

Data Privacy Newsletter

January 2020 / Issue 12

Selected legal and regulatory developments in data privacy

Quick Links

[Regulator guidance](#)

[International transfers](#)

[Enforcement overview](#)

[Case law update](#)

[Views from... Australia](#)

[Data Privacy at Slaughter and May](#)

[Our other publications](#)

We were delighted to welcome so many of you to our annual Data Protection and Privacy Forum at the beginning of December. Once again it was a fantastic opportunity for us all to share knowledge, insights and market practice (as well as the now traditional mince pies and mulled wine!)

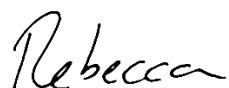
Reflecting on our conversations at the Forum, for me, the standout issue this year was data retention. Challenges around data retention were our attendees' top privacy compliance concern (voted for by 57% of our audience), far outweighing other issues such as direct marketing (12%) or third party transfers (10%). This perhaps reflects the stage organisations are now at with their GDPR compliance - the headline policies have been put in place, the easy challenges dealt with, and now we are all left wrangling with the thorny systemic issues that require real organisational buy-in to rectify.

These experiences are being mirrored in the latest guidance from regulators, including the EDPB's draft guidelines on data protection by design and default and the ICO's draft guidance on DSARs and direct marketing. These documents clearly show that our regulators' focus is now on organisations driving through changes to systems and processes to make real data privacy improvements.

We are also seeing the risk profile of data privacy continuing to evolve. The Court of Appeal's decision in *Lloyd v Google* has focused minds on class action claims, with the potential for an unfavourable Supreme Court decision on employer's vicarious liability in the *Morrison* case to follow. Likewise, the ICO's super-sized notices of intention in July, although yet to be finalised, have clearly impacted the risk-benefit analysis of privacy compliance in the UK.

2020 certainly promises to be another interesting year for privacy with a number of significant developments anticipated, including the final version of the ICO's data sharing code of practice, the ECJ's judgement in the Schrems II litigation and, of course, Brexit.

With that backdrop we will continue to keep you up to date with developments and support you in delivering the next stage of privacy compliance.



Rebecca Cousin
Partner

[Contents page](#)

Regulator guidance

Key pieces of guidance published by the Information Commissioner's Office (ICO) and the European Data Protection Board (EDPB) since July 2019 are included in the table below.

Key Regulator Guidance	
ICO	
Age appropriate design: a code of practice for online services	January 2020
Draft direct marketing code of practice (consultation closing 4 March 2020)	January 2020
Draft right of access guidance (consultation closing 12 February 2020)	December 2019
Draft guidance on explaining AI decisions (consultation closing 24 January 2020)	December 2019
Detailed guidance on special category data	November 2019
Guidance on data protection and no-deal Brexit for small organisations	September 2019
Draft data sharing code of practice (consultation closed 9 September 2019)	July 2019
EDPB	
Guidelines on the territorial scope of the GDPR (Article 3)	November 2019
Draft Guidelines on Data Protection by Design and by Default (Article 25) (consultation closing 16 January 2020)	November 2019
Guidelines on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects	October 2019
Draft Guidelines on the processing of personal data through video devices (consultation closed 9 September 2019)	July 2019

ICO issues detailed guidance on special category data

In November, the ICO published new detailed guidance on special category data (SCD) under the GDPR. In its [blog](#), the ICO emphasises that controllers are expected to take all necessary precautions to protect SCD due to the potential harm that misuse of such data can cause to individuals' fundamental rights. The guidance is largely consistent with the ICO's guidance on sensitive personal data under the previous regime but there are a few points worth noting. For example, the ICO restates its previous position in relation to photos and names from which SCD may be inferred, for example, where a name or photo seems to indicate a particular ethnicity or religion. The guidance explains that such photos or names will not automatically constitute SCD unless the controller is processing them specifically because they indicate ethnicity or religion (for example, to enable the targeting of services). Whether this data is SCD or not therefore depends on the controller's processing purposes.

The guidance also reconfirms that the term 'necessary', as used in the GDPR's Article 9 conditions for processing SCD, presents a high bar. It makes clear that the relevant Article 9 condition does not apply if controllers can reasonably achieve the same purpose by other less intrusive means; it is not enough that the processing is necessary as part of a particular business model.

