

## Data Privacy Newsletter

May 2020 / Issue 13

### Selected legal and regulatory developments in data privacy

#### Quick Links

[Regulator guidance](#)

[Enforcement overview](#)

[Case law update](#)

[Views from...  
New Zealand](#)

[Data Privacy at  
Slaughter and May](#)

[The Lens](#)

[Our other  
publications](#)

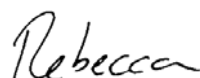
On behalf of the whole team at Slaughter and May, I hope you are all keeping safe and well during these very unusual times. We, like many of you, have now transitioned to working from home and communicating with our friends and colleagues on a day-to-day basis over video link (sometimes, with the occasional guest appearance from our children, pets or other family members!); these are changes that few of us would have predicted at the start of the year.

Whilst we must not forget the gravity of the current health crisis, now also feels like an appropriate time to reflect on our 'new normal'. Over these past months, we have become increasingly reliant on technology and in the UK, and indeed in many other countries around the world, we now find ourselves being encouraged to make use of contact tracing applications to better protect ourselves and others around us. With this in mind, it is clear that data privacy considerations remain key - not least because now more than ever before, they touch both our personal and professional lives.

We have seen considerable activity from regulators across the globe, as data protection authorities have raced to issue guidance on data processing practices affected by COVID-19. Not all such guidance has been aligned. However, it is encouraging to see that the ICO has taken steps to reassure organisations that it will take a "reasonable and pragmatic approach" in the current climate. At a time when many organisations have been forced to make difficult decisions concerning the allocation of their resources and workforce, we know that the ICO's comments will reassure many.

Beyond COVID-19, there have been a range of exciting developments in the data privacy world - many of which we have already featured on our new Digital blog, [The Lens](#). In recent months, we have seen the courts hand down significant decisions in *Morrison* and *Dawson-Damer*, Google has been granted permission to appeal by the Supreme Court in the ongoing litigation in *Lloyd v Google* - and, of course, we now know that the much-anticipated decision in *Schrems II* will be delivered on 16 July. Whilst regulatory action has understandably slowed in recent times, it has also been reported that the ICO's decisions in relation to the British Airways and Marriott data breaches, albeit likely to be much lower than initially anticipated, will be delivered by the end of the year.

Against this backdrop, we remain focused on supporting you with the next stages of your data 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 January 2020 are included in the table below. Some of these are explained in more detail in the following sections.

Key Regulator Guidance	
ICO	
<a href="#">Data protection and coronavirus information hub</a>	Maintained
<a href="#">Guidance on GDPR certification schemes</a>	February 2020
<a href="#">Guidance on codes of conduct</a>	February 2020
<a href="#">Draft guidance on the AI auditing framework</a> (consultation closed 1 May 2020)	February 2020
EDPB	
<a href="#">Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak</a>	April 2020
<a href="#">Guidelines on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak</a>	April 2020
<a href="#">Draft guidelines on Articles 46(2)(a) and 46(3)(b) of the GDPR for transfers of personal data between EEA and non-EEA public authorities and bodies</a> (consultation closing 18 May 2020)	February 2020
<a href="#">Draft guidelines on processing personal data in the context of connected vehicles and mobility related applications</a> (consultation closed 4 May 2020)	February 2020

### *ICO and EDPB respond to the COVID-19 pandemic*

In response to the ongoing situation with COVID-19, privacy regulators across the world have been extremely active – not least the ICO, which has published a range of guidance, good practice recommendations, FAQs and blog posts addressing the current health crisis. A comprehensive list of these resources can be found in the ICO's [Data protection and coronavirus information hub](#).

In a [document](#) setting out its regulatory approach during the COVID-19 pandemic, the ICO reminds us that the GDPR's core data privacy principles must be upheld, even for emergency data use. However, the ICO commits to adopting an "empathetic and pragmatic approach" and says it will act with flexibility where required, "taking into account the impact of the potential economic or resource burden [its] actions could place on organisations". In particular, the ICO [acknowledges](#) that it cannot extend statutory timescales, but indicates that delays – for example in the context of responding to data subject access requests (DSARs) – are "understandable" in the current climate, as the ICO appreciates that resources may need to be diverted away from data privacy compliance or information governance programs. With this in mind, the ICO [indicates](#) that it will be looking to take regulatory action against only the most significant breaches of data privacy legislation – in particular, focusing on those who are looking to take advantage of the current crisis.

