fieldfisher

Data Protection Times

26 February 2021

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

A note from our editor, Hazel Grant

It goes without saying but I will say this once - it has been another busy month for data protection! As confirmation of the UK's adequacy becomes more of a reality and data transfers between the US and EU are cited as a priority, the ability to be able to transfer data seamlessly and compliantly without a raft of administration is essential. But given the vulnerability of these mechanisms to challenge, some companies are beginning to focus on a more localised approach to data to avoid future disruption. I can understand why. The details of data protection fines in recent weeks, notably Grindr and CAXIABANK, offer a practical reminder to all that the content of privacy notices needs to correspond to the actual data processing activities that are taking place and notices need to provide sufficient detail. Equally those fines highlight too how any consent collected needs to be valid. In the UK, how many more times will we see the ICO fining companies for unlawful marketing calls? Now that the Covid vaccine has received Royal approval, it will be fascinating to see what happens with "vaccine passports". I note the Ada Lovelace Institute is keeping a tracker but the privacy implications and other legal considerations will need to be given due consideration.

Top of the Privacy Pops

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

4. **UK employers setting up Covid-19 vaccine passports.** Employers throughout the UK have announced their intentions to create IT systems in order to track whether their employees have been vaccinated against Covid-19 – a 'vaccine passport'. Barchester Healthcare, a care home management company, have stated that they will even dismiss or decline to employ anyone who has refused the vaccine for non-medical reasons. Workday and BrightHR have each rolled out their own monitoring tools this month.

3. **Gina Raimondo: Privacy Shield replacement a 'top priority'.** Speaking ahead of her now confirmed nomination for secretary of the Department of Commerce, Gina Raimondo said that she would work to complete a data transfer deal between the US and EU. She told Politico that the negotiations are going well, and "*if confirmed, it would be a top priority of mine to finish the negotiations swiftly and ensure that there's a successor agreement that protects the interests of American businesses and provides for that transfer of data*".

   Time will tell how quickly Privacy Shield 3.0 will take to agree and (without wanting to jeopardise its longevity) for how long any agreed transfer mechanism will remain valid!

2. **A big step for the ePrivacy Regulation.** The Council of the EU announced it has approved its position on the ePrivacy Regulation, and this will now move to trilogue negotiations. This is the first major EU-wide legislative development in EU data protection law post-Brexit. Everyone will be watching to see what the UK decides to do with respect to PECR (Privacy and Electronic Communications Regulations).

1. **One step closer to UK Adequacy.** The European Commission has published positive draft decisions on the UK's adequacy. These relate to the GDPR and the Law Enforcement Directive. We are not quite there yet though—the EDPB will provide its formal opinion on the decision. Following this, confirmation will be required from Member States' representatives. The UK government (along with many organisations) "*welcomes the European Commission's draft data adequacy decisions*".

ICYMI

Amidst the waterfall of information, these headlines also caught our attention.

ENISA has published a report on **Data Pseudonymisation: Advanced Techniques and Use Cases**. The report provides guidance on the practical application of these techniques and examines advanced solutions for more complex scenarios that can be based on asymmetric encryption, ring signatures and group pseudonyms.

The **Council of Europe's guidelines on facial recognition**, which are intended to address the significant privacy risks presented by such technologies, call for prohibition of the use of facial recognition for the sole purpose of determining a person's skin colour, sex, or racial or ethnic origin.

The **ICO** launched its **data analytics toolkit** which is designed to provide organisations with key data protection points to consider at the outset of any project involving data analytics and personal data.

Letters

Dear Data Protection Times

I was intrigued to read last week a BBC News article about the prolific use of "spy pixels" in marketing emails, which was uncovered by a study run by a messaging service. Even after discounting spam mail, the study found that **two-thirds** of emails received by its users contained these pixels. What's worrying is that recipients are so often unaware of the use of these pixels, which can log data such as: if and when they open an email; what device they use; and their approximate geographic location (sometimes even down to street level!). The pixels are often far too small to be visible and can be automatically activated upon opening the email—leaving data subjects in the dark about this data collection. I think it is important for organisations to consider both the distinction between pixels that are used for analytics compared to retargeting, and whether the analytics in question request consent.

