Thursday Thoughts – 3rd June 2021

This week there has been lots of talk in the media about the NHS Digital Service having access to your data and potentially sharing it. I decided to do some digging of my own and have included the details in this blog. Whether you want to opt out or not is your choice but at least you have some facts on which to base your judgement.

News this week of Facebook and linked in hacks highlight again the need for us all to enable 2 factor authentication on our accounts. Yes it will probably drive you mad, but trying to get an account back without it is really a lot more stressful. The privacy group noyb are taking action on our behalf and reporting the 10000 most used websites for cookie violations. Maybe sometime in the near future we won't be faced with a huge list of legitimate interest buttons to "revoke" when we just want to read an article! The EU are unhappy with Ireland's lack of action with regard to GDPR fines and there is welcome news in a ruling that an EU rep classes as an agent of the data controller and therefore has no litigation liability under GDPR. As I go to print we can expect the much awaited newly adopted EU Standard Contractual Clauses tomorrow and data protection experts believe that we may have longer to implement them than originally planned.

Blogs of the Week
NCSC (Hannah H) - Getting Cybersecurity Right in Your Business
Gabriel Friedlander- I was hacked on LinkedIn

What's the Story with the NHS and MY Data

There are lots of stories in the media at the moment about NHS Digital Services and the need to opt-out to stop them sharing your data. What many are unaware of is that the General Practice Extraction Service has been doing this for over 10 years, it is old and needs replacing which is why the new digital system was proposed. Health and adult social care organisations were given until September 2021 to comply the new directive so that data can be shared from 1 July 2021.

NHS Digital have worked with the British Medical Association, Royal College of GPs and the National Data Guardian and have stressed that they will not collect patients' names or addresses and they use pseudonymisation so that patients cannot be identified directly in the data. This means that they replace data such as NHS Number, date of birth, full postcode with a unique code. In addition being used for research the new service will "support the planning and commissioning of health and care services, the development of policy, public health monitoring and interventions (including for COVID-19) and help to analyse healthcare inequalities". An example of the way patient data from GP medical records has been used in the past was the work that showed that there was no association between the MMR vaccine and the development of autism.

Because of GDPR patients can decide that their data should only be used solely for their individual care and treatment or if it can be also used for research or planning purposes. But many privacy experts are concerned that the message has not been clearly communicated to patients so many will not have sufficient time to make an informed choice. The do-nothing option will be classed as "implied consent" and therefore the data will be shared. If you do not wish this to happen then you should contact your GP practice and ask for a Type 1 Opt-out by 23 June 2021. Thereafter you can opt out at any time.

There is more information on the NHS fact check page which includes a confirmation that the NHS do not sell health and care data nor do they share data with marketing and insurance companies. The link is here: https://digital.nhs.uk/services/national-data-opt-out/mythbusting-social-media-posts

What if your Facebook has Been Hacked

Over the last year there have been many cases where people have been unable to log in to their Facebook accounts. Just clicking on a link can give someone access to your account which means they can then lock you out of it. Then you will find yourself conducing lots of research, internet searched and will probably spend hours trying to get Facebook to reset it for you. This week I heard that the ICO had interceded on one user's behalf asking Facebook to address the misuse of their personal data. It's the first time I've heard of them taking on an individual's case but it prompted me to post another reminder to set up 2FA.

Please, Please, Please …set up Two Factor Authentication on your phone, social media accounts and everything you hold dear. Yes it will almost certainly drive you mad but imagine how much worse it would be if a hacker gets access and you lose everything.

Cookie Banners on Most sites 'do not comply' with GDPR

According to the Privacy Group Noyb (none of your business) most Cookie banners do not comply with the requirements of GDPR. By law website owners must give users a clear yes/no option. However, many websites still force us to revoke consent for dozens of marketing partners individually or highlight the "accept all" to make it stick out. This is all designed to make us give up and accept what is before us. Noyb have now created an automated system to find violations and auto-generate a complaint. They have started with the 10000 most used websites. This will be one to watch!

Is an EU GDPR Rep an Agent of the Controller

This week's judgment (Rondon v LexisNexis) has settled the argument about whether an EU GDPR rep can be sued under GDPR or if they are "simply an agent for the extra EEA controller/ processor". Mrs Justice Rowena Collins Rice dismissed the case agreeing with LexisNexis "that the GDPR imposes no litigation liability on Article 27 representatives". I sense a collective sigh of relief from GDPR Reps around the EU.

Ransomware actors add DDoS attacks to their arsenals

There is a new tactic for the cybercriminals in the "ransomware-as-a-service" world. They have started to offer a DDoS attack as an extra service. This is seen as "It's a little bit ransom, a little bit DDoS extortion, and a lot of trouble," according to NETSCOUT. By adding DDoS to the ransomware attack the pressure on the victim is increased making them more likely to pay the ransom.

European Parliament Unhappy with Ireland's Lack Of GDPR Enforcement

The European Parliament is not happy with Ireland's lack of enforcement action against the large tech companies headquartered in the country. So they recently voted in favour of a resolution on "an infringement procedure" against Ireland to try to force the issue.

Fines

According to a recent survey EU countries over the past three years have imposed a total of €283,673,083 of fines and 648 penalties against organizations for violating GDPR.

ICO Fine the Conservatives £10,000

The Conservatives were fined £10,000 by the ICO for sending unsolicited marketing emails after Boris Johnson became prime minister in July 2019. During the period the organisation sent "more than a million marketing emails" the vast majority of which were "validly sent" but the party did not have consent from 51 recipients. The party had failed to transfer records of who had unsubscribed from its marketing emails when they switched email provider. The Conservatives have subsequently improved their processes.

Blog and Podcast of the Week

NCSC (Hannah H) - Getting Cybersecurity Right in Your Business

Cyber security is a board-level responsibility, so it follows that board members should be aware of the risks to their business from ransomware. No you don't need to understand all the technical details but you should be able to ask the right questions. This blog from the NCSC together with their "toolkit for boards" is a great starting point.
https://www.ncsc.gov.uk/blog-post/what-board-members-should-know-about-ransomware

Gabriel Friedlander- I was hacked on LinkedIn

This is a great video and one you can certainly share with friends and family, the message is simple and easy to understand for the non technically savvy. The story of a person who suffered a phishing attack on LinkedIn and lost access to their Gmail account because the hacker got in and turned on 2FA so they couldn't get back in. The moral of the story is to be careful with what you are sharing and verify who you are talking to. Even if you are just wanting to help someone you need to make sure they are genuine. And… if you haven't done it already turn on Multi Factor Authentication. Here's the video link:
https://videos.wizer-training.com/videos/e8e720050c274183bf0665b55887e841