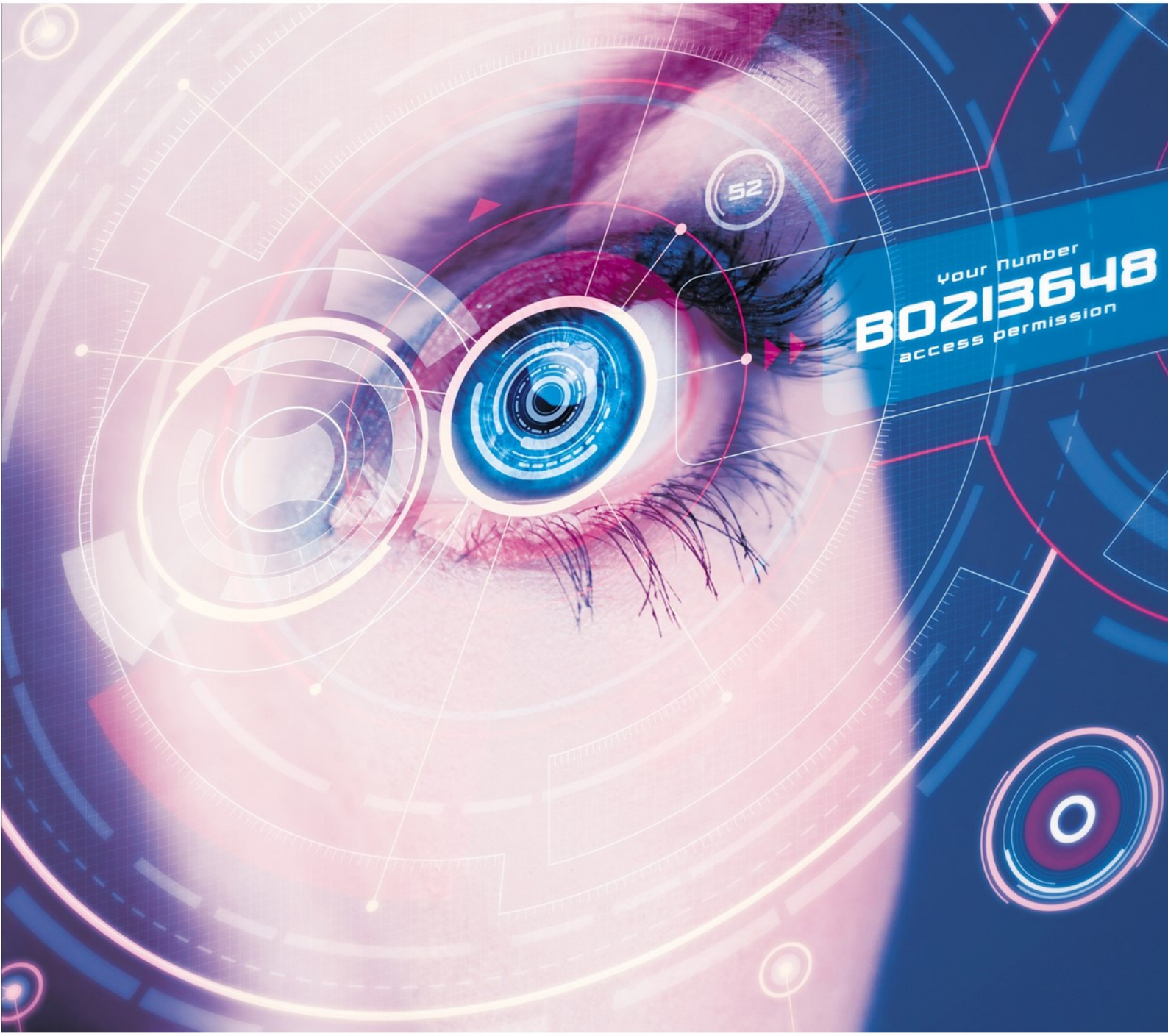
fieldfisher

Data Protection Times

March 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

As the UK's lockdown restrictions begin to ease, socially and economically, the UK government and companies are thinking about how we can safety interact whilst the pandemic remains so prevalent and variants threaten to challenge existing vaccines. Data protection is central to these efforts and the proportionality of data collected and retained needs careful consideration. Public health is of the utmost importance and there is clearly some balancing of interests to be done. The government's call for evidence may not be closed but this is a fascinating arena to be involved with from a data protection standpoint.

