fieldfisher

Data Protection Times

June 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

Undoubtedly the EU's new Standard Contractual Clauses are the headline of June 2021. After the initial dissection, the work now begins on how to transition to them for existing and new contracts alike. Creating a strategy with timeline and refreshing a business's data mapping will greatly assist, what could be, a time intensive task. At the 11th hour the UK received adequacy to the relief of many. Elsewhere, facial recognition and the use of biometric data per se is creating a lot of discussion and regulatory opinions on the safeguards needed to ensure fair processing. It's interesting to note the calls in the US to implement the ICO's Age Appropriate Design Code. Whether this leads to the desired outcome is another matter but it clearly shows the direction of travel with regards to children's data.

Top of the Privacy Pops

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

5. **Google provides commitments for its Privacy Sandbox.** You will no doubt be aware that Google is phasing out the use of third party tracking cookies. Google has been working with the CMA and the ICO to produce commitments that its new Privacy Sandbox will adhere to, to avoid being anti competitive. The collaborative working of the ICO and the CMA reflects the importance of data protection and competition. You can learn more about the future of cookies in our webinar here.

4. **NHS data pool delay.** Recent reports of the UK's NHS Digital's plans, to pool the medical records of 55 million UK patients onto a database and share them with third parties, have sparked warnings from privacy campaigners and GPs alike. Due to such pressure and overall lack of clarification for patients, the government has delayed the move for another two months. Perhaps this will allow the government time to create a new name for the programme too, which is presently referred to as the **GPDPR** (GP Data for Planning and Research)!

   The database would be available to academic and commercial third parties for research and planning purposes. Whilst NHS Digital states that data will be anonymised, it will be given codes that can be used to re-identify the patient where there is a "valid legal reason" to do so. Individuals can opt out of having their record included on the database by sending a letter to their GP.

3. **The EDPB and the EDPS publish a joint opinion on the proposed AI Act.** The Opinion calls for a prohibition of social scoring by private companies as the act currently only prohibits social scoring by public authorities or on their behalf. It also calls for a ban on the use of AI for automated recognition of human faces, as well as other biometric signals. Calls are also made for a ban on the categorisation of individuals into clusters on the basis of special category data and an almost complete ban on the use of AI to infer emotions.

   The Opinion also shows concern over how notice is given to individuals who are subject to AI identificatication systems in public spaces. The Opinion is critical of the Act for only requiring providers of AI systems to carry out a risk assessment rather than the users, who will usually be the data controllers and therefore in a better position to assess the risks for their specific use of the AI system.

2. **The UK receives adequacy.** With a couple of days to spare before the 30 June 2021 deadline, the European Commission adopted two adequacy decisions for the UK with respect to the GDPR and the Law Enforcement Directive. Perhaps a somewhat inevitable outcome given the UK had until 31 December 2020 followed the EU GDPR. The decision is valid for four years and whilst data protection provisions do not need to be the same, they do need to be essentially equivalent. The authors of the UK TIGRR Report need to heed this criteria since the suggestions made in their report, pp49-54, calling for a replacement of the GDPR, could put the two data protection regimes on entirely different paths.

1. **New EU SCCs and finalised EDPB Recommendations**. It's been a long time coming, with the existing SCCs dating from 2001, 2004 and 2010 and the GDPR now applicable for three years ... With their four module format the SCCs provide some formal provisions for processor to (sub) processor agreements. The EDPB also published its final recommendations on supplemental transfers tools. It is hoped that the updated SCCs will prevent a Schrems III judgment. Time will tell.

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

The ICO has published the first chapter of its new draft **guidance on anonymisation**, pseudonymisation and privacy enhancing technologies. You can read the Fieldfisher blog on the main takeaways and practical implications of the guidance here.

Biometric data The UK Commissioner has released an opinion on the use of live facial recognition in public places by private companies and public organisations.

There has been much coverage of biometric data and its misuse in EU fines this month. Stockholm's public transport network, SL, (paywall) has been fined €1.9m for equipping ticket inspectors with body cameras for recording incidents but they had not informed the public about this surveillance. Again in Sweden, a 2019 decision of the DPA against a school for using facial recognition for school attendance, was upheld by the Court of Appeal, (paywall) which noted that consent could not be voluntarily given and therefore could not be used as the legal basis for using facial recognition. UAB VS Fitness, (paywall) a sports club in Lithuanian was fined after a user complained that entry was conditional on of a fingerprint scan being given.

Due to the sensitive nature of biometric data, when embarking on its use, it is essential that data protection compliance is consider from the outset and throughout a project.

Children's Data A US senator and several members of Congress have called on the CEOs of the largest US tech companies to apply the ICO's Age Appropriate Design Code to US children since the Code's remit goes far beyond that of the US' COPPA regime.

