fieldfisher

Data Protection Times

Summer 2021

This edition of the Data Protection Times provides a round-up of the latest data protection developments that have caught the attention of Fieldfisher's Privacy, Security and Information law team over the summer.

A note from our editor, Hazel Grant

We hope that you have managed some sort of holiday this summer, although we expect that your choice of destination was far more limited than the portfolio of Transfer Impact Assessment templates we now have available. Data will travel! Despite Parliaments and Courts in recess, the news continues unabated. The Luxembourg DPA has issued a staggering fine against Amazon (to be appealed) for €746m (seven hundred and forty six million) with an interesting summary published by the CNIL days after a press announcement. The original complaint was made to the CNIL who passed it on to Luxembourg. Data protection is such an #influencer that, in our summer bundle of news, we bring you details of how China has adopted its first law to solely protect personal data and is—you've guessed it—likened to the GDPR. Further calls have been made from Congress in the US, this time to a dozen gaming companies, to apply the UK's Age Appropriate Design Code to children in the US. The ICO has thankfully announced that it is considering adopting existing models of data transfer agreements, whilst the preferred candidate for the next Information Commissioner's role, John Edwards, now just awaiting his appointment from HM the Queen, is another member of the Commonwealth! ...and, without further ado, the UK Government releases its consultation to overhaul UK data protection provisions and the ICO!

Top of the Privacy Pops

The Data Protection Times counts down the most prominent global developments from Summer 2021.

5. Austrian Supreme Court referral to CJEU

Austria's Supreme Court has asked the CJEU for clarification on the legality of Facebook's processing of personal data after campaigner Max Schrems brought a case before it. The Court in Luxembourg will now decide whether the US giant complied with the GDPR with respect to data minimisation and explicit consent.

Prior to the GDPR, Facebook had argued that users had given consent to the processing of their data however following the strengthening of consent requirements imposed by GDPR, Facebook has changed the legal basis of processing data to necessary for the performance of a contract.

The CJEU will need to determine whether Facebook is trying to undermine the stricter legal basis of consent by reinterpreting its services as contractual performance. The CJEU will also need to examine whether the use of personal data from other sources such as advertising and the collection of data from "Like" buttons is compatible with the principle of data minimisation.

4. Guidelines on Codes of Conduct for Transfers

The European Data Protection Board ('EDPB') is welcoming feedback on the Guidelines on codes of conduct as tools for transfers until 1 October 2021.

The guidelines intend to clarify the application of Articles 40(3) and 46(2)(e) of GDPR and will provide guidance on the content of codes of conduct, their adoption process as well as the requirements to be met and the guarantees to be provided by a code of conduct so it can be used for transfers.

Once the provisions have been approved by the relevant supervisory authority and granted general validity within the EEA by the Commission, a code of conduct may be adhered to and used by controllers and processors not subject to the GDPR located in third countries to provide appropriate safeguards to transfers of data outside the EU.

3. British Airways

British Airways has settled a data breach claim after over 400,000 of their customers were left vulnerable when personal data was processed without adequate safety measures and was subsequently left exposed to a cyber-attack. BA was originally fined £183m for the breach in July 2019, however this was significantly reduced to £20m following representations made by the company.

The ICO conducted an investigation that confirmed weaknesses in BA's IT security that could have been remedied with measures that were readily available at the time. BA's settlement did not include an admission of liability and the settlement amount and terms remains confidential. Law firm PGMBM have confirmed that the terms of settlement include the provision for compensating those affected by the data leak. Such claims brought by data subjects are in addition to the regulator's fine.

2. Enforcement Action Against Amazon

Luxembourg's National Commission for Data Protection ("CNPD") has issued a penalty notice against Amazon of €746 million (the largest GDPR fine to date) together with an injunction to make its processing activities compliant within a period of 6 months. Failure to adhere with the injunction will incur a further penalty of up to 0.1% of the fine, i.e. €746,000. Details of the decision have not been made public but will be made so once all remedies have been exhausted in accordance with Luxembourg law. Amazon has indicated that it will vigorously defend itself on appeal.

Interestingly, the CNIL (the French DPA), to whom the original complaint about Amazon was made by La Quadrature du Net ("LQDN"), published a statement (French) days after the press revelation on this fine.

The statement discussed how LQDN represented 10,065 users and their complaint focused on the fact that Amazon had no lawful basis for its processing of personal data in relation to its behavioural analytics and targeted advertising. LQDN's complaint discussed why this was the case and that, in the absence of a legal basis, the LQDN claimed that Amazon's processing is therefore unlawful and particularly violated Article 6 of the GDPR. LQDN called for the following measures to be made against Amazon:

- the prohibition of behavioural analysis and targeted advertising, in application of Article 58(2)(f), GDPR; and
- an administrative fine which, due to the "massive", "ongoing" and "clearly deliberate" nature of the violation, must be the highest possible, pursuant to Article 83(2) and (5), GDPR.