Whilst there's been no recent announcement about the UK's adequacy status, an adequacy decision for South Korea is moving forward and negotiations for a replacement / amended Privacy Shield gathers pace. It is clear data today needs to travel seamlessly across continents. The EDPB has set out an extensive work programme whilst the ICO cements its position in the post Brexit world in a Memorandum of Understanding with DCMS on future adequacy assessments. Guidance and fines continued to be issued and the Dutch DPA's latest fine against Booking.com highlights the importance of knowing what to do in the 72 hours post a data breach. When did you last do a table top exercise? How would your procedures work remotely at present? Preparation is key.

This month we bring you a special feature on what's happening with regard to children's data and online harms. In short, a lot.

Top of the Privacy Pops

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

6. **A load of rubbish? AI 'litter cam' trial.** New AI software has been developed which matches footage of littering motorists to the number plate of the vehicle—and then automatically issues a £90 fine to the car's owner, which can increase to £120 if not paid within 15 days. The software is being trialled in Kent, with a wider rollout anticipated in the future.

   This regime will undoubtedly be controversial and creates something of a privacy minefield, as a result of the combination of video footage, automatic number plate recognition and the automated decision-making process involved in the fine's issue. Maidstone Borough Council's says its use of the technology is as a deterrent. #KeepBritainTidy

5. **Are Covid-19 vaccine passports becoming more likely?** The debate rages on as to whether vaccine passports will be rolled out or required for certain pockets of society. The UK Government has issued a call for evidence as part of its review on whether "Covid-status certifications" should be used. The consultation was opened for 2 weeks only and closed on 29 March 2021. Others are taking matters into their own hands—care home provider, Barchester Healthcare, has introduced Covid vaccine passports for its staff. The government has already committed to trialling vaccine passports at particular sporting and social events. Similarly, in Barcelona a Covid screening system was used for 5,000 people to attend a rock concert. This may well become a new way of life but privacy issues, discrimination and disability considerations will need to be considered and balanced against any formal decisions in the UK. The ICO has engaged with the government to foster public trust in any such system.

4. **Privacy Shield 3.0?** The EU Commissioner and the US Secretary of State released a press statement that the "*US Government and the European Commission have intensified negotiations on an enhanced EU-US Privacy Shield framework*". Is the Privacy Shield 3.0 getting closer? It will be interesting to see how any decision overcomes the concerns raised in Schrems II and for how long any new system remains unchallenged!

3. **Adequacy for South Korea.** Talks between the Commission and South Korea regarding adequacy concluded this month. The Commission will now proceed with the decision-making procedure for adopting an adequacy finding, which includes obtaining an opinion from the European Data Protection Board (EDPB).

2. **What's on the horizon?** The EDPB has released its 2021-22 Work Programme. The programme focusses on four pillars: harmonisation and compliance, enforcement and cooperation between SAs, fundamental rights with new technologies and promotion of EU standards globally.

1. **The EDPB and EDPS have adopted a joint opinion on the Data Governance Act**, acknowledging the "legitimate objective" of improving conditions for data sharing in the internal market. They have called on co-legislators to ensure the future DGA will be aligned with EU data protection legislation—a development to watch out for in future.

Letters

Dear Data Protection Times

As a Swiss resident and avid reader of your publication, I thought I would write in following the recent referendum in which 64.4% of Swiss voters rejected proposed plans for a digital identity verification system due to privacy concerns.

