

Data Protection Times

May 2021



The Data Protection Times is a monthly round-up of the latest data protection developments that have caught the attention of Fieldfisher's Privacy, Security and Information law team.

A note from our editor, Hazel Grant

25 May 2021 marked the GDPR's third anniversary. There has been much reflection on its achievements to date and how it needs to evolve and address the problematic issues that have arisen — the backlog of complaints and enforcement action, the mechanics of how the One Stop Shop works in practice and the resourcing of DPAs, to name but a few. Yet, the model of the GDPR continues to be replicated around the world with Ecuador the latest to implement data protection law based on it. 38% of these three years has occurred during the pandemic and regulators have had to spend much time reacting to this in addition to business as usual activities, not to mention the raft of new challenges presented by AI, biometrics, adtech and the rest. With the UK's exit from the EU, is the EDPB missing the injection of pragmatism that the ICO is known for? As you read on you'll see much is happening in the data transfer space—my crystal ball is slightly opaque as to whether an EU-US solution will follow!

Top of the Privacy Pops

The most prominent global developments since our last edition

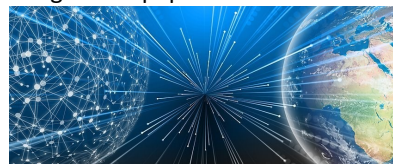
5. Portuguese DPA suspends US transfers. The Portuguese DPA, Comissão Nacional de Proteção de Dados (CNPD) [ordered](#) the National Institute for Statistics (INE) to suspend its data flows from the Census 2021 to service provider Cloudflare, established in California, US within 12 hours. Prior to the investigation commencing, the CNPD received a number of complaints about the questionnaire, in particular the collection of citizen identification data, i.e., full name. It also received complaints about the transfer of data to the US.

4. "What's that coming over the hill?" Is it SCCs? From whom? There are [reports](#) that the final publication of the EU SCCs (standard contractual clauses) is imminent after the comitology unanimously approved the European Commission's draft proposals for SCCs. It will be interesting to see how the draft documents, which were open for feedback via a [public consultation](#) differ to the published ones. Apparently, the changes will be significant. Remember there was a grace period in the draft allowing organisations a year to implement? Word is, the transition time may well be extended from this 1 year grace period!

On 5 May, the ICO held its annual Data Protection Practitioners' Conference (DPPC). One of the key announcements was the [UK's SCCs](#), which are due to go out for

consultation in the summer. Given the likelihood that we will already have the EU ones by then, how will the UK version differ, especially if the UK is to obtain and sustain adequacy. Same, same and essentially equivalent?

Nearly a year on from the CJEU's Schrems II decision, it could be another busy summer for international transfers. Best get that paper order made!



3. Facebook and the DPC ... again The [Irish High Court](#) rejected Facebook's application for judicial review against the DPC. The proceedings were brought by Facebook following the DPC's publication of their preliminary draft decision (the "PDD"), which sought to implement Schrems II.

The PDD was adopted by the DPC at the beginning of an "own-volition" inquiry into Facebook's EU-US data transfers. The PDD contained the Commissioner's views regarding the lawfulness of such transfers and Facebook sought to show that they were being treated unequally when compared to other data processors, and that the PDD demonstrated premature judgment and objective bias. The High Court dismissed each argument and found that the DPC's proposed procedure was not unfair to Facebook on any ground.

The DPC must now investigate the initial complaint of Max Schrems from 2013 using the original complaints procedure, and at the same time continue their "own volition" inquiry into Facebook in parallel. Of note, in the Court's largely procedural decision, is the reference to how there was no mention in Facebook's privacy notice about any supplementary measures that had been taken when transferring data outside of the EU.

2. European Parliament urges the Commission to amend its UK Adequacy decision. In a [resolution](#) passed by the European Parliament, MEPs call on the Commission to amend the draft decisions especially in relation to bulk access and onward transfers. A political statement perhaps but the 30 June deadline for an adequacy decision is fast approaching.

1. NHS makes passports available on its app. The UK's [NHS app](#) (not the Covid-19 app) has been updated to allow individuals to provide they have received the Covid-19 vaccination.

Letters

Dear Editor, Genuinely, how is everyone managing to keep their frustration at bay at the lack of a workable solution for EU-US data transfers? I'm struggling. Is there any light at the end of the [transatlantic] tunnel?

I read with hope, how the Irish High Court decision may provide a [catalyst for negotiations](#) (MLex, payroll) between Brussels and Washington to find a long term agreement for EU-US data flows. Similarly, comments from the IAPP's [KnowledgeNet](#), detailing how the European Data Protection Board will finalise its recommendations on supplementary measures for international data transfers at its 15 June plenary are welcoming. This is especially so if the EDPB does take a "risk-based approach" even for transfers that are captured under FISA section 702 (the big red flag of US government surveillance) although inevitably strong technical security measures will be needed.

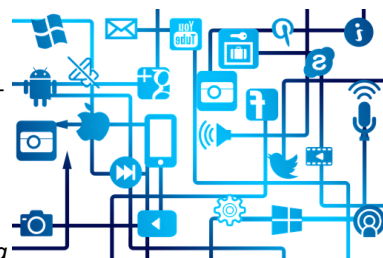
With the French government endorsing its national Cloud Strategy recently and stating its Health data hub will be hosted in the future by a French or other European host, does the EU want data localisation as we've seen in Russia and China? What about big data and the benefits it brings?