Companies providing goods and services or monitoring the behaviour of children in the UK, have until 2 September '21 to become compliant with the Code.

Letters

Dear Data Protection Times

It has come to my attention that 'Noyb' (or 'None of your business', an organisation headed up by privacy campaigner Max Schrems) has launched an attack on websites it deems to be non-compliant with cookie banner law. Noyb has sent over 500 draft complaints to websites about their apparent failure, along with Noyb's own guidance purporting to show the path to compliance. Thousands more complaints are threatened. Noyb states that, if a website in receipt of one of its complaints fails to rectify its practices within one month, it will file a formal complaint to an enforcement authority.

One can only imagine the panic that this will be generating amongst website operators across the continent — not to mention amongst the (often already under-resourced) regulators anticipating the flood of complaints!

Dedicated reader, Berlin

Dear Editor

It seems to me that the potential fall out from data protection civil claims could far exceed a regulatory fine and harm to reputation. The details that a Dutch consumer group will bring speculative class action proceedings against TikTok for €1.5 billion shows how expensive these claims can be. This is in addition to a similar class action in the UK.

Clearly data protection, once considered a largely non contentious subject, is shaping itself to be quite a generator of litigation too.

A non litigator, Republic of Ireland

Data transfers

June was an extraordinary month with regards to data transfers and demonstrates the importance attached to the protection of an individual's personal data in the EU and UK, besides the need for pragmatic solutions in a digital centred world. Attention went beyond the new SCCs and UK adequacy decision to updates on the EU-US transfer mechanism and a draft adequacy decision for South Korea. Now that we have passed the date of the summer solstice we eagerly anticipate the publication of the ICO's SCC. Here, we take a further look at what has been a very busy month for international data transfers and discuss some of the key developments.

New EU SCCs On 4 June, the European Commission adopted new SCCs for the transfer of data to third countries. The new SCCs retain the 'modular' structure of the draft issued in November of last year, which allows parties to select the modular clauses applicable to the nature of their data transfers. The four modules cover: controller-to-controller transfers (module 1); controller-to-processor transfers (module 2); processor-to-processor transfers (module3); and processor-to-controller transfers (module 4).

There is a transition period for adopting the new SCCs. For new agreements, the existing SCCs can be used for 3 months until 27 September 2021. All existing transfers will need to move to the new SCCs by 27 December 2022. Whilst that date may seem a long way off as we enjoy the summer weather and sports, it comes straight after the Christmas period so data exporters and importers alike need to plan and consider their strategy of adopting and transitioning the new SCCs.

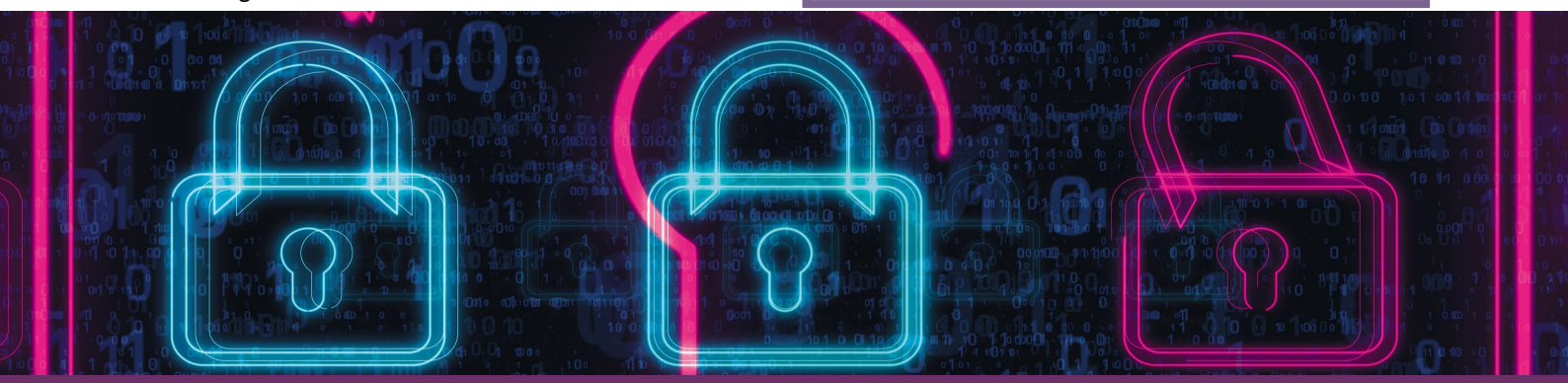
Clause 14 of the SCCs deals with *Local laws and practices affecting compliance with the Clauses* and in addition to the EDPB recommendations for supplemental measures, footnote 12 offers some practical support.in evidencing how local laws can be compliant with the Clauses. In conducting an overall assessment, companies can evidence details of requests from public authorities or the lack of. Such details need to be regularly checked and signed off by senior management. Such internal records though are not enough on their own "to conclude that the data importer will not be prevented from complying" with the SCCs. It needs to be "corroborated and not contradicted" by information that is externally available in the public domain including "case law and reports by independent oversight bodies".