The crux of voters' concerns seems not to be the introduction of such a system per se — but the use of private companies to provide it. Reports suggest that citizens' mistrust in private companies swung the vote, with voters making clear that any such system should be exclusively state-managed.

It has been interesting to consider how privacy concerns materialise not only from what is done with personal data, but also who is doing it.

Intrigued voter, Geneva

Get Data Protection Fit with Fieldfisher's YouTube series

Why not ***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 am particularly pleased to see both the EDPB and the ICO actively engaging with stakeholders with respect to their forthcoming guidance. The ICO has laid out its plans for its anonymisation guidance whilst the EDPB is to host an event on processing personal data for scientific research purposes, similar to a previous event it did on legitimate interest.

I sincerely hope that such engagement will produce pragmatic guidance for those of us working in house who on occasion have to grapple with some rather theoretical, unrealistic guidance that is quite divorced from real world examples.

In house counsel, Birmingham

ICYMI

In case you missed it: These headlines also caught our attention

The EDPB adopted guidelines on virtual voice assistants. The guidelines look at the most relevant compliance challenges and recommendations for addressing them. Also published and adopted after consultation were the guidelines on processing personal data in the context of connected vehicles and mobility related applications

The Urząd Ochrony Danych Osobowych, data protection authority in Poland, published advice on the use and processing of biometric data. The guidance reiterates the serious privacy risks inherent in the processing of biometric data, the initial need to carry out a DPIA (Data Protection Impact Assessment) and how the GDPR principles of necessity, purpose and proportionality must be taken into account before the construction of any biometric database.

The ICO and the Secretary of State for the Department for DCMS have agreed a Memorandum of Understanding setting out each organisation's role in future adequacy assessments under the UK GDPR. It will be interesting to watch which countries are considered first.

The ICO issued new guidance on the use of personal data in political campaigning. The guidance is intended to provide clarity and advice in light of amended legislation and developing technologies and campaign methods.

Special Feature

Children's Data and Online Harms

At the beginning of March, the ICO reminded stakeholders that there was only six months (now five) until the Age Appropriate Design Code (AADC) - a.k.a. the Children's Code - becomes applicable on 2 September 2021. Besides the AADC, we are starting to see a flurry of activity related to children's data and online harms.

Online harms legislation is not exclusive to children and will also focus on content delivered to adults. However, companies when considering their compliance activity with respect to the AADC are encouraged to think about the bigger picture and the legislation on the horizon. Whilst the UK and the European Commission are yet to publish draft legislation on online harms there is a considerable amount happening in this space and children's data.

UN Committee on the Rights of the Child

On Wednesday 24 March, there was a celebratory webinar about the UN's adoption of General Comment No.25 on children's rights in relation to the digital environment. This adoption makes it explicit that children's rights apply in the digital world and requires all 196 states who are signatories to the Convention to report formally on their provisions in this area. You can listen to the webinar here.

Safety Tech

Taking place within the hour of this webinar was the UK's first Safety Tech expo. The full agenda highlights the breadth of work going on here and the objective to create a safer environment online, in particular for children. All the recordings from the online conference are available here. There were some superb discussions with companies detailing what best practices they are employing. For example, Electronic Arts discussed how it has developed a Positive Play Charter. On that note, it will be interesting to monitor the UK's three-year research project about play online and how this can be done effectively and safety.

Age verification

Age appropriate application is the third standard of the AADC which at times will require a controller to "establish age with a level of certainty that is appropriate to the risks" of the data being processed. Whilst the AADC does not prescribed one particular approach it does discuss third party age verification services. Also in March, the 5Rights Foundation, a charity working for a digital world where children and young adults can thrive, published its report on age verification *But how do they know it is a child?*

Separate to this work, DCMS (the Department for Digital, Culture, Media and Sport), the Home Office and GCHQ have also been collaborating on the **Verification of Children Online (VoCO)**. Their report states that there is a need for the age of children, using services online, to be known by the service provider so that the child user is shown appropriate content. What these work streams highlight is the direction of travel in the UK and the resources that children's online safety is receiving. The government's latest Online Harms White Paper was published at the end of 2020, although at the end of March 2021 a report on "Digital opportunities and harms" dated April 2020 was published. Given the lapse in time since the report was authored and how children have engaged online over the last 12 months throughout the pandemic it is conceivable that an update will be required.

