fieldfisher

Data Protection Times

April 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

Whilst this month's news leaves us in no doubt as to how central data is to our lives, the articles collectively remind us about the importance of the data protection principles. Regulators want to ensure that there is no mission creep in Covid vaccine passports nor any inappropriate retention of data. The fraught topic of surveillance concerns the EDPB in its opinion on UK adequacy under the GDPR...but surveillance today is not limited to states and law enforcement as individuals continue to install and use CCTV! A fine in Spain prompts individual users about how they too need to consider data protection principles if the household exemption does not apply. With the GDPR's third anniversary fast approaching there is increasing frustration in certain quarters about the enforcement of it. With such increase in AI activity perhaps it won't be too long before we get enforcement by AI!

Top of the Privacy Pops

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

5. **"Data protection does not constitute an obstacle for fighting the current pandemic".** The EDPB and EDPS issued a joint opinion on the data protection aspects of a proposed EU "Covid-19 Digital Green Certificate Framework". The opinion notes that the certificate must not be used to discriminate against individuals, and must be fully in line with the GDPR principles. The green certificate should cease to be used once the Covid-19 pandemic has ended, rather than the current scope to allow for future use with other epidemics. The "digital green certificate", which is to be operational by 21 June 2021, is aimed to make travel easier across the bloc (but should not be a pre-condition of free movement).

France has become the first EU member state to test travel certificates including vaccination certificates. Denmark and the Netherlands are also trialling other similar schemes to allow other areas of the economy to reopen. The Czech Republic data protection authority has issued its own opinion on this, including ensuring this is not compulsory.

Following last month's UK update, the UK Government is consulting on whether a Covid-19 vaccination should be required for staff at elderly care homes and as the country opens up considers how people will show their "Covid status".

4. **'Uber' impacts from automated decision making.** A Netherlands court has ordered that five British and one Dutch Uber drivers be reinstated after they were struck off as a result of a decision based solely on automated processing. Uber had been alerted of fraudulent activity on the drivers' accounts (allegedly mistakenly). Uber was also order to pay a daily penalty for each day it failed to comply with the court order, as well as damages.

3. **Are we 'adequate' yet?** The EDPB's opinions (GDPR and Law Enforcement Directive (LED)) on UK adequacy were adopted earlier this month. Whilst the EDPB agrees that there is alignment between the EU and UK laws, it outlined some concerns, which include how the UK's legal system will evolve, aspects of onward transfers and the inevitable mention and analysis of "lawful interception". This has resulted in a request for an extension for MEPs to review the opinions.

2. **European AI framework.** The EU Commission has released a proposal for a harmonised framework on AI. The framework seeks to impose obligations on both providers and users of AI, and focuses on three categories:

- Certain systems that are expressly prohibited in most instances (e.g., manipulative and exploitative practices).
- High-risk systems which will be subject to mandatory requirements (including relating to data quality and documentation). The draft list of high-risk systems includes AI used to evaluate creditworthiness.
- Other systems intended for human interaction or to generate/manipulate content will be subject to transparency obligations, regardless of risk level.

The proposal is GDPR-like in terms of fine levels and its extra-territorial effect.

1. **Apple and Google block privacy-breaching updates to NHS Covid-19 app**. The planned update would have asked users to upload their venue history after testing positive for Covid-19—in breach of Apple and Google's condition that the app must be decentralised (i.e. data kept on the user's phone, and not a centralised database). In other related news, Apple has announced that it will reject apps which fail to comply with new transparency rules and will ban those which reward users for turning on data tracking. #PrivacybyDesign

ICYMI

In case you missed it …

EU DPAs under pressure … As we approach the third anniversary of the GDPR next month, data protection authorities are facing criticism with respect to their lack of enforcement. The Irish DPC in particular is under increased pressure for the time it is taking to bring enforcement proceedings besides its handling of the Schrems case. The EU Parliament's LIBE committee will debate its resolution that "calls on the Commission to start infringement procedures against Ireland for not properly enforcing the GDPR" in a future plenary session. On 27 April, the Irish Commissioner, Helen Dixon, defended her office at a Joint Committee on Justice of the Irish Parliament, where she faced questions from MPs and Schrems himself.