[Contents page](#)

In an employment context, the ICO [highlights](#) that organisations have an obligation to ensure the health and safety of their employees and that data protection legislation should not act as a barrier to this. The ICO has also published additional [detailed guidance](#) for employers, which addresses the processing and collection of employee health data, the operation of employee health checks, the exercise of employees' information rights and other general GDPR compliance issues. Most notably, the ICO does not rule out the use of more intrusive technology - such as temperature checks or thermal cameras - when checking an employee's health status, providing organisations can adhere to the GDPR's core data protection principles and adequate safeguards are in place.

As this situation evolves, the ICO [suggests](#) that data is likely to play an important role in combatting the spread of COVID-19 and further, [indicates](#) that the development of GDPR compliant contact tracing technology will be a priority for the regulator over the coming months. The ICO is working closely with [NHSX](#) in the UK Government's effort to create a contact-tracing mobile application, but [reiterates](#) that a "high level of transparency and governance" must be guaranteed.

Following calls for a pan-European approach to contact tracing technology and combatting the spread of COVID-19 more generally, the EDPB also adopted new guidelines in April. The [guidelines](#) clarify how geolocation data and other tracing tools can be used in a way that is compatible with both the GDPR and the ePrivacy Directive. Interestingly, as governments across the EU race to roll-out contact tracing applications, the EDPB [highlights](#) that the use of such technology must be voluntary. Separate [guidelines](#) published by the EDPB in March (in the context of processing health data for scientific research) address key legal questions around legal basis' for processing, the adequacy of safeguards, data subjects' rights, and international data transfers - including in the absence of an adequacy decision. The EDPB's guidelines will supplement existing guidance published by the EU Commission in its [EU toolbox for the use of mobile applications for contact tracing and warning](#), which we discuss in our [blog post](#) on The Lens.

### *ICO consults on AI auditing framework*

In February, the ICO launched a [public consultation](#) on its draft guidance on the AI auditing framework. The guidance contains specific AI-focused advice on data privacy compliance programs, recommendations for implementing technical and organizational measures to mitigate risks to data subjects and a broader methodology for the audit of AI applications. Whilst the consultation closed on 1 May, the regulator sought feedback from both technology specialists and those fulfilling a broader compliance role (such as DPOs, General Counsel and risk managers). See our [blog post](#) on the The Lens for further information.

## Enforcement overview

### *British Airways and Marriott: ICO decisions subject to further delay*

As discussed in previous issues of this newsletter, the ICO issued in July 2019 notices of its intention to fine [British Airways £183m](#) and [Marriott £99m](#) for GDPR infringements. The ICO's final decisions in each case were initially delayed from the end of 2019 until 31 March 2020. However, in light of the current health crisis, a series of extensions were agreed and the ICO's final decisions have now been even further delayed. The final decision in relation to British Airways is expected by the end of August, whilst the Marriott decision is now due on 30 September.

Both British Airways and Marriott have indicated that they anticipate the final amounts to be significantly lower than the above figures. Although this may be in part following the representations they made to the ICO prior to the pandemic, the impact of COVID-19 cannot be ignored as both the ICO and the companies will have had staffing and related procedural issues to cope with. In addition, COVID-19 will undoubtedly

[Contents page](#)

be having an impact on the financial situation of both companies, which is a factor the ICO has said it will take into account when imposing monetary penalties (see the ICO's [guidance on its regulatory approach during COVID-19](#)).

### *The ICO's first confirmed GDPR fine goes to appeal*

In our [January newsletter](#), we reported that the ICO's first confirmed GDPR fine had been levied against [Doorstep Dispensaree Ltd](#) for significant physical security failings. The pharmacy announced in February that it had filed an appeal against the ICO. This will be the second time Doorstep Dispensaree has contested the ICO before a first-tier tribunal. In January 2019, Doorstep Dispensaree [challenged](#) the ICO's decision to issue a formal information notice, compelling the pharmacy to hand over information to the ICO. The 2019 appeal was quickly dismissed and we continue to await the decision in the present case.