1. Ireland's DPC fines WhatsApp €225million after EDPB interjects

Back in December 2018, Ireland's DPC began an investigation into whether WhatsApp Ireland Limited had fulfilled its transparency obligations with respect to the information and the clarity of the information it provided to its users and non-users of its service. Some two years later in December 2020, the DPC, as lead authority for WhatsApp, proposed a fine of between €30-€50m in its draft decision for Concerned Supervisory Authorities to consider, eight of whom ultimately objected. With a lack of consensus amongst the supervisory authorities, a dispute resolution process started on 3 June 2021 in accordance with Article 65, GDPR.

By 28 July 2021, the EDPB adopted a binding decision that directed the DPC to:

- amend its decision regarding infringement of transparency;
- reassess and increase its proposed fine; and
- reduce the timescale it had provided to WhatsApp in order for the company to make its processing compliant.

Whilst the draft decision focused on severe breaches of Articles 12 – 14, GDPR, the EDPB highlighted specific defects in information provided that impacted "users' ability to understand the legitimate interests being pursued".

The EDPB decided that the turnover of an undertaking needs to be considered when calculating a fine to ensure the fine is effective, proportionate and dissuasive. In in this matter, the EDPB said that the consolidated turnover of the parent company (Facebook Inc.) is to be included in the turnover calculation. In addition, the EDPB determined that with respect of Article 83(3), GDPR, all the infringements in this matter should be taken into consideration in calculating the total fine amount.

In the draft decision, the DPC included a period of six months for WhatsApp to bring its processing operations into compliance. Yet, due to the significance the EDPB attached to this happening in the least amount of time possible, the deadline was cut to three months.

WhatsApp has confirmed that it will appeal the decision both in respect of the transparency provided in 2018 and the level of the fine. It will be interesting to monitor this appeal and see how it concludes with respect to the level of transparency requirements required by Articles 12-14 and how these are presented to data subjects in practice.

ICYMI

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

ICO calls for views on data protection and employment practices

The UK's Information Commissioner's Office is seeking input on data protection and employment practices from stakeholders such as employers, workers, recruitment agencies and more. The ICO has issued this call in anticipation of a refresh of its guidance in this area. The regulator aims to issue a more user-friendly online resource that will, amongst other modernisations, reflect changes in the ways that employers interact with their employees and use technology.

The consultation closes on **21 October 2021**.

ICO's review of its "Explaining decisions made with AI" guidance

The ICO published a blog reviewing its guidance on "Explaining decisions made with AI" a year on.

The guidance, which was produced as a "best practice" document, was reviewed and feedback sought from 56 organisations of different sizes and sectors.

Whilst the feedback was positive, areas of improvement focused on the length of the document. As a result the ICO has added "at a glance" sections to the document. The ICO is also intending to add case studies to the guidance, which will be beneficial. Details of good case studies can be sent to AI@ico.org.uk.

ICO Property Raid: The ICO have raided two properties as part of their investigation into the leaked CCTV footage of politician Matt Hancock kissing his aide. The computer equipment and electronic devices have been seized in connection with alleged breaches of the Data Protection Act. Emcor, who provided CCTV services to the Department of Health, reported itself to data protection investigators.

UK- Brexit: The ICO has published updated guidance for organisations, explaining data protection following Brexit. This follows the adequacy decisions granted by the European Commission and the Law Enforcement Directive. The ICO's guidance is tailored to provide a more detailed understanding of data protection law to DPOs and those with specific data protection responsibilities.

New Information Commissioner

New Zealand's Privacy Commissioner John Edwards was announced as the preferred candidate to be the successor to Elizabeth Denham when her term as Information Commissioner expires. Mr Edwards appeared before the DCMS Select Committee on 9 September 2021, who approved of Mr Edwards' appointment.

EDPB Guidelines ... The EDPB has now published its its final version of its guidelines on the concepts of controller and processor. The guidance provides detailed analysis of the of the role of joint controllers as well as the controller/processor positions.

EDPB overview on resources by Member States to DPAs

The EDPB has issued a report on resources made available to supervisory authorities and enforcement action. This comes following a request from the LIBE Committee for these statistics. There's a rich level of detail to consider.

Whilst some supervisory authorities' budgets have increased, the report notes that the vast majority of SAs need more resource. For those interested, the report provides an overview of the number of cases and complaints and fines issued by SAs. There are details on employees per SA, the number of cross border enforcement cases as well as the number of cases based on data breaches.

