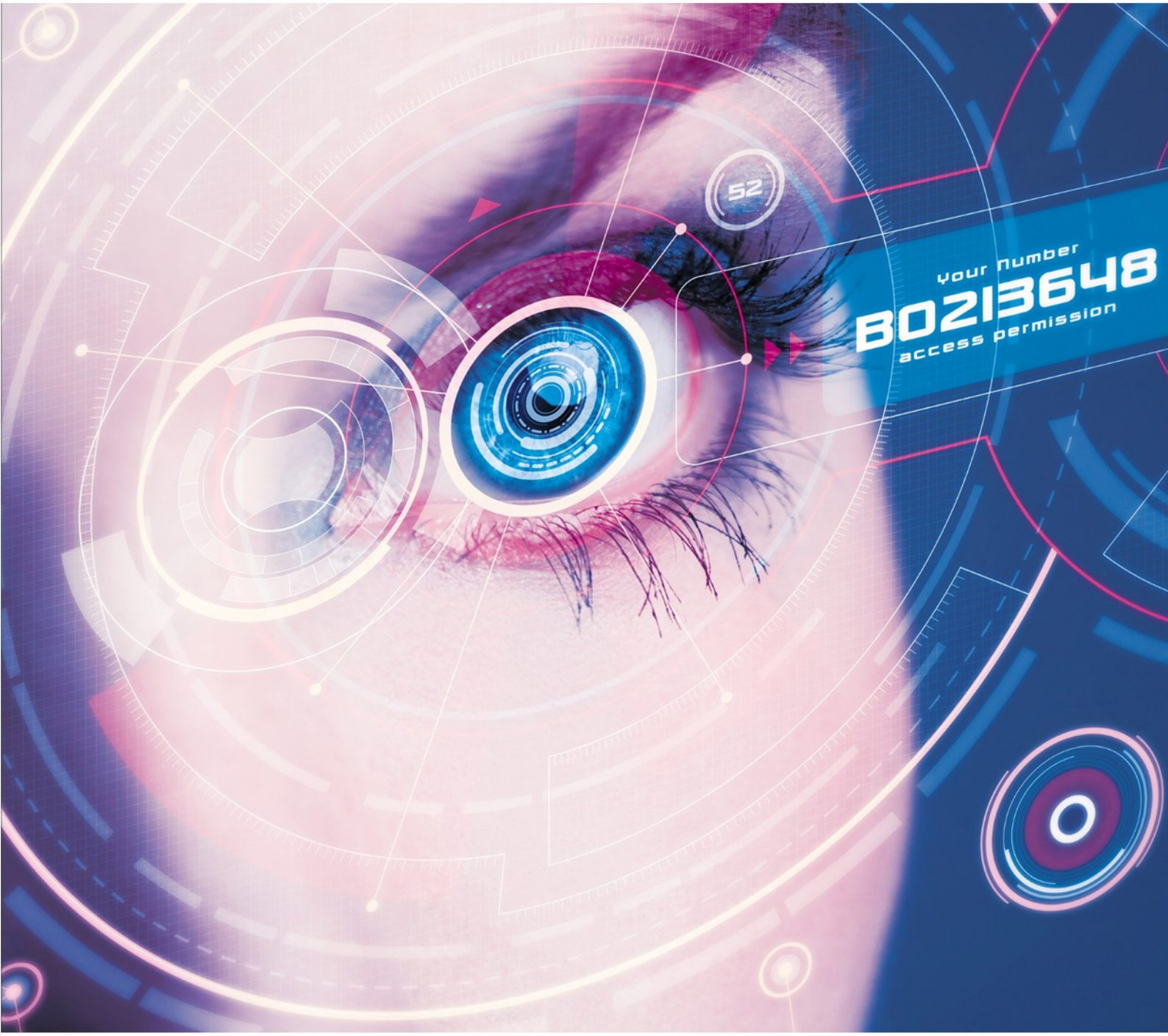
fieldfisher

Data Protection Times

28 January 2021



A data protection round up of 2020, brought to you by Fieldfisher's Privacy, Security and Information law team this 14th Data Protection Day.

A note from our editor, Hazel Grant

Welcome to the first edition of Fieldfisher's *Data Protection Times*, fittingly launched on this year's Data Protection Day. This newsletter looks back on some of the key data protection and privacy developments that took place around the world in 2020. In future editions we will bring you a selection of the latest legal updates. Whilst 2020 will forever be synonymous with the outbreak of the coronavirus pandemic and the devastation it has and continues to wreak, it was by no means a quiet year for data protection, either at home or aboard. We began to see larger fines implemented under the GDPR and there was a concentration of regulatory activity both in terms of enforcement and guidance on cookies from many a European SA. The impact of Schrems II continues to resonated and time will tell how effective the European Commission's Standard Contractual Clauses will be. With the final draft of those documents awaited, numerous high profile regulatory investigations ongoing, data protection legislation updates the world over, the ICO announcing the relaunch of its adtech investigation and its Children's Code applicable from 2 September 2021, the realm of data protection continues apace.