For more insight on the SCCs and how to strategically approach the changeover, read our colleague's assessment of the clauses in this blog and watch our webinar here.

EDPB recommendations on supplementary measures The recommendations retain the six steps outlined in the draft to assist exporters in meeting their compliance requirements. The six steps focus on data mapping; verifying the data transfer mechanism in use; assessing the recipient country's legal system, considering supplemental measures; addressing any formalities; and periodically reviewing. Annex 2 of the recommendations provides comprehensive examples of supplemental measures whilst Annex 3 gives suggestions of possible external sources to corroborate your internal documents as per the all important footnote 12, SCCs.

EU-US data transfer mechanism With the one year anniversary of the invalidation of the Privacy Shield fast approaching, the EU Justice Commissioner, Didier Reynders, said at Digital Europe's Summer Summit (paywall) that both sides "will try to see if it is possible to get to a political agreement this year". As with the new SCCs, will any new US-EU transfer measure stand up to the test? Data transfers were also discussed when President Biden visited Europe this month.

Need help repapering numerous SCCs? Look no further. Condor, our alternative legal services provider, aided by cutting edge technology solutions and process improvement techniques, is able to assist you complete this repapering exercise. For further information, please contact james.buckingham@fieldfisher.com



fieldfisher

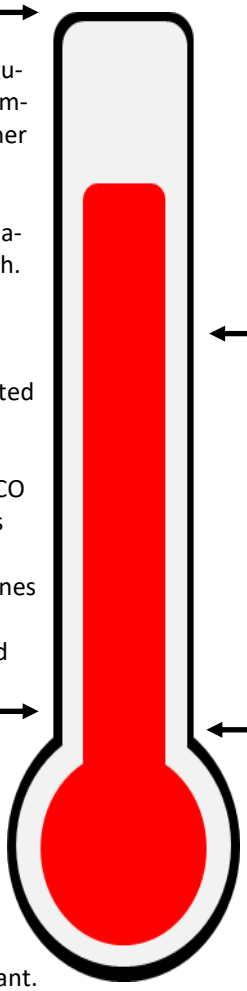
RECENT DATA PROTECTION FINES

Huge fine on the way for Amazon? According to the Wall Street Journal, Luxembourg's data protection regulator proposed a fine of around €350 million against Amazon. The draft decision has been circulated to the other data protection authorities in the EU.

So far all we know is this is not related to AWS but Amazon for breaches of the GDPR. This will be one to watch.

The ICO fined three companies a total of £415K for sending nuisance marketing—two of which were related to nuisance calls and the other one was for text messages. The ICO were notified about complaints by members of the public, who complained both to the ICO and the TPS (Telephone Preference Service). The ICO's investigations found that none of the companies had valid consent under PECR. A point to note about the fines in the statement of Andy Curry, Head of Investigation, ICO, "Company directors who disregard the law should be in no doubt that we will pursue them - other businesses should take note".

With all direct marketing fines and the ICO issues a number, the problem usually stems from the lack of consent as with all three companies here. It therefore goes without saying that organisations should ensure they have valid consent and company directors should heed to the ICO's warning. Correct management of those who unsubscribe is also important. This was made clear in the ICO's fine of £10K against the Conservative Party for sending unlawful marketing emails. Here, the ICO stated that the Party had failed to retain clear records and did not ensure that the records of those who had unsubscribed were properly transferred to its new email provider.



Fine and suspension for Ikea France. Ikea France have been fined €1 million for spying on its staff between 2009-2012. The CEO and head of risk also received suspended sentences and personal fines. Ikea France reportedly used private detective and police officers to collect individual's information (including illegally accessing criminal records and data on individual's finances).

Whilst this is not a fine from a data protection regulator, it shows the potential liability for organisations (and directors) who still carry out illegal checks or obtain personal data

As the reported ICO fines show there is much activity in the area of unsolicitored marketing. It was therefore interesting to see reported this month a fine of €300,000 for a breach of the GDPR's accountability principle by VfB Stuggart by Germany DPA Baden-Wurttemberg (paywall).

The breach focused on the transfer of several tens of thousands of club members' data, including members under 18s, to an external service provider. Baden-Wurttemberg was not impressed by VfB Stuggart's inability to explain the contractual provisions between itself and the new service provider, including the specific powers given to the provider.

Legal commentators do not think that this level of fine is solely due to a breach of Article 5(2) but a number of other things and it will be interesting to watch how Baden-Wurttemberg acts in the future with respect to accountability.

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