Although the EU Commission's new standard contractual clauses (SCCs) came into use at the end of September for transfers out of the EU, the ICO's answer, the new international data transfer agreement (the IDTA) and accompanying transfer risk assessment tool (TRA) have not yet been finalised. The ICO's [consultation](#) on those documents and on changes to its international transfers guidance only closed on 11 October, with final versions of the IDTA and TRA not expected before the end of the year or early in 2022. Further uncertainty and potential complexity, this time in relation to EU data transfers, has recently been indicated by the European Commission suggesting (at the September European Data Protection Board [plenary meeting](#)) that they are intending to develop another new set of SCCs to deal with transfers from organisations subject to the extraterritorial provisions of the EU GDPR.

In another marker of a new era in the UK data privacy regime, this month will see Elizabeth Denham's departure from the ICO on 30 November, with the new Information Commissioner, John Edwards [taking up the post](#) on 3 January, after his appointment was approved by the Digital, Culture, Media and Sport Select Committee on 9 September.

We will consider these developments and the outlook for UK data privacy in more detail at our annual Data Privacy Forum that is taking place virtually during the week commencing 29 November. We really hope you can join us but needless to say, if you have any questions before the Forum or if you would you like to discuss any of the current developments, please do give me a call.

On behalf of the Data Privacy team here, may I wish you a very happy festive season and I look forward to seeing you in 2022 if not before.



LEGAL UPDATES

The UK's future data protection regime

Following the publication of the [National Data Strategy](#) last September (which we discussed [here](#)), the Government greeted this academic year by launching a [consultation](#) on data protection reform. It sought views from organisations on its strategy which aims to create a more “pro-growth and pro-innovation” regime. The consultation document outlines wide-ranging changes to the current UK GDPR regime, including those that could affect automated decision-making, cookies, data breach reporting, the subject access regime, the GDPR’s accountability requirements and institutional reform of the ICO. We discuss the consultation in more detail in this [blog post](#), and the potential for reform of the cookies regime in [this post](#).

The ICO [has subsequently published](#) its own view on the consultation with the outgoing Information Commissioner, Elizabeth Denman, stating: ‘It is important government ensures the UK is fit for the future and able to play a leading role in the global digital economy. I therefore support this review and the intent behind it. As the proposals are developed, the devil will be in the detail. It will be important that Government ensures the final package of reforms clearly maintain rights for individuals, minimise burdens for business and safeguard the independence of the regulator.’

Also following on from the National Data Strategy, the UK Government has announced its intention to [independently strike data adequacy decisions](#) with international partners and has published a list of priority jurisdictions for such adequacy decisions, with Australia, Colombia, the Dubai International Financial Centre, the Republic of Korea, Singapore and the US being labelled ‘top priority’ candidates, with India, Brazil, Indonesia and Kenya listed as ‘longer term priorities’.

CASE LAW UPDATE

Lloyd v Google - class action update

As mentioned above, on November 10, the Supreme Court handed down its long awaited [judgment in Lloyd v Google LLC](#). As we discuss in more detail in our recent [blog](#), if successful, My Lloyd’s claim could have opened the door procedurally to many more data privacy class actions, such as those already in train in relation to TikTok, Facebook and Marriott.

Warren v DSG Retail Limited

The High Court’s judgement in the [Warren v DSG Retail Limited](#) case has also provided some positive news for controllers in relation to their potential exposure to data privacy litigation following external cyber-attacks. The case related to a claim brought against Dixons in connection with their 2018 data breach by external cyber criminals. It was brought on the basis of several different heads of damage that are often pleaded together in data litigation cases (misuse of private information, breach of confidence, breach of the data security principle of data protection legislation and negligence). The claims for misuse of private information and breach of confidence were dismissed by the court on the basis that neither impose a data security duty on the information holder but are concerned with prohibiting their ‘positive’ actions. This finding served to limit the ability of the claimants to recover the premium for their ‘after event insurance’ (which gives them costs protection) from the defendant under the CPR. Accordingly, this judgement may make it less inviting for individuals to bring such claims if they risk being on the hook for defendant’s costs and could make it less inviting for those firms looking to amass such claims.