At first glance it may seem that number of complaints are dropping off. Alas, the figures provided for 2021 only go up to 31 May 2021.

TikTok Taskforce

Following the establishment of TikTok in Ireland, the EDPB has decided to disband its TikTok Taskforce and pending cases raised in Denmark, Netherlands and France have now been transferred to the Irish DPC. The Irish DPC can now add TikTok to the growing list of companies over which it is designated the leading supervisory authority under the One-Stop-Shop procedure.

China adopts new privacy law

On 20 August 2021, China's National People's Congress officially passed a law designed to protect personal information of natural persons in China. The new law is called the Personal Information Protection Law (PIPL) and it will come into effect on 1 November 2021. This is the first law China has adopted that is designed solely to protect personal information. Our Chinese colleague, Zhaofeng Zhoe explains in this LinkedIn post the similarities between PIPL and the GDPR. PIPL has extra-territorial effect and sets out (among other things) lawful bases for processing personal information, principles of processing data, data subjects rights and obligations when transferring data outside China. Beware though of the distinction between controllers and processors! "*Under the PIPL, data processors are similar to controllers under the GDPR, while trustees under PIPL are similar to processor under the GDPR*".

Letters

Dear Data Protection Times

Apple, which has historically promoted its privacy-first approach to its technology as somewhat of a U.S.P. recently announced plans to automatically scan US iPhones for images of child abuse, in a move designed to protect children.

In this digital age, where the complexity of technology, or lack of regulation, has so often enabled online misdemeanours to go under the radar, we (the public; the press…) are often critical of tech companies for failing to intervene sooner (or at all). For example, there has been condemnation of social media companies' failures to combat misinformation about vaccinations or electoral candidates. In this context, one can see why Apple is looking to publicly take responsibility by introducing these features – and the enhanced protection of children is undoubtedly an important area that should be addressed.

I see though that Apple has for the moment paused the implementation of this project due to public comment and to allow time for it to seek feedback and make improvements. It is interesting (to me!) to see the difficult balancing act that is required between public good and privacy rights playing out again—this time in the private sector.

iPhone addict, Swansea

Dear Editor

It has been written about here before, but I wonder whether all privacy advisers need to learn to speed read as I suspect organisations will not start offering "reading weeks" to keep up with the vast swathes of material that is continually produced. Ireland's DPC's WhatsApp decision and the EDPB's binding decision together total over 350 pages. I heard from a colleague that they're not easy to read in tandem either due to their individual styles, format and language! Any suggestions?

Yours, ***a conscientious but time limited DP practitioner, Manchester***

Children's Data

Besides the ICO's update to its Children's Hub with a practical design guide for developers, the ICO has also approved its first certifications including two from Age Check Certification Scheme (ACCS) which focus on age assurance and children's online privacy.

Fieldfisher Webinar

Thursday 23 September 4pm BST

Unpicking the proposed UK regime on international data transfers. Divergence from the EU?

Join us to hear about the ICO's consultation on international data transfer compliance under UK law. What are the practical implications for those transferring data out of the UK and how does this IDTA difference from the EU regime? Register here.

The CNIL (the French data protection authority) has published 8 recommendations to enhance the protection of children online. In June 2021, following a public consultation and a survey on the digital rights of minors, the CNIL adopted a set of recommendations regarding the processing of minors' data online. A minor, unless specified otherwise, is a person under 18, which (like the Age Appropriate Design Code) adopts the definition of a child in the UN Convention on the Rights of the Child. The recommendations focus on the following themes:

- regulating the ability of minors to act online;
- encouraging minors to exercise their rights;
- supporting parents in digital education;
- seeking parental consent for minors under the age of 15;
- promoting parental control tools that respect minors' privacy and interests;
- reinforcing transparency and the rights of minors through design;
- verifying the age of the minor and the parents' consent in respect of their privacy; and
- providing specific guarantees to protect the interests of the minor.

For each of these eight themes, the CNIL has adopted short and general recommendations. For example, the CNIL did not recommend any specific age verification mechanisms. However it does state that such mechanisms: (1) should be in line with the principles of data minimisation and proportionality; (2) should be easy to use; (3) should be strong and robust for high-risk processing; (4) may rely on a third party; and (5) may rely on industry-wise norms. Similarly, the CNIL highlighted general considerations regarding consent mechanisms, for example, stating that it is necessary to take into account the minor's level of maturity when obtaining his or her consent and that it is sufficient to obtain the consent of only one holder of parental responsibility.

As a result, some of the recommendations pave the way to a dialogue with stakeholders to make the recommendations technically operational and more practical. The CNIL also intends to publish a second set of recommendations once it has deepened its understanding of the involved legal issues.