EDPB Guidelines … The EDPB is consulting on its guidelines on the application of Article 65(1)(a) (the dispute resolution mechanism used between lead supervisory authorities and concerned supervisory authorities in the context of data transfers). The EDPB has also recently adopted its guidelines on the targeting of social media users.

Letters

Dear Data Protection Times

This is a bit of a morbid subject, but I think an important one in today's increasingly digital world: a recent article got me thinking about creating a 'digital will' and the data protection obstacles involved in this. I (and likely many others) have never put much thought into how many memories I have stored only digitally within a range of platforms, and the issues in preserving these in my absence. Due to understandable privacy grounds, the terms of service of many platforms prevent third parties from accessing a user's account. It was interesting to absorb the article's suggestions for preserving your online presence: e.g. regularly downloading data from social media sites; designating a 'legacy contact' to manage your accounts; and the facility offered by the state trustee in Victoria, Australia to create a 'digital register' of logins, alongside a will.

Anonymous, London

Dear Editor and fellow readers

Sometimes it's the small things in life that bring a smile, especially in these difficult times … Have you seen the EDPB's redesigned website? A fresh, elongated, triple column page to host all the latest EEA activity! I have noticed though how the website does not always list the latest DPA fines. Yet, it's extremely up to date on the news of Portugal's suspension of data flows to the US of Census 2021 data by the National Institute of Statistics.

Data Protection Expert, Poland

Dear Editor

I am presently engaged with a number of DPIAs to assist clients with the Age Appropriate Design Code and data relating to Covid-19. It has made me wonder how regularly companies revisit DPIAs and how mindful they are of the DPAs' blacklists, which specify situations where a DPIA is expected. Whilst completing a DPIA is time-consuming and can be extremely intense, many a client has reported how valuable they find the process especially to a product's or service's design beyond the compliance piece.

Data Protection Lawyer, Sussex

Data protection issues in Artificial Intelligence

Want to know about the core data protection issues here, some of the practical challenges they present and more detail on the EU Consultation? Then listen here to our team's webinar on our YouTube channel!

fieldfisher

RECENT DATA PROTECTION FINES

It has been reported that **Ticketmaster's appeal** of an ICO fine has been stayed until after the judgment of a civil action brought against Ticketmaster by a group of 795 affected customers. The £1.25m fine was issued in 2020, after a third-party chat bot used on the Ticketmaster site was found to have been infected by malware that scraped personal data and payment details of customers.

This case – along with other group civil claims (e.g. British Airways) – acts as a reminder to data controllers that, although data protection authority fines can be significant, they are not always the end of the story nor the most costly element, when it comes to the financial impact of data breaches.

Lloyd v Google LLC, Supreme Court hearing

The last week of April witnessed the hearing of Lloyd v Google LLC, which concerns the validity of Google's collection and use of browser generated data from more than 4 million+ iPhone users during 2011-12. It is now an anxious wait for the decision, which may be instrumental for future representative actions, of which there are a number waiting in the wings.

An unnamed individual has been fined by Spain's AEPD (Spanish) for violating the GDPR's principle of data minimisation. According to the regulator, the individual installed video surveillance cameras without authorisation.
Whilst organisations should already be aware of the data protection implications of using CCTV, individuals using home CCTV may also want to consider the impacts of this decision, especially given the rise in home security technology being used.

The Spanish regulator has fined Equifax €1m for several failures under the GDPR.

According to reports (original decision in Spanish), individuals complained about Equifax's use of their personal data which was publically available. Equifax had also failed to provide the individuals with a privacy notice. Equifax apparently had no legal basis for processing the personal information.

Organisations should remember that just because information is publically available they do not have "free rein" to use it. You still need to comply with your obligations under data protection laws.

Did you know … the Spanish data protection authority (the AEPD) retains the money it receives from issuing financial penalties for GDPR breaches?

As we reported last month, the AEPD recently issued a multi-million € fine to Vodafone Spain. Whilst the Data Protection Times can't help but think there is a conflict of interest at play when a DPA has a financial interest in the fines it awards we are assured by a Spanish qualified colleague that this is in accordance with Spain's Organic Law 3/2018, Article 46.3. Also the income derived from the development of its powers, including the powers set out in Article 58, GDPR is not its only source of income. As ever, it's far better knowing the bigger picture!

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