Rolfe & Others v Veale Wasbrough Vizards LLP

In the case of [Rolfe & Others v Veale Wasbrough Vizards LLP](#) the High Court granted summary judgement and dismissed a data breach case in which the damages suffered by the claimant were ‘trivial’ and not above the required de minimis threshold. The case centred on a mis-sent email from a solicitors’ firm, relating to the claimants’ failure to pay school fees. The email was sent to a single incorrect recipient, was quickly deleted by that recipient and was not subject to any further misuse. In a reassuringly sensible judgement, Master McCloud cited the Court of Appeal decision in [Lloyd v Google](#) as authority for the fact that there needs to be some non-trivial damage in addition to the loss of control of data for damages to be recoverable in claims for breach of data protection regulations. He stated: “In my judgment no person of ordinary fortitude would reasonably suffer the distress claimed arising in these circumstances in the 21st Century, in a case where a single breach was quickly remedied. [...] In the modern world it is not appropriate for a party to claim, (especially in the in the High Court) for breaches of this sort which are, frankly, trivial.” The relevance of the [Lloyd v Google](#) case to

this decision was highlighted by the Master extending the deadline for appeal until 21 days after the Supreme Court’s decision in *Lloyd v Google*.

REGULATOR GUIDANCE

Key pieces of guidance published by the ICO, the EDPB and European Data Protection Supervisor (EDPS) since July 2021 are included in the table below. Some of these are explained in more detail in the following sections.

KEY REGULATOR GUIDANCE	
ICO	
Data sharing: a code of practice (came into force on 5 October 2021)	December 2020
Call for evidence on the use of age assurance (consultation closes on 9 December 2021)	October 2021
Consultation on the draft journalism code of practice (consultation closes on 10 January 2022)	October 2021
Consultation on the AI toolkit (consultation closes on 1 December 2021)	October 2021
Call for views on employment practices (consultation closed on 28 October 2021)	August 2021
Consultation on the UK’s data transfers regime (consultation closed 11 October 2021)	August 2021
Direct marketing and the public sector (new guidance)	August 2021
Accountability Framework (published on 15 July 2021)	July 2021
EDPB	
EDPB launches first coordinated action	October 2021
EDPB guidelines 10/2020 on restrictions under Article 23 GDPR (final version)	October 2021
EDPB establishes cookie banner taskforce	September 2021

Updates from the ICO

ICO consultation on personal data transferred outside of the UK

In mid-August the ICO launched a wide ranging [consultation on the UK’s international data transfers regime](#). The consultation includes a number of documents and questions, addressing both the UK’s new post-Brexit data transfer regime and the fall-out from the Schrems II case. In particular, it includes:

- questions on and proposals for the amendment of the ICO’s current international transfer guidance;
- a draft set of new UK specific standard contractual clauses for international data transfers, named the UK ‘International data transfer agreement’ (IDTA). The ICO anticipates that the final version of the IDTA will be available to use in early 2022;
- a draft ‘[International transfer risk assessment tool](#)’ (TRA). The TRA is the UK’s equivalent to the EDPB’s [supplementary measures guidance](#) (01/2020) and provides a relatively user-friendly guidance tool for organisations carrying out post-Schrems II risk assessments ahead of making international transfers via one of the ‘appropriate safeguards’ in Article 46 of the UK GDPR; and
- a draft ‘[UK Addendum](#)’ as an alternative to the IDTA, that could be used to accompany the new EU SCCs to make them work for transfers from the UK.

While some of the welcome features of the new EU SCCs are mirrored in the IDTA (e.g. the ability to include multiple parties, the full range of data sharing scenarios (e.g. C2C, C2P, P2P, P2C)) it is clear that the ICO has taken a markedly different approach to the EU in these documents and has sought to provide a suite of materials that are more accessible for SMEs, using plain English with significant guidance notes. It will be interesting to see how much the ICO’s documents

are amended following consultation and the extent to which larger organisations choose to use the ICO's IDTA rather than the EU SCCs with the ICO's UK Addendum. The ICO's consultation closed on 11 October and we provided substantial feedback to the ICO through our role on the City of London Law Society's Data Law Committee. Please do get in touch with us if you would like to discuss the ICO's proposed approach to international transfers or our view on its consultation drafts.

ICO anonymisation guidance: Chapter 2

In accordance with its plan of March 2021 (see '[Building on the data sharing code - our plans for updating our anonymisation guidance](#)'), the ICO published the first Chapter of its [draft guidance on anonymisation, pseudonymisation and privacy enhancing techniques](#) for consultation in May (discussed in our [July newsletter](#)) and has now published [Chapter 2](#). Chapter 2 covers what is meant by 'identifiability', indicators of identifiability and 'the spectrum of identifiability' and how organisations should approach the assessment of 'identifiability risk'. It also retains the 'motivated intruder test' that was present in the pre-GDPR version of the guidance and discusses how it should be applied. The ICO's consultation on this chapter closes on 28 November 2021.

Alongside the ICO's work on anonymisation, the Centre for Data Ethics and Innovation (CDEI) has been exploring the role [privacy enhancing technologies](#) (or PETs) can play in helping to enable data sharing and analysis while protecting the privacy of sensitive data. We discussed the CDEI's work and the adoption of PETs in our August [client briefing](#).