### *EU DPAs: GDPR enforcement overview*

The table below sets out a selection of interesting or noteworthy GDPR fines brought by data protection authorities (DPAs) within the European Union since our previous Newsletter, along with an indication of the principal areas of non-compliance addressed by each enforcement action.

DPA (Country)	Company	Amount	Date	Description
DPC (Ireland)	<a href="#">Tusla</a>	€75,000	17 May 2020	<ul style="list-style-type: none"> <li>Unlawful processing</li> </ul>
AP (The Netherlands)	<a href="#">Unknown organisation</a>	€725,000	30 April 2020	<ul style="list-style-type: none"> <li>Unlawful processing</li> </ul>
APD (Belgium)	<a href="#">Proximus</a>	€50,000	28 April 2020	<ul style="list-style-type: none"> <li>Data Protection Officers</li> <li>Co-operation with supervisory authority</li> </ul>
AZOP (Croatia)	<a href="#">Unnamed credit institution</a>	€20,000,000	16 March 2020	<ul style="list-style-type: none"> <li>Data subjects' rights</li> <li>Right of access</li> </ul>
Datainspektionen (Sweden)	<a href="#">Google</a>	€7,000,000	11 March 2020	<ul style="list-style-type: none"> <li>Data subjects' rights</li> <li>Right to be forgotten</li> <li>Unlawful processing</li> </ul>
Garante (Italy)	<a href="#">TIM</a>	€27,800,000	1 February 2020	<ul style="list-style-type: none"> <li>Direct marketing</li> <li>Transparency</li> <li>Unlawful consent</li> </ul>

Generally speaking, whilst there were still a number of fines issued by EU DPAs in relation to data security failings and direct marketing, what is particularly noteworthy from the table above is that DPAs are continuing to impose fines, sometimes quite high in value, for non-security breaches of the GDPR. In addition, the Greek, Croatian and Danish DPAs have all recently issued fines in relation to DSARs, whilst a number of DPAs continue to issue fines for unlawful processing (e.g. Norway and Spain).

[Contents page](#)

The Spanish DPA has been particularly active, with over 25 fines issued since late January (with amounts up to €120,000), compared to between 0-3 fines for most other EU DPAs. These fines relate to unlawful processing, unauthorised data sharing, lack of transparency, data minimization and lack of co-operation with the DPA.

COVID-19 will undoubtedly have an impact on GDPR enforcement trends, with many DPAs now looking to prioritise only the most serious breaches. Note that some DPAs, such as Hungary's NAIH, have even indicated that ongoing enforcement action (and, in fact, the application of some GDPR articles) will cease until the health crisis is over, attracting criticism from [civil rights organisations](#) across the EU.

## Case law update

### *Spotlight on collective data privacy litigation*

In April, the [Supreme Court](#) handed down the much-anticipated judgement in *Morrison Supermarkets v Various Claimants*. It concluded that Morrisons was not vicariously liable for the actions of a rogue employee who unlawfully shared personal data in breach of data protection legislation. Although this decision is reassuring for employers, the Supreme Court's view was that a controller's compliance with its obligations under data privacy legislation does not automatically exclude a claim for vicarious liability, so this remains a risk to be managed. See our [blog post](#) on The Lens and our briefing [Morrisons in the Supreme Court: a welcome decision with a sting in the tail](#) for further information.

In March, the Supreme Court granted Google permission to appeal the Court of Appeal's [decision](#) in *Lloyd v Google*. In a landmark decision for data privacy collective actions in the UK, the Court of Appeal had previously allowed a representative action to proceed against Google outside the jurisdiction (see our [January newsletter](#) for further details). The Supreme Court's judgement is not expected until late 2020 or early 2021.

This was followed in April by news that the action in *Atkinson v Equifax Ltd* was being withdrawn. Mr Atkinson had brought a representative action shortly after the Court of Appeal's judgement in *Lloyd v Google* in relation to Equifax's 2017 major data breach. It is understood that the action was withdrawn after Equifax filed its defence challenging the Court of Appeal's judgement in *Lloyd v Google* and that Equifax would be entitled to recover its costs.

