Thursday Thoughts – 24th June 2021

With apologies to those who missed Thursday Thoughts last week – I was somewhat under the weather and took to my bed!

This week we have the welcome news that the UK has an adequacy decision so all our data can continue to be transferred to/from Europe. The NCSC has provided another round of guidance for schools and colleges. Also good news from the courts that common sense prevailed in a recent case in which a small company faced a £1000 claim for damages for "breaking" GDPR. The case was dismissed and the upshot is if you receive an outrageous claim for money from an 'instant expert', then check your processes are in place and take appropriate advice.

Computer repairmen in South Korea have been arrested for making and distributing ransomware on customers' computers, the follow-on question is, are there "sleeper" agents in large tech companies like Dell/HP and should we already be assuming systems are infected with ransomware and working on that premise. Also news that TikTok has stealthily updated it's privacy policy to allow it to collect faceprints and voiceprints, a worrying change for parents and children alike. In the 3rd year since GDPR the data protection authorities across Europe have issued a total of 287 fines in the 12 months between March 2020 and March 2021 (a 120% increase on the previous year). I list the most recent fines.

Podcasts of the Week

Debbie Reynolds – "The Data Diva" Talks Privacy Podcast (technology-related changes to court proceedings in the US due to Covid 19)

Databasix UK Ltd - The Data Rockstar's Coffee PodCAST (Episode 53 - UK Adequacy Decision & TIGRR)

UK Adequacy Decision

Last week the EU member states "voted unanimously in favour" of UK obtaining an adequacy decision. Thus personal data can continue to flow freely between UK and EU and there is no need to change policies and procedures. We are still waiting for a statement from the ICO but these links may help:

- https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/what-does-adequacy-mean/
- https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Common Sense Prevails In Recent GDPR Court Case

GPDR has sadly lead to rise of the "over excitable Consultant" who predicts doom and retribution and sky-high fines to any organisation who transgresses the legislation in the

slightest. There has also been an increase in individuals who think it's a great idea to try and get money out of organisations by threatening them with court action for minor transgressions. This week one of the latter individuals has found, 18 months on, that a case they had taken against a small company for "breaking GDPR" was dismissed by the judge in 10 minutes because they had not in fact suffered damages and had the opportunity to "unsubscribe" in the usual way but had chosen to send an email instead. In this case human error was to blame for the company continuing to contact the individual but the organisation had put in place systems to deal with the situation. If you receive an outrageous claim for money from an 'instant expert', then check your processes are in place and take appropriate advice.

NCSC Provides More Resources for Schools

We have seen a concerning rise in cyber-attacks against education establishments. It is now true to say that an educational establishment is **more** likely to suffer a cyber security breach than the average business in the UK (58% of high schools and 78% of further education colleges compared to 39% of all other businesses). These attacks can take many forms and in August and September 2020 the National Cyber Security Centre (NCSC) issued an alert to the education sector. As more ransomware attacks came to light since February 2021 the NCSC has updated its alert and issued specific guidance for schools. If you have not seen it I recommend that you take a look. The resources include documents and videos to help schools/colleges to keep on top of cyber security.
https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools

Cybercriminals Found Working Inside Computer Repair Companies

In South Korea 9 computer repairmen have been arrested for making and distributing ransomware on their customers' computers in a scheme valued to have cost the businesses $321,000. Repairmen initially helped to deal with the ransom demands before going on to tamper with the encrypted computers, modifying the ransom notes and inflate the ransom demands. This story could also imply that there could be employees inside a large retailer (Dell, HP, etc.) or service provider who is on the payroll for a crime syndicate infecting PCs, laptops, servers, etc. that they manufacture or maintain. It is getting to the stage that you almost need to assume that the threat is already inside and work from that premise.