[Contents page](#)

ICO consults on right of access guidance

In December 2019, the ICO also published detailed guidance on the right of access (often referred to as subject access requests, or 'DSARs') for consultation. Although the draft may yet be subject to amendment following feedback, the current version provides controllers with some useful and pragmatic advice on dealing with DSARs. For example, it provides useful clarification on the "complexity" basis for extending the response time to a DSAR. The draft guidance sets out a list of factors that contribute to complexity, such as the requirement for specialist work requiring redaction. However what amounts to a complex request will depend on the individual circumstances of the request, including the size and resources of the organisation in question. Requests involving a large volume of information will not automatically be viewed as complex. The draft guidance also includes more detail on how organisations should manage third party personal data in a DSAR response.

Potentially less helpfully, the draft guidance adds significant GDPR compliance obligations into controllers' preparation for DSARs. It advises controllers to prepare for and take a proactive approach to DSARs even if they do not receive them regularly. Steps they should take to prepare include having "retention and deletion policies" and "asset registers" in place. The draft guidance, however, does recognise that what is appropriate will depend on the size and resources of the organisation in question, the types of data they process and number of DSARs they receive. The consultation period for the new guidance closes on 12 February 2020.

ICO consults on data sharing code

In July, the ICO launched a public consultation on its draft data sharing code of practice. The data sharing code is one of the statutory codes that the ICO were required to prepare under the Data Protection Act 2018 (DPA 2018) and is likely to have wide-ranging application. Although the current draft contains much useful guidance, some parts may be challenging for organisations to follow, as we discuss in our November article '[Take care before you share](#)'. The consultation period for the data sharing code ended on 9 September 2020.

ICO consults on direct marketing code

On the 8 January this year, the ICO launched a public consultation on its direct marketing code of practice. The direct marketing code was also provided for in the DPA 2018 and the draft code follows on from the ICO's initial call for views on the topic in December 2018. The current draft is twice the length of the ICO's previous guidance and provides updated guidance on direct marketing under the GDPR, DPA 2018 and the Privacy and Electronic Communications Regulations 2003 (as amended) (PECR). As well as focusing on the GDPR concepts of accountability and data protection by design and default, the guidance also contains significantly more detail on the application of the direct marketing rules in the context of online advertising and new technologies. Unlike the ICO's previous guidance, the new version will be a statutory code of practice meaning that it must be approved by Parliament and taken into account by the ICO when considering an organisation's compliance and by the courts wherever relevant. The consultation period on the code ends on 4 March 2020 and the final version is expected later this year.

It is worth noting here that, at the EU level, the draft e-Privacy Regulation (ePR) which would supersede PECR has stalled. Given the continuing delay, it is unclear to what extent the ePR will affect the UK post-Brexit as it is looking increasingly unlikely that the new ePR will both come into force and apply in the UK before the end of the Brexit transition period.

[Contents page](#)

International transfers

Standard contractual clauses: Schrems II

As we have discussed in previous issues of this newsletter, the Schrems II ECJ case is testing the validity of the EU's standard contractual clauses (SCCs) (often referred to as the 'model clauses') that facilitate international transfers of personal data outside the EU (see our [July 2018](#) and [July 2019](#) newsletters). The ECJ heard the Schrems II case on the 9 July and on 19 December the opinion of the Attorney General Saugmandsgaard Øe was published. The AG opined that the SCCs remain valid and that analysis of [the questions referred by the Irish High Court to the ECJ](#) has disclosed nothing to affect the validity of the European Commission decision establishing the SCCs (2010/87/EU).

However, as part of his reasoning, the AG did emphasise that the SCCs contain an obligation on controllers (and where they fail to act, the relevant supervisory authorities) to suspend or prohibit transfers when the SCCs cannot be complied with because of a conflicting law imposed by a third country. The opinion talks at some length about the "examination" which the parties to SCCs should carry out in relation to the third country before any data is transferred. This process would appear to require significant diligence by parties to the SCCs and signals a note of caution against some existing marketing practice of simply "rubber stamping" the SCCs. However, as the ECJ isn't bound to follow the AG's opinion, we are now waiting for the ECJ's judgement, which is expected this spring.