ICO consultation on its AI toolkit

The ICO [has opened](#) a consultation on the beta version of its [AI and data protection risk toolkit](#). The toolkit was published in July 2021 and is part of the ICO's commitment to enable good data protection practice in AI. In the meantime, the Government has launched the [National AI Strategy](#) that defines a ten-year plan to make Britain a global AI superpower. We discuss these developments in this [blog post](#).

ICO guidance now in force

- The ICO's [Age Appropriate Design Code](#) (the Code) came into force on 2 September 2021 (as we discuss in our [Lens blog post](#)). In addition, on 14 October the ICO published an "[Opinion on "Age Assurance for the Children's Code"](#)", which provides more information on the ICO's expectations regarding age assurance in the context of the Code.
- The [Data Sharing Code of Practice](#) (which provides guidance on controller to controller data sharing) came into force on 5 October 2021. We discussed significant features of the Data Sharing Code in draft form in this [briefing](#).

Updates from the EDPB

The EDPB has [launched its first coordinated action](#), under the Coordinated Enforcement Framework it established in October 2020, on the use of cloud-based services by the public sector. Under the 'coordinated action', the EDPB prioritises a particular topic for EU data protection authorities (DPAs) to work on at a national level with these actions subsequently being reviewed at the EDPB level to inform further national and EDPB follow-up. The EDPB's use of this 'coordinated action' procedure gives insight into how the DPAs may focus on particular bloc-wide issues and sectors for enforcement in the future.

In another sign of increasing coordination between EU DPAs, the EDPB established a [cookie banner taskforce](#) in September to coordinate the response to complaints about cookie banners filed with a number of EU DPAs by Max Schrems' campaign group NOYB. The task force aims to 'promote cooperation, information sharing and best practices' between the EU DPAs.

ICO ENFORCEMENT OVERVIEW

HIV Scotland

The ICO [has issued](#) its sixth GDPR fine of £10,000 to HIV Scotland due to an email error. An individual at the charity mistakenly used the 'cc' field rather than 'bcc' one and sent an agenda for a quarterly meeting to 105 members of the charity's 'Community advisory network'. In their correspondence with the ICO, HIV Scotland accepted that the incident was down to human error and although none of the data disclosed was special category data, 'assumptions could be made about the individuals HIV category or risk'. As such the ICO advised that the data should have been dealt with by the charity in line with the ICO's guidance on special category data.

As with the regulator's fine against the [Mermaids](#) charity earlier this year (more information on this fine can be found in our [July newsletter](#)), this latest penalty serves as a reminder of the importance of basic data security measures and staff training (as once again the ICO found that the data protection training provided by the charity was inadequate). While the amount of this monetary penalty is relatively low in comparison to some of the blockbuster GDPR fines (particularly from some of the EU DPAs discussed below) it represents a relatively large amount in comparison to the charity's annual income (of just under £254k in 2018-19 according to its publically available figures) and indicates that the ICO will use the full extent of its UK GDPR fining power in circumstances where the potential impact of organisations' data privacy failings puts individuals at particular risk.

E-marketing penalties

The ICO has continued to issue regular monetary penalties for breaches of the UK's e-marketing rules, and in the last few months has brought actions against a number of household names: in September [We Buy Any Car](#) was fined £200,000, [Saga Services Ltd](#) and [Saga Personal Finance Ltd](#) were fined £150,000 and £75,000 respectively, while [Sports Direct](#) was fined £70,000. The [ICO's press release](#) for these actions outlined that up until 15 September the regulator had issued 17 fines totalling more than £1.7 million so far this year (2021/22) for breaches of direct marketing laws.

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
DSB (Austria)	Österreichische Post	€9.5 million	29 September 2021	• Data subjects rights
DPC (Ireland)	WhatsApp	€225 million	20 August 2021	• Transparency
DSB (Austria)	Unser Ö-Bonus Club	€2 million	2 August 2021	• Legal basis for processing (inadequate consent)
CNPD (Lux)	Amazon	€746 million	27 July 2021	• TBC
AEPD (Spain)	Mercadona	€2.52 million	23 July 2021	• Legal basis for processing
Garante (Italy)	Deliveroo	€2.5 million	22 July 2021	• Data processing principles (inc. transparency and minimisation)

Amazon appeals Luxembourg fine

Amazon [has appealed](#) to the Luxembourg Administrative Tribunal against the record €746 million GDPR fine [issued](#) by the Luxembourg DPA in July for breaches by the company of the EU's GDPR. The contraventions giving rise to the fine have not been made public by the Luxembourg DPA, in line with the provisions of its national data protection legislation, and the fine only came to public attention when it was acknowledged in Amazon's quarterly results and subsequently by the DPA. Amazon's fine is by far the largest fine issued under the GDPR to date.