Did you Know TikTok Quietly Updated Privacy Policy to Collect Faceprints and Voiceprints

You may have missed this. TikTok decided to quietly update its privacy policy to collect biometric identifiers and biometric information (faceprints and voiceprints). The app added a new section to its privacy policy called 'Image and Audio Information' and can now automatically collect those new types of biometric data. According to the updated privacy policy, the data will be used for non-personally-identifying operations such as enabling special video effects, content moderation, demographic classification, and advertising recommendations. Data leaks are not uncommon, and many fear one day such information

might end up in the wrong if mishandled. More here: https://www-pandasecurity-com.cdn.ampproject.org/c/s/www.pandasecurity.com/en/mediacenter/mobile-news/tiktok-privacy-faceprints/amp/

Fines

This year has seen GDPR fines become more frequent and more punitive. Data protection authorities across Europe have issued a total of 287 fines in the 12 months between March 2020 and March 2021 (a 120% increase on the previous year). The most common violation is the illegal processing of personal data (38 % of all fines) with data security the second most common violations (21% of fines). Almost a third of all fines have been issued by the Spanish DPA, followed by Italy, Romania, and Hungary. Most recent international fines are:

Data Protection Authority of Sweden Issues a €1,600,000 Fine
On 21 June the Data Protection Authority of Sweden Issues a €1,600,000 to the Stockholm Local Transport Company for the excessive use of body worn cameras which recorded sound and vision and violations of the principles of legality and transparency as well as data minimization (recordings were kept for longer than 15 minutes).

Lithuanian DPA impose a fine of €20,000
The Lithuanian DPA has imposed a fine of €20,000 on a Fitness Centre (UAB VS FITNESS) for the excessive use of Fingerprint technology without consent.

Swedish DPA fines Rescue Service €34,800
The Swedish DPA has imposed a fine of €34,800 on the directorate of the Östra Skaraborg Rescue Service. After receiving information that fire stations in Östra Skaraborg operated surveillance cameras that filmed areas where firefighters were changing during an emergency. The 24/7 monitoring was considered too far-reaching and that camera surveillance should be limited to emergency cases.

UK ICO Fines Papa John's £10,000 – For Sending Unsolicited Texts and Emails
The Information Commissioner's Office fined Papa John's (GB) Limited £10,000 for sending nuisance texts and emails to customers. The company relies on the 'soft opt in' exemption for marketing but customers had placed a telephone order were not provided with a privacy notice at point of contact nor given the option to opt out.

ICO fines contact tracing business £8,000 for PECR breach
The Information Commissioner's Office imposed an £8,000 fine on Tested.me Ltd (TML) for sending 84,000 direct marketing emails to individuals who had provided their details for contact tracing purposes. TML provides contact tracing services to businesses by providing them with unique QR codes for visitors to scan. At the bottom of the page into which this personal information was entered, TML had added a consent tick box for marketing communications. The fact was not made clear in their privacy documentation.

Podcasts of the Week

Debbie Reynolds – "The Data Diva" Talks Privacy Podcast

In this podcase Debbie Reynolds talks to the Honourable Justice Tanya R. Kennedy discussing technology-related changes to court proceedings in the US due to Covid 19. The fact that virtual hearings are here to stay and the benefit that some participants who are intimidated in court have found as a result of there being a virtual route to representation was interesting to listen to. The conversation also focusses on the digital divide, access to justice and the benefits of technology balancing the loss of privacy in the digital age. In particular I found the need to explain technology in court cases, the proactive elements of the NY Shield Act and the difficulty in obtaining consensus on the legal adoption of technology most interesting. Well worth a listen!
https://thedatadivatalksprivacypodcast.buzzsprout.com/1734607/8733500-the-data-diva-e33-honorable-justice-tanya-r-kennedy-and-debbie-reynolds

Databasix UK Ltd - The Data Rockstar's Coffee PodCAST (Episode 53 - UK Adequacy Decision & TIGRR)

This Podcast discusses the UK adequacy decision and the Taskforce on Innovation, Growth and Regulatory Reform (aka TIGRR) report. Some great explanations on the adequacy decision confirmed the as-is approach with respect to the data protection/transfer between UK and EU and what it means, what the EU concerns are etc. TIGRR has the task to reform and improve the data laws (i.e. GDPR) after the UK-EU agreement looking towards the future. It will be key to changes in the UK so makes an interesting listen:
https://podcasts.google.com/feed/aHR0cHM6Ly9mZWVkLnBvZGJlYW4uY29tL2RieHVrL2ZlZWQueG1s/episode/ZGJ4dWsucG9kYmVhbi5jb20vZDI0MWE5NTktNjVhNS0zYTRlLWFjNTgtNjdiZDEwY2Q2MGQ4?hl=en-GB&ved=2ahUKEwir-qyw4rDxAhXP2qQKHXwvBwYQieUEegQIBhAF&ep=6