Whilst these recommendations are non-binding, the fact that the CNIL has published them in English is a demonstration that they are important for global companies offering goods and services to children in France to consider and implement.

China too has shown how it is concerned about the wellbeing of children and their engagement online! The Chinese government is severely limiting the time under 18s can play games online to one hour on a Friday, weekends and public holidays. Any child outside China, complaining to their parents or guardian about time limits imposed in their household, will undoubtedly be reminded of how strict things could be!

Endorsing the trend and upsurge globally about what's happening in the field of children's data, the IAPP has launched its own children's page.

Biometric data processed through a facial recognition system found unlawful by the AEPD

Mercadona, a chain of supermarkets in Spain, began the use of a facial recognition tracking pilot scheme in 40 - 48 of its stores in May 2020. The purpose of facial recognition was to detect any individuals who were subject to a restraining order from the supermarket. The system applied a filter to the supermarket's existing video surveillance cameras and, once a relevant person had been identified, it would issue an alert to be verified by the on-site security staff.

Following complaints, the AEPD began an investigation which concluded that none of the exemptions under Article 9 (for the processing of sensitive data) were available to Mercadona and that its processing was unlawful and not legitimate. The processing did not adhere to the principle of data minimisation, transparency obligations were not fulfilled and a DPIA that was conducted was deficient because it had not taken into account the processing of employees' data and that of other customers not subject to a restraining order. The fine was for €2,520,000. The decision, whilst only available in Spanish, highlights the importance of completing a DPIA ahead of processing biometric data, and the need for companies to focus on their transparency obligations and ensure that they have an appropriate reason for processing sensitive data.

Recent Data Protection Fines

Aside from the fines against Amazon and WhatsApp that featured in our Privacy Top of the Pops (on page 2), we also found this enforcement action noteworthy.

Foodinho, the food delivery platform, has been fined €2.6m by the Italian SA for several serious infringements, such as unlawfully processing riders' data, failing to implement suitable safeguards to ensure accuracy and fairness of the algorithmic results that were used to rate riders' performance and failing to adequately inform its employees on the functioning of the system.

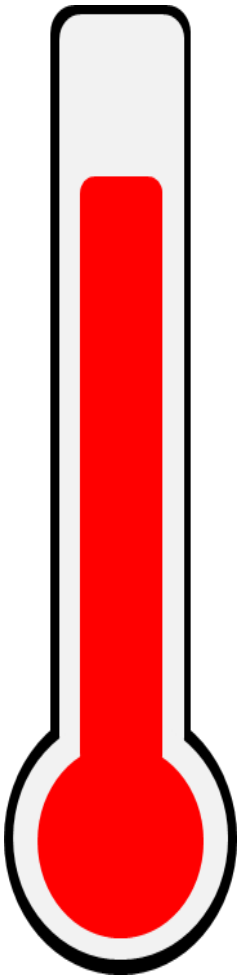
Foodinho were given 60 days to start implementing the measures required to remedy the shortcomings, with an additional 90 days granted to finalise the rehauling of its algorithms.

Not always given proportionate attention, this decision emphasises how data protection and a company's data protection practices extend to employee's personal data.

AG2R La Mondiale, the French multinational insurance firm, has been fined €1.75m by the French data protection authority ('CNIL') for retaining data belonging to millions of prospective and current clients beyond the required time limits.

This included retaining the data of 2,000 prospective clients who had not been in contact with AG2R La Mondiale for over 3 years and retaining the data of over 2 million current clients beyond the necessary period.

In relation to telemarketing, they were also found to have breached GDPR by not informing data subjects of the processing of their data and the right to object to such processing.



TikTok has been fined €750,000 by the Dutch DPA for violating the privacy of young children in the Netherlands by not providing a privacy notice in Dutch from May 2018 to July 2020 when users installed the app.

By not offering their privacy statement in Dutch, TikTok failed to provide an adequate explanation of how the app collects, processes, and uses personal data.

TikTok has since published their privacy notice in Dutch and are appealing the fine.

Transgender charity Mermaids has been fined £25,000 for failing to keep the personal data of its users secure.

Mermaids' data breach stemmed from insufficient security settings on an internal email group which was used from August 2016 until July 2017. It led to personal data of 550 people being searchable online for nearly three years. Some of this data related to physical and mental health, as well as sexual orientation. The charity only became aware of the breach in July 2019.

During the ICO's investigation it was discovered that Mermaids had a negligent approach towards data protection, including inadequate policies and a lack of staff training. Following on from the investigation, Mermaids has made significant improvements to its data protection practices.

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