Irish DPC's WhatsApp fine

The Irish Data Protection Commissioner (DPC) [fined WhatsApp €225 million](#) in September for breaches of the GDPR transparency obligations. The DPC had initially proposed a fine of €30 - 50 million but its approach to the enforcement action was called into question by other affected EU DPAs under the EU GDPR's cooperation and dispute resolution mechanisms. As the EU DPAs could not reach a mutual position on the action, the EDPB was called on to issue a binding decision (under Article 65) resulting in the significant uplift to the Irish DPC's fine for WhatsApp. We will soon be publishing further commentary on GDPR enforcement trends.

Perhaps unsurprisingly, given the disputes surrounding the fine at DPA level and the strong financial position of the WhatsApp group, WhatsApp is progressing several separate avenues of challenge and appeal against the fine concurrently.

It has: (i) been [granted permission](#) from the Irish High Court to apply for judicial review of the DPC's decision; (ii) launched a court appeal against the EDPB for its role in increasing the Irish DPC's proposed fine in the EU's first tier General Court; and (iii) [launched a court appeal](#) against the fine in the Irish courts.

In the start of a potentially similar legal saga, Facebook could be fined between €28 million and €36 million for transparency failings by the Irish DPC after the NOYB (Max Schrem's NGO) published a [draft decision](#) from the Irish DPC against the tech firm in October. While finding Facebook in breach of the GDPR's transparency obligations, the DPC did not find the firm in breach of the regulation's consent provisions, something which other affected DPAs may challenge.

VIEWS FROM ... THE PEOPLE'S REPUBLIC OF CHINA AND HONG KONG

Contributed by Wynne Mok, Partner (Hong Kong)

2021 has seen some very significant legal developments in the People's Republic of China (PRC) in relation to data protection and security. The Data Security Law (DSL) and Personal Information Protection Law (PIPL) have now come into force. Both pieces of legislation could potentially affect businesses which operate outside of the PRC but engage in collecting, storing, using, processing, transmitting or disclosing relevant data.

The DSL primarily regulates activities involving data which the Chinese government considers to be crucial to its national security, economy and public interest. In particular, foreign companies engaging in data processing overseas which harms Chinese national security, public interest or the legitimate rights of Chinese persons may be investigated and severely penalised.

PIPL is the PRC's first comprehensive legislation on personal data protection. It sets out data subjects' rights over their personal information and data processors' obligations (PIPL's 'data processor' concept is close to the concept of a controller under the UK GDPR), and imposes stringent requirements for cross-border transfers of personal information. Collection of data for the purposes of providing products and services or analysing consumers' behaviour is regulated. Operators of important network infrastructure and information systems which could seriously affect Chinese national security, economy and public interest must store the data collected and generated within the PRC locally and can only transfer such data across the border after undergoing a security assessment by the Cybersecurity Administration of China (CAC). Other personal data processors must either pass a CAC security assessment, conduct personal data protection certification or enter into a contract formulated by the CAC with the offshore recipient before any cross-border data transfer.

Hong Kong has recently amended its personal data protection law which was first enacted in 1995. The amendments are aimed at protecting data subjects in the city from disclosure of their personal data with ill intent. To eradicate such behaviour, which has been widespread in recent years, the Privacy Commissioner for Personal Data (the Commissioner) is empowered to order entities which own or host social media platforms accessible to the Hong Kong public to remove offending material. Non-Hong Kong service providers may also be affected if they provide relevant services to any Hong Kong person. Severe penalties may be imposed on those who do not comply with the Commissioner's order.

THE LENS

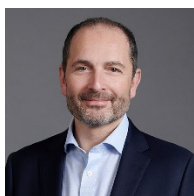
Our blog, [The Lens](#), showcases our latest thinking on all things digital (including Competition, Cyber, Data Privacy, Financing, Financial Regulation, IP/Tech and Tax). To subscribe please visit the [blog's homepage](#). Recent posts include: [Small issue, big consequences; increased regulatory focus on the GDPR representative requirement](#); [Can data trusts help unlock the value of your data?](#); and [Has the cookie banner crumbled?](#)

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 entities 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.

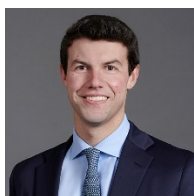
CONTACT



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, 2021.
For further information, please speak to your usual Slaughter and May contact.

www.slaughterandmay.com

570912266