### *Taylor Wessing v Dawson-Damer: Manual records and personal data*

In another welcome development, the [Court of Appeal](#) handed down its judgement in *Taylor Wessing v Dawson-Damer* in March on the question of when manual records form part of a "relevant filing system" (e.g. personal data) under the Data Protection Act 1998, with implications for the equivalent definition under the GDPR. See our [recent blog post](#) on The Lens for further details.

[Contents page](#)

## Views from... New Zealand

### *New Zealand's incoming privacy legislation*

*Contributed by Kelly McFadzien (Partner) and Stephanie Gray (Senior Solicitor), Chapman Tripp*

While New Zealand's new privacy legislation is still awaiting its third reading, it is due to come into force on 1 November 2020. An update is well overdue: the Privacy Act 1993 was drafted in an entirely different technological landscape, and work on its replacement has been ongoing for almost a decade. While the Bill is a big step forward, it doesn't go so far as to align New Zealand with the GDPR. Once passed, it's likely that the law will shortly require amendments to keep pace with international standards and developments.

### *Key changes introduced by the Bill*

- ***Mandatory data breach reporting regime:*** Privacy breaches that cause, or are likely to cause, serious harm to affected individuals, must now be reported to both the Privacy Commissioner and affected individuals. The "serious harm" threshold is similar to the equivalent notification threshold in the Australian legislation.
- ***Restrictions on international transfers:*** Currently personal information collected in New Zealand is freely transferrable to other jurisdictions. Under the Bill, international transfers will only be permitted if one of six grounds apply - the overall effect being that information may only be sent outside New Zealand if it will remain protected by safeguards comparable to those required under New Zealand law. These restrictions don't apply when the overseas recipient is a cloud storage provider or other overseas processor that is holding personal information only as an agent.
- ***Clarity on extra territorial effect:*** The Bill clarifies that both New Zealand agencies (when conducting activities inside and outside of New Zealand) and overseas agencies "carrying on business in New Zealand" will be caught by the new law.

### *Gaps remain*

The Bill doesn't give individuals the right to be forgotten or the right to data portability, and there is no right to transparency in relation to algorithmic decisions. Another major difference from the GDPR is that reputational damage remains the principal risk for agencies who don't comply with New Zealand privacy law. Under the Bill, the Privacy Commissioner can't seek civil penalties, and the maximum fine for offences, including failing to notify the Privacy Commissioner of a notifiable data breach, is NZD 10,000.

### *Next steps*

Many New Zealand businesses will need to prepare for the new law by formalizing a data breach notification process, and data mapping personal information transfers. Multinational organizations with New Zealand offices will need to ensure that New Zealand is included in any regional or global data breach notification assessments.

[Contents page](#)

## The Lens

### *Digital developments in focus*

Our new blog, [The Lens](#), showcases our latest thinking on all things digital. It brings together, in one place, content from all of our different practice streams that advise on tech and other digital topics, including Competition, Cyber, Data Privacy, Financing, Financial Regulation, IP/Tech and Tax.

Some of the latest thinking from our Data Privacy team can be found below:

- [‘NHS COVID-19’ app: are privacy concerns justified?](#)
- [Is COVID-19 making hopes of UK adequacy fade further? Privacy in a pandemic](#)
- [EU privacy regulators on COVID-19 contact tracing apps](#)

## 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](mailto:rob.sumroy@slaughterandmay.com)



**Rebecca Cousin**  
Partner  
T +44 (0)20 7090 3049  
E [rebecca.cousin@slaughterandmay.com](mailto:rebecca.cousin@slaughterandmay.com)



**Richard Jeens**  
Partner  
T +44 (0)20 7090 5281  
E [richard.jeens@slaughterandmay.com](mailto:richard.jeens@slaughterandmay.com)



**Duncan Blaikie**  
Partner  
T +44 (0)20 7090 4275  
E [duncan.blaikie@slaughterandmay.com](mailto:duncan.blaikie@slaughterandmay.com)



**Jordan Ellison (Brussels)**  
Partner  
T +32 (0)2 737 9414  
E [jordan.ellison@slaughterandmay.com](mailto:jordan.ellison@slaughterandmay.com)



**Peter Lake (Hong Kong)**  
Partner  
T +852 2901 7235  
E [peter.lake@slaughterandmay.com](mailto:peter.lake@slaughterandmay.com)



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



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

© Slaughter and May 2020

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