# Thursday Thoughts – 20th May 2021

This afternoon I am looking forward to speaking at Kirsty's Colony Networking event where we will be doing things differently and using a game of Snakes and Ladders to have a conversation about data protection and GDPR. This got me thinking about what GDPR and now UK GDPR really means for businesses and what they have to do. I've included a couple of slides from the presentation in this piece for those who still have their head in the sand as well as those who have started on their journey. Also some super advice from Tash Whitaker on some tech solutions for businesses wanting to put systems in place.

A new term this week – "Vishing"! There is also information on a huge fine for the Irish Credit Bureau, a new Brazilian banking trojan and how Apple gave the Chinese Government Access to iCloud Data. I've also found an update on last week's news which shows just how much bitcoin the "US pipeline" cyber-attacker managed to amass in 9 months. Oh and Microsoft retires Internet Explorer 11. I also have had my first "inside catch up" with friends, am I the only one that ended up exhausted as a result?

**Blogs of the Week**
Helen Calvert - 5 Self Care Rituals in 5 Minutes

## UK GDPR and small businesses

My most common questions to businesses is what camp are you in when it comes to UK GDPR

- Done it all
- Its in the bin because it doesn't apply to me
- I know it's important but don't want to do something wrong so I am doing nothing or If I don't think about it it'll go away….

For those in camp 1 – congratulations! You are in the minority. If you think you fall in camp 2 – I recommend you look at this again. There are very few cases where UK GDPR doesn't apply. If you are in camp 3 then there are some things you really need to do.

First of all we need to recognise that individuals have the right to know:

- what data we have
- when we share it and who we share it with
- how we dispose of the data

This means that we as businesses are expected to look after the personal data that we process but most importantly we have to be able to DEMONSTRATE our compliance with the legislation. You can start your journey by taking the following steps.

1. Understand what information you hold and why you hold it
2. Decide what your lawful basis is for holding data

3. Record what you do with personal data, who you share it with and how you dispose of it
4. Register with the ICO (renewing this annually)
5. Publish your privacy information in some kind of notice or policy

## Tools for data mapping/ROPA

Tash Whitaker is my "go to" for sound data protection advice. This week she made some great recommendations for tools to help with data mapping, records of processing activities and risk assessments. This week she was reviewing PrivIQ (previously GDPR365) and says their current solution "has come on leaps and bounds, and is particularly easy to use". She also thinks Keepabl and DPOrganizer should be on you short list. #passingiton

## We've had Phishing and Smishing now it's "Vishing"

We've had Phishing and Smishing now the latest thing is "Vishing" or voice phishing. Where scammers send out loads of messages using voice over internet protocol (VOIP). Victims may be cold-called or receive emails that contain phone numbers, voice notes, and messages. Sadly by using voice messages they are able to bypass existing spam filters. Another one to be on your guard against!

## Cybercriminals behind US Fuel Pipeline Hack amass a fortune

The cybercriminals behind the US Fuel Pipeline shutdown known as DarkSide have been behind reportedly $90 million worth of ransom attacks on multiple victims in the last 9 months. In a bizarre twist last week the cartel announced plans to wind up their Ransomware-as-a-Service (RaaS) program. They claimed that their bitcoin wallet had been emptied and its servers had been seized by law enforcement. Some cynics would say this is just a front to rebrand somewhere else and avoid paying affiliates. You can read more here: https://thehackernews.com/2021/05/darkside-ransomware-gang-extorted-90.html

## Bizarro Brazilian banking trojan

Bizarro is the latest example of a Brazilian banking trojan affecting Windows and Android devices. The campaign has a number of moving parts, starting with a convincing looking phishing email from a high street bank, which lurks in the background on the computer and only activates if the user logs on to that bank. It then activates and tricks users into entering two-factor authentication codes in fake pop-up windows

## Microsoft retires Internet Explorer 11

Microsoft has decided to retire Internet Explorer 11 from some Windows 10 versions. It plans to replace it with the Chromium-based Microsoft Edge.

## Protecting Personal Data in the Whistleblowing System

The Spanish Data Protection Authority has published a document that gives practical guidance on how to protect personal data in areas such as the whistleblowing system, the use of automated decisions and wearable technologies.

A decision on SCC's expected in two weeks

News from the International Association of Privacy Professionals yesterday that a decision on Standard contractual clauses (SCCs) is expected in two weeks. This is because the voting period has ended and it has now gone for “decision of the Commission” after which the guidance will be published in all EU languages. No decision on SafeHarbor 3.0 or Privacy Shield 2.0 are expected any time soon.

## How the Chinese Government Access iCloud Data

Guizhou-Cloud Big Data (GCBD) hosts iCloud data belonging to Apple's China-based users on their servers. This means that the concessions that Apple have made to put this in place mean that the company has pretty much ceded legal ownership of its customers' data to GCBD. They have even agreed to move encryption keys to its Chinese data centres. This will make user data vulnerable to state surveillance, making it “nearly impossible for the company to stop the Chinese government from gaining access to the emails, photos, documents, contacts and locations of millions of Chinese residents." These actions are in stark contrast to Apple's commitment to privacy and highlight a pattern of conceding to the demands of the Chinese government in order to continue its operations in the country.

## Fines

**€90,000 fine for the Irish Credit Bureau**

A The Data Protection Commission Ireland has fined the Irish Credit Bureau a €90,000 for 2 breaches of GDPR which relate to the need to keep information accurate and the need to report data breaches. The organisation had failed to put in place systems (technical and organisational measures) to protect and update the data of the data subjects. They also failed to undertake appropriate testing of proposed changes to a database which resulted in a breach.

## Blogs of the Week

**Helen Calvert - 5 Self Care Rituals in 5 Minutes**

Helen’s blog this week has a self-care theme and so many I have spoken to this week would really benefit from some time looking after themselves. This is a joint blog with Kimmy Drain about building a self-care routine and covers everything from joyful journaling to brisk nature walks. I am loving the idea of Karaoke at the sink and finding my favourite colour while out on my daily walk. Who knows I may even start a journal! We all need to discover new ways to unwind. You can read the blog here: https://www.clear-day.co.uk/blog/5-self-care-rituals-in-5-minutes/