Yours extremely concerned

In House Counsel, Cloud Co., US

Hello DP Times! As we reflect on three years of the GDPR, I'm sorry to say but I do not believe the legislation is achieving the level of consistency that was intended, by some margin. Monitoring enforcement across the EU, there appears much inconsistency both with the amount of fines and the reasons for enforcement action. I appreciate the reasons for strict data breach reporting time-scales but I find it somewhat ironic that regulators fine companies for late reporting (e.g., Dutch DPA, Booking.com) when regulators themselves are not always so responsive, especially as they remain so completely under resourced themselves.

In my opinion we need approachable, business friendly regulators who can promote and engage and produce workable compliance solutions in a fast moving technological environment. As for the One Stop Shop ...



Data Protection Specialist, Bristol, UK

ICYMI

In case you missed it ... Years in the making but we finally have our first codes of conduct. This month the [EDPB adopted](#) the EU CLOUD Code of conduct, addressed to cloud service providers presented by the Belgium SA and the CNIL's CISPE Code of conduct, addressed to cloud infrastructure service providers.

Germany's [LfDI Rheinland–Pfaiz](#) (German) has this month written to dozens of organisations and businesses in the region urging them to review their data processing operations in connection with data transfers to third countries. Companies were asked to take a deep dive into their data processing to determine if they are transferring data to a third country. The information campaign is a fair warning, since the regulator plans to examine whether controllers have responded to the new challenges of data transfers in relation to the Schrems II decision and if not to impose fines.

The [ICO's Data Sharing Code has been put before Parliament](#). This code sets out some extensive expectations about data sharing which are beyond the UK GDPR. In the absence of any objections, this will come into force after 40 sittings days. Check out the [ICO's hub](#) on this code.

Undoubtedly, there is a real convergence between competition and data across the digital sector. This is reflected in the ICO's and the UK's Competition and Markets Authority [joint statement](#) about their relationship and willingness to cooperate in dealing with competition in digital markets and safeguarding people's data.



RECENT DATA PROTECTION FINES

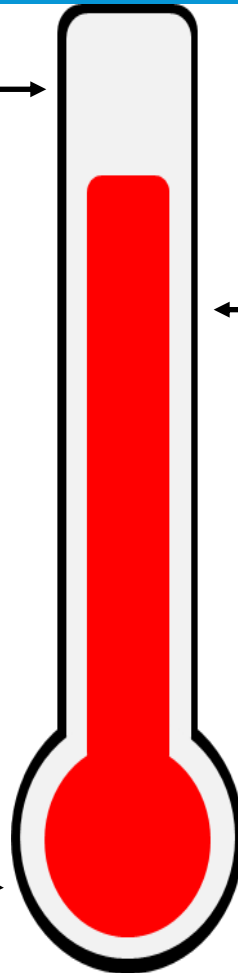
A busy month again for the Norwegian DPA who according to the EDPB website has issued more than 5 fines in May. This includes an [intent to fine](#) American company, Disqus Inc, **€2,5 million** for breaches of accountability, lawfulness and transparency.

Disqus were apparently unaware the GDPR applied in Norway, and conducted unlawful tracking of website visitors and disclosed this to third parties.

Organisations should be mindful of the different data protection regimes in the countries they operate in, as well as the extra territorial scope of these regimes.

The UK ICO issued its first fine since 5 March 2021 to [Tested.me](#) Ltd in the amount of **£8,000**, for sending direct marketing emails to people who had provided their personal data for the purposes of contact tracing.

Organisations collecting data for contact tracing purposes should not be using this information for other purposes.



The Dutch DPA fined [Locatefamily.com](#) **€525,000** for not having appointed a representative in the EU in breach of the GDPR. This case should spur UK and other businesses outside the EEA to review whether they need to appoint an EU-based representative to continue servicing EU-based consumers going forward.

The ICO fined [Amex](#) **£90,000** for sending over 4 million marketing emails to individuals who had specifically opted out. The ICO's investigated following complaints from individuals. Amex argued that these emails were service emails rather than marketing, but the ICO disagreed.

Organisations should be mindful of what constitutes "marketing" rather than service emails. This should also serve as a reminder to organisations to check they have sufficient consent **and** any suppression lists before sending out marketing communications.

How much? Dutch DPA wants €100m

The Dutch data protection authority has requested a structural increase in its budget to €100 million per year for its operating costs. The funding is needed to allow the DPA to deal with today's fast moving digital society. The amount sought is apparently on a par with other Dutch regulators, according to the [DPA's paper](#) (Dutch).

Compare this to the [Irish DPC's modest budget](#) increase for 2021 to €19.1m. Are member states really fulfilling their Article 52(4), GDPR obligation?

More enforcement coming soon?

In his own reflections on the GDPR at 3, [Wojciech Wiewiórowski, the EDPS](#), talks a great deal about enforcement. Regulators need courage "to step up enforcement actions" he said whilst questioning the model that places the burden of enforcement on a few regulators. With a call to "prioritise enforcement" and redistribute enforcement costs more equitably, enforcement will certainly be taken against those who do not protect EU citizen's data although it may be done differently in the future. It's time to audit your processes and procedures if you are not already doing so.



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



Charley Guile
Junior Editor / Solicitor
+44 (0)20 7861 6727
charley.guile@fieldfisher.com