In parallel, the European Commission has announced that it is in the process of updating the SCCs with input from industry¹, so even if the SCCs stand firm in light of the Schrems II challenge, the current versions could soon become obsolete.

Enforcement overview

ICO's first GDPR fine(s)

In July, the ICO issued notices of intention to fine [British Airways £183m](#) and [Marriott £99m](#) for GDPR infringements. Though the ICO's suggested fine amounts were headline grabbing, the level of fines and the full rationale behind them have yet to be confirmed. Interestingly, it was reported in January that BA and Marriott have each reached an agreement with the ICO giving the regulator more time to issue their final penalty notice. Under the DPA 2018, the ICO have a maximum of 6 months from the issue of a notice of intention to issue their final penalty notice and this period can only be extended by agreement with the party in question. The ICO's new deadline for both fines is the end of March this year.

It appears that the ICO's focus for major enforcement actions remains, for now at least, on security breaches.² The ICO's [first confirmed GDPR fine of £275,000, against the pharmacy Doorstep Dispensaree Ltd](#), was also levied for security failings, albeit that the pharmacy failed to take adequate measures to physically protect special category data, rather than in relation to a cyber breach. This case is a useful reminder for organisations that, in addition to cyber security protections, simple physical data security measures must not be overlooked.

¹ Comments made by Ralf Sauer, Deputy Head of Unit in the European Commission, DG Justice and Consumer's International Data Protection Unit, during a session on "US-UK-EU cross-border data transfers after Brexit" at the Sedona Conference on 6 November 2019.

² The Marriott notice highlights the increased importance of adequate data protection due diligence in M&A, as we discussed in our article in [July](#).

[Contents page](#)*DPAs GDPR enforcement overview*

The table below sets out a selection of the most substantial GDPR fines brought by the European data protection supervisory authorities (DPAs) in the past 6 months, along with an indication of the principal areas of non-compliance addressed by each enforcement action.

DPA (Country)	Company	Amount	Date	Description
Garante (Italy)	Eni Gas e Luce	€11,500,000	17 January 2020	<ul style="list-style-type: none"> • Direct marketing • Data accuracy
BfDI (Germany)	1&1 Telecom GmbH	€9,550,000	9 December 2019	<ul style="list-style-type: none"> • Data security
CNIL (France)	Futura Internationale	€500,000	21 November 2019	<ul style="list-style-type: none"> • Special category data • Unlawful consent • Data minimisation
BfDI (Germany)	Deutsche Wohnen	€14,500,000	5 November 2019	<ul style="list-style-type: none"> • Data retention / deletion
DSB (Austria)	Österreichische Post	€18,000,000	23 October 2019	<ul style="list-style-type: none"> • Special category data • Direct marketing
UODO (Poland)	Morele.net	€645,000	10 September 2019	<ul style="list-style-type: none"> • Data breach • Data security
KZLD (Bulgaria)	National Revenue Agency	€2,606,600	29 August 2019	<ul style="list-style-type: none"> • Data breach • Data security
KZLD (Bulgaria)	DSK Bank EAD	€511,100	28 August 2019	<ul style="list-style-type: none"> • Data breach

It is noticeable that the amounts fined have risen significantly since our previous newsletter edition when only the CNIL's Google fine was above €500,000. It is also worth noting that the largest fines are not focused exclusively on data security, with the substantial Deutsche Wohnen fine arising from the estate agency retaining unnecessary data and the Österreichische Post fine arising from unlawful data processing and sharing, as well as non-compliant direct marketing by the postal company.

Case law update

Lloyd v Google

The [Court of Appeal](#) has overturned the High Court's findings and has permitted Lloyd's "Safari workaround" case to proceed against Google through an opt-out representative action. As we discussed in our article, [Data breach claims: a rebalancing by the English Courts](#), the High Court had previously refused to let the action proceed. The Court of Appeal made contrary findings to the High Court on two central points. Firstly, it held that the claimants' 'loss of control' over their data was sufficient in itself to entitle them to each recover damages, and did not require any further damage or distress on the part of claimants to be established. Secondly, the class of claimants could be widely drawn as they had the 'same interest' based on that 'loss of control' alone (whereas the High Court had determined that there were greater restrictions on the constitution of the class).