Top of the Privacy Pops

The Data Protection Times counts down the most prominent global developments from the past year.

5. The fifth notable news item is the ICO's fines of **British Airways and Marriott**, which were a fraction of the figures published in the Notice of Intention. The £183m intention to fine figure for BA was reduced to £20m, whilst Marriott's fine fell from £99m to £18.4m. The content of the Enforcement Notices are informative about the dos and don'ts of data security and the expectations of the regulator although there is no apparent reason for the significant reductions. Yes, the economic impact of Covid-19 was taken into consideration when calculating the final penalties but this was as a proportion of the reduced level of fine, such that BA's and Marriott's fines were reduced by £4m as a result of Covid-19.

4. Our fourth chart-topping story is the **new draft Standard Contractual Clauses**, which were published by the European Commission on 12 November 2020. The draft includes modules for (i) controller-to-controller, (ii) controller-to-processor, (iii) processor-to-processor and (iv) processor-to-controller transfers. Read about our colleague, Phil Lee's first impressions on the draft here.

3. Christmas wishes were granted for privacy practitioners UK-wide by our third story: the **EU/UK Brexit deal**. The Trade and Cooperation Agreement announced on Christmas Eve created a six-month 'bridging mechanism' allowing data to continue flowing freely from the EEA to the UK. It seems likely that the EU will issue a UK adequacy decision during this period. For UK to EEA data transfers, the UK government has deemed the EEA adequate on a transitional basis. This is likely to endure for a few years whilst the UK conducts its own full adequacy assessment. You can read our blog about these changes here.

2. News item number *II* is, of course, **Schrems II**, the CJEU judgment that invalidated the EU-US Privacy Shield and the sense of déjà vu vis a vis Safe Habor! The judgment set out numerous requirements that must be met before data can be transferred out of the EEA. The EDPB has since published recommendations on these supplemental measures, which can be technical, contractual or organisational. Our assessment of the recommendations is available in this blog.

1. The most prominent story is of course, the Covid-19 pandemic, which has given rise to unique privacy challenges. Increased rates of homeworking have heightened security risks. Employers have sought to navigate privacy law requirements when collecting relevant health and travel data from employees. For how long can you retain negative test results and what about a who's who of vaccine recipients? Finally, who could forget the privacy centred debate in the context of track-and-trace apps worldwide?

Homeworking can increase security risks

Letters

Dear Data Protection Times

I have recently reviewed the EDPB's Recommendations 01/2020 on supplemental measures.

I appreciate that the EDPB will inevitably have faced difficulties when trying to lay out in practice the supplemental measures required to facilitate data transfers outside of the EEA. However, it seems to me that some of the recommendations specified are impractical and unrealistic. One example is step three of the EDPB's six-step approach to data transfers, which effectively requires data exporters to carry out an adequacy assessment, taking into account the laws and practices within the receiving country. This seems an onerous and complex requirement – particularly for smaller organisations. This, I believe is made clear by the fact that it takes the European Commission itself years to make a decision on a country's adequacy. **Long Time Reader, Manchester**

Dear Data Protection Times

Much is happening in the space of children's data protection and privacy, for which the ICO's Age Appropriate Design Code, aka the Children's Code, is arguable at the forefront and according to the Commissioner's foreword is "the first of its kind". The Code itself is undoubtedly a positive thing for children's data yet it must be remembered that the Code solely focuses on processing and collection of personal data. Whilst the Code is part of a wider piece about content and online harms, this is a separate workstream both here and on the continent. Only later this year is an Online Safety Bill expected. Also each stakeholder, in my opinion, has a role to play with respect to children whether that be a parent/guardian, the children themselves, device manufacturer, government, education provider as well as information society services. **AADC Reviewer, London**

Dear Data Protection Times

Ever since the GDPR, there has been a huge increase in the receipt of Data Subject Access Requests. But have you noticed the sheer volume of documents when an employee DSAR includes instant messages? It can be exasperating, not to mention costly, financially and in terms of resourcing. Companies need to have clear policies on when and for what purposes instant messaging platforms can be used in their organisation and consider whether to save such communications in the event of an employee DSAR! **Anonymous**

Get Data Protection Fit with Fieldfisher's YouTube series

Struggling to stick to your New Year's resolution to get in shape? Why not try flexing your privacy law muscles instead and ***Get Data Protection Fit*** with our YouTube series?

More content coming in 2021: our YouTube channel can be accessed here.

Beyond the Headlines

The 2020 privacy developments that you may have overlooked …

Accountability is key

The ICO released its Accountability Framework in September. This resource is intended to assist organisations across all sectors to assess and manage their data protection compliance as well as being able to evidence that their processes work in practice. The Framework is split into a number of categories, such as individuals' rights,

Beyond the Headlines cont.

transparency, policies and procedures. Each category is then broken down into key expectations and a non-exhaustive list of how these can be met.