Privacy promoter, Birmingham

Dear Data Protection Times

We are in the midst of another acquisition and I am concerned about the lack of information provided on the target's data protection practices. Surely two and half years post the GDPR, privacy and cyber risk should be considered earlier in the deal process. We have requested information from the seller, but that hasn't been very fruitful. We have been provided with one or two procedure documents to review, which I hope will provide some detail. I am worried about the potential blank cheque we could be writing to deal with any remediation post-completion. The quintessence of data protection to the due diligence process cannot be underestimated.

Frustrated reader, Southampton

To all at the Data Protection Times

I welcome the Government's commitment to review a "vaccine passport". Undoubtedly, there has, at times, been a tension between privacy and the implementation of contact tracing apps. Any discussion of a vaccine passport creates a multitude of concerns from ethical, employment and privacy perspectives. It may create a potential divide between the public and private sectors, not to mention inconsistency across the globe. Whilst no vaccine developed to date is 100% effective against Covid -19 and its variants, I personally feel that any privacy compromise that enables a reduction in restrictions to mitigate the spread of the virus is worthwhile.

A former international traveller holed up in London's Zones 1-2 for the last 12 months (FWP)

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 will be available throughout 2021: our YouTube channel can be accessed here.

Dear Editor

I would welcome your thoughts on how best to future-proof and minimise any repapering exercise to allow for the various changes in the international data transfers space. Whilst we've waited an age for replacement sets of SCCs, it seems like challenges to EU-US data transfer mechanisms, and potentially the UK's adequacy, will be akin to "learning to live with Covid". I expect we'll see more data localisation! You?

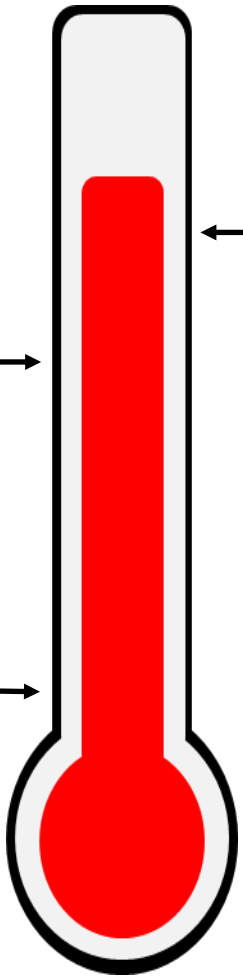
An anxious DPO, Global Company

fieldfisher

RECENT DATA PROTECTION FINES

The EDPB reported that AEPD, the Spanish DPA, issued a **EUR 6million** fine to **CAIXABANK** (reportedly the AEPD's highest under the GDPR). CAXIABANK failed to provide sufficient information regarding the details of processing (in breach of its transparency obligations) and the bank's collection of customers' consent did not comply with GDPR. In addition to the fine, the AEPD has ordered CAIXABANK to bring its processing operations into compliance with Articles 6, 13 and 14 of the GDPR.

This fine is a reminder to companies to ensure that their privacy notice provides sufficient detail to support the data processing activities that they are doing.



The UODO, Poland's DPA, has fined **Smart Cities** the equivalent of **£2,305** for failing to reply to its letter and for failure to provide access to personal data and other information needed for the UODO to perform its tasks.

A somewhat startling response from Smart Cities. Sometimes, in general, companies do not want to engage with a data protection regulator to avoid becoming on their radar. However, surely once you're already on the regulator's radar it is advisable - unless there is good reason not to - to do anything to minimise your stay there and fuel their further attention!

At the end of January, Datatilsynet, the Norwegian DPA, issued a draft decision with a notice to fine **Grindr** (a location-based "*social networking app for gay, bi, trans, and queer people*") the equivalent of **£8.6 million** (10% estimated annual turnover). A legal complaint was received by the Norwegian Consumer Council ("**NCC**") in January 2020. The NCC then filed the complaint citing unlawful sharing of personal data with third parties for marketing purposes, including disclosing user profile data, location data and that the fact that they are users of the app all without consent—which the Norwegian DPA has concluded is necessary. The DPA has also highlighted that, since the use of Grindr can infer someone's sexual orientation, this is special category data and needs appropriate protection.

It will be interesting to observe the final decision. Nonetheless, this case sounds an alarm to companies to have compliant collection of consent in place, with transparent information provided with respect to any data sharing.

The Norwegian DPA has had a busy start to the year. Whilst this comment is not dedicated to one fine in particular, in addition to the Grindr fine in late January, the EDPB has reported a further eight fines issued by the Datatilsynet in February. Several relate to the performance of credit ratings without a legal basis whilst another is for breach of confidentiality.

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