[Contents page](#)

This action therefore potentially opens the doors to more representative style class actions for privacy infringements in the UK, including as a follow up to data breaches. Organisations will be following developments in this case closely, particularly as similar class actions against Equifax and others are in progress. Google has indicated that it will look to appeal to the Supreme Court.

Morrison's: a watching brief

In November, the Supreme Court heard the final round of submissions in the ongoing *Morrison's* action. This followed the [Court of Appeal's decision](#) in 2018 to find Morrison's vicariously liable for the actions of a rogue employee who exposed the personal data of nearly 100,000 Morrison's personnel. The Court of Appeal decision threatens to expose Morrison's to the costs of compensation claims from individuals affected by the data leak and, significantly, potentially paves the way for equivalent claims against other controllers. The Supreme Court appeared sympathetic to the submissions of Morrison's counsel, particularly in relation to their argument that there was not a "sufficiently close connection" between the employee's wrongful conduct and what he was employed to do to justify a ruling of vicarious liability. However, it remains unclear which way the Court will conclude.

Views from... Australia

The Australian Government responds to the Digital Platform Inquiry

Contributed by Mellissa Fai, Partner, and Nupur Sachdev, Lawyer, Gilbert + Tobin

Background

Last month the Australian Federal Government released its response (Government Response) to the Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry (DPI) - a report released by the ACCC in June 2019 which outlined broad recommendations for regulatory reform in various areas affecting digital platforms, in particular Facebook and Google. The Government Response supported the majority of the ACCC's recommendations for reform with either a commitment to implement the recommendations or to further consultations over the next two years.

Reform of the Australian federal privacy regime was a major, if somewhat surprising, aspect of the DPI (given the ACCC is not the Australian privacy regulator) with the ACCC calling for greater transparency in business practices as well as more direct rights for consumers to protect their privacy. The ACCC's proposed revisions to Australian privacy law, if implemented, would have far-reaching and economy-wide consequences. While affirming the ACCC's recommendation for a broad review and reform of the Australian privacy law, the Government Response took a cautious approach, resolving to persist with its previously announced amendments to the *Privacy Act 1988* (Cth) (the Privacy Act), as well as committing to implement further proposed reform only subject to further consultation and design of specific measures.

Government Response: key privacy aspects

The Government Response builds on existing commitments the Government has made towards reform of the Privacy Act. Specifically, the Government intends to strengthen the Privacy Act's enforcement regime, including increasing maximum civil penalties that may be imposed under it to match penalties under the Australian Consumer Law, as well as introduce a binding online code for social media platforms and other online platforms that trade in personal information.

[Contents page](#)

Alongside these existing commitments, the Government Response announced an immediate intention to commence a general review, over the next 12 months, of the Privacy Act and to consider whether reform was required to empower consumers and protect their data. The Government has also committed to consult on the ACCC's more specific privacy recommendations including:

- amending the definition of 'personal information' to clarify that it captures technical data such as IP addresses and other online identifiers;
- a strengthening of the notification requirements, consent requirements (such that express consent is required in all cases of collection) and pro-consumer defaults;
- the introduction of a direct right of action (including class actions) for individuals in respect of breaches of the Privacy Act; and
- separate from the Privacy Act, the implementation of a statutory tort for serious invasions of privacy.

Implications for businesses

With previously announced Government initiatives underway and further reform to be subject to consultation, the year ahead is likely to be a turning point for the Australian privacy regime. The strengthening of the Privacy Act is likely to bring Australian privacy law in line with international models such as the GDPR, a result that may allow greater interoperability of the Australian privacy regime with overseas jurisdictions and minimise regulatory hardship for businesses.

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 EU and non-EU clients 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 of 6 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.

If you would like further information please contact one of the team below, or your usual Slaughter and May contact.

Our other publications

All of our publications on the GDPR and data privacy more generally are available on our [website](#).

[Contents page](#)



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



Peter Lake (Hong Kong)
Partner
T +852 2901 7235
E peter.lake@slaughterandmay.com



Cindy Knott
Professional Support Lawyer
T +44 (0)20 7090 5168
E cindy.knott@slaughterandmay.com



Bryony Bacon
Professional Support Lawyer
T +44 (0)20 7090 3512
E bryony.bacon@slaughterandmay.com

© Slaughter and May 2020

This material is for general information only and is not intended to provide legal advice.