Irish DPC's cookie guidance

In April, the Irish Data Protection Commission ("**DPC**") published a report on its "cookie sweep" that surveyed a wide range of sectors across media and publishing, retail, hospitality, sports and leisure as well as insurance and the public sector. Its report was used to inform the guidance on tracking technologies including cookies that was published simultaneously.

The report found that almost all websites reviewed had set cookies on user devices on their landing pages. Further, 26% had pre-selected consent boxes enabling non-necessary cookies and failed to implement sufficient methods to inform users of their opt-out rights.

Diverging views amongst regulators in the UK and EU emerged throughout 2020. With respect to analytics cookies, like the ICO, the DPC will require consent. In contrast, Germany and France allow for particular analytics cookies, subject to certain conditions. The DPC does however align with the CNIL in its expectation that where a cookie is used to record consent it is refreshed after six months.

Meanwhile, the wait for an agreed version of the ePrivacy Regulation goes on.

CNIL fines Google and Amazon, €100m and €35m respectively

At the beginning of December, the CNIL handed out large EU regulatory fines to these two companies. Google LLC and Google Ireland Limited were fined for not obtaining prior consent and for not providing adequate information when placing advertising cookies on users' computers of google.fr. Amazon was fined for the same reasons with respect to cookies on the amazon.fr page.

Children's data protection

It is not only the ICO focusing on children and embracing Recital 38's provisions for "specific protection" for children. Ireland's DPC published its Fundamentals for a Child-Oriented Approach to Data Processing in December, which is open for comments until 31 March 2021. Sweden has also published guidance [Swedish] in this area.

The global influence of the GDPR

It was anticipated that the EU's GDPR would influence the direction of data protection travel. The extent of that is now becoming clear as across each continent we are seeing new legislation take effect such as Brazil's LGPD, California's CCPA, itself setting a benchmark for other US States, New Zealand and South Africa's Protection of Personal Information Act 2013 (yes it took seven years to enter in to force). Meanwhile, draft legislation has been issued in Canada, China and New Zealand.

Oh and not forgetting how we now have the UK GDPR. Are you managing to cross reference it using the latest Keeling Schedule and the EU GDPR 679/2016? Tricky ... Just as well we've made things easier for you with our UK GDPR website (details below).

Guidance from the EDPB and the ICO

Understandably, from both institutions as well as regulators across Europe, there was a lot of guidance issued in relation to the pandemic, especially with regard to the processing of health data as well as location data and contract tracing apps. Other notable guidance from the EDPB included guidelines on the targeting of social media users, concepts of controller and processor and the adopted version of guidelines on consent which added to its recommendations of supplemental measures for data transfers.

The ICO continues to provide a plentiful supply of guidance. In 2020 we had guidance on AI; updated guidance on the Right of Access, publication of its statutory codes on Data Sharing and the Age Appropriate Design Code, to

Introducing the **Fieldfisher UK GDPR website** and saving you from the difficulty of cross-referencing the EU GDPR with the Keeling Schedule and the mechanics of the Withdrawal Act.

DATA PROTECTION FINES: 2020 SCALE

Our 2020 scale sets out the value of a number of notable GDPR data protection fines that were issued across the globe last year and by way of comparison the FTC's fine of Facebook in the US. Will that kind of fine ultimately be generated by the GDPR?

OFF THE SCALE: A **US$ 5 billion** penalty issued by the Federal Trade Commission to **Facebook, Inc.** to settle charges that the company used deceptive settings and practices to undermine users' privacy preferences, in violation of a 2012 FTC order.

CNIL (the French data protection authority) issued two fines totalling **EUR 100 million** against **Google LLC** and **Google Ireland Limited** in December. CNIL found that the Google entities had breached cookie rules, noting that the google.fr page automatically placed non-necessary cookies on user devices without obtaining adequate consent.

A **EUR 50 million** fine issued by CNIL against **Google LLC** was confirmed by France's most senior administrative court in June 2020. The fine was issued in 2019 after CNIL found that Google's Android operating system failed to comply with the GDPR information, transparency and consent requirements.

In February, Italian telecoms company **TIM SpA** was issued with a **EUR 27.8 million** fine by the country's data protection authority for its unlawful marketing practices. The violations, which affected several million individuals, involved the company making unsolicited marketing phone calls without consent and in some instances despite recipients having already opted out of such communications.

EUR 22.5 million and 20.7 million – respectively, the approximate value of the fines issued to **BA** and Marriott by the ICO in respect of the companies' much-reported data breaches (GBP 20 million and 18.4 million).

AOK Baden-Württemberg, a German health insurer, was fined **EUR 1.24 million** for failing to implement adequate technical and organisational measures and sending marketing messages to 500 people without consent.

Hazel Grant
Editor / Partner
+44 (0)20 7861 4217
hazel.grant@fieldfisher.com

Lorna Cropper
Deputy Editor / Director
+44 (0)20 7861 4984
lorna.cropper@fieldfisher.com

Ally Hague
Junior Editor / Solicitor
+44 (0)20 7861 6762
alexandra.hague@fieldfisher.com