Video sharing platform guidance

Ofcom, which is expected to be the regulator of any online harms legislation, has published a consultation on guidance for VSP providers to protect users from harmful content. The consultation is open until 2 June 2021.

Europe and children

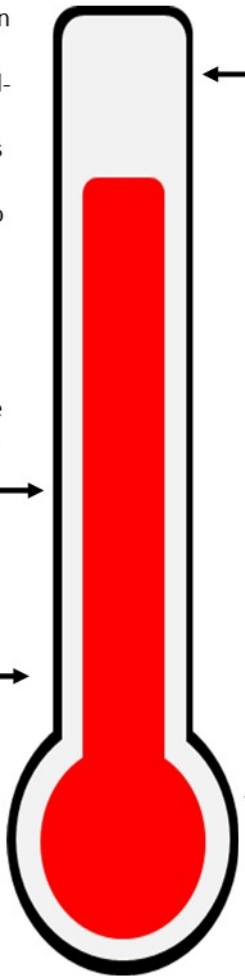
Ireland's consultation on its draft guidance on children - *Fundamentals* - closed at the end of March 2021, so further guidance can be expected in this area from another DPA. In March the Netherlands (Dutch only) also release a code which is based around the UK's AADC. The EDPB's work programme 2021-22 specifically states that guidance on children's data will be published during this time.

It is quite phenomenal how much is happening but the real challenge is how we connect this activity on a global scale across jurisdictions and between all stakeholders to ensure children are safe online.

fieldfisher

RECENT DATA PROTECTION FINES

Booking.com has been fined **€475,000** by the Dutch DPA for failing to report a data breach within the mandatory 72 hour period following the notification of a breach. It reported it 22 days after the breach was discovered. The breach involved criminals stealing the personal data of more than 4,000 Booking.com customers, including the credit card details of nearly 300 customers. The criminals used the personal data to engage in 'phishing', an attempt to rob the customers by duping them into believing they were being contacted by hotels that they had legitimately booked via Booking.com.
The fine emphasises the regulator's view that reporting a data breach on time minimises the damage caused to customers by not giving criminals the opportunity to exploit stolen data. It also highlights the responsibility on large organisations to act quickly when things go wrong with regard to personal data.



Vodafone Spain has been fined (Spanish) approximately **£7million** by the Spanish regulator. Over half of this fine relates to breaches of the GDPR including data transfers without ensuring appropriate safeguards were in place and contacting individuals without consent. Reports suggest that the AEPD found that Vodafone Spain had little control over the data because so many of its operations are outsourced.

Organisations should be mindful of the data processing activities that they outsource or subcontract to ensure they have adequate knowledge and control over the whereabouts and safeguards for personal data besides records of any consent collected.

The Dutch DPA has fined an **Amsterdam hospital EUR 440,000** for failing to prevent unauthorised employees from accessing medical records. It was found that the hospital had not implemented adequate computer security measures or sufficient checks on who was viewing the records. The DPA recommended that the hospital use a two-factor authentication process to ensure that only authorised persons view the medical records.

This story serves as a further reminder of the importance of implementing appropriate technical and organisational security measures — particularly where the processing involves special category data.

The ICO continues to issue fines for unlawful marketing. This month against two different companies.

Leeds Work, a lead generation company, were fined **GBP 250,000** for sending over 2.7 million marketing texts during the pandemic without valid consent.

Muscle Foods were fined **GBP 50,000** for sending over 142million unsolicited communications to individuals.

UK readers should be mindful of the fact that valid consent is needed to send marketing communications like this.




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