THURSDAY THOUGHTS

This week in Thursday thoughts we have Wagamama and Experian in the news for unlawfully using data gathered for another purpose. Wagamama apparently used data gathered under "COVID track and Trace" to send out a survey and Experian were accused by the ICO of "enriching and enhancing people's personal data without their knowledge".

There is also a warning to be on your guard against insider breaches in 2021 and a warning that cyber criminals are targeting healthcare providers. In European news the French and Spanish Data Protection Authorities have produced some guidance that may be of use to developers and businesses alike. In the courts a potential antitrust case is looming for Google in the US and a case being taken by British drivers against UBER in the Dutch courts over using automated data to "sack" drivers.

My "Blogs of the Week"
Jill Bottomley/Sam Alford - Don't get caught out by GDPR when making redundancies
NCSC - Bugs happen, so make sure you're ready to fix them

Wagamama under investigation

Wagamama are under investigation by the UK ICO after customers in the UK were sent a survey using data that had been shared for Covid-19 contact tracing. Just to recap. Under GDPR you may only use personal data for the purpose that you gave when collecting it. A second purpose such as a survey would require per mission at the point of data collection. You can read more here: https://www.thetimes.co.uk/article/wagamama-in-the-soup-for-exploiting-tracing-data-pff66g506

Experian Unlawful Using Data for Marketing Purposes

The ICO has issued a warning to Experian for unlawful using data for marketing purposes and ordered the credit reference agency Experian to make "fundamental changes" to how it's direct marketing service handles people's personal data. This follows a two-year investigation which revealed that the agency had "invisible" data processing and provided insufficient privacy information.

According to the ICO "The investigation found how the three CRAs were trading, enriching and enhancing people's personal data without their knowledge. This processing resulted in products which were used by commercial organisations, political parties or charities to find new customers, identify the people most likely to be able to afford goods and services, and build profiles about people." You can read the PrivSec report here: https://gdpr.report/news/2020/10/28/ico-issues-enforcement-notice-to-experian-over-unlawful-use-of-data-for-marketing-purposes/

A Third of Data Breaches In 2021 Could Be Caused by Insider Incidents

It is expected that one in three data breaches in 2021 will come from insider incidents, mainly because of the way we have changed our working patterns. It is anticipated that remote working in 2021 will rise to 300% of pre-COVID levels. This represents both security and business risk for business leaders. New processes and procedures will need to be considered and the potential damage that an insider attack could wreck should be mitigated against by putting safeguards in place.

Uber Sued by British Drivers Over 'Automated Robo-Firing'

In the first legal challenge of its kind under Article 22 of GDPR. Courts in the Netherlands (where Uber's data is stored) have been asked by former Uber drivers to overrule the algorithm that caused them to be fired. Uber claims that the drivers accounts were cancelled after a "manual review by humans". But it is reported that there are over 1,000 cases where British drivers have allegedly been wrongly accused of fraudulent activity and immediately had their accounts terminated without a right of appeal and without reporting the driver to Transport for London (TfL). You can read more here: https://www.bbc.co.uk/news/business-54698858

Google possible antitrust case in US

Google has long been accused of abusing its dominance (Facebook, online searches and delivery of advertising) and stifling competition in order to boost its profits. This week there was news that there are plans for an antitrust case to be lodged in the Washington federal court.

Is Europol unlawfully processing huge datasets of personal data?

Europol falls outside the scope of GDPR as it is governed by the Europol Regulation 2016. But the failure of the organisation to abide by their own rules has caused the EDPS to accuse them of "unlawfully processing personal data on people it should not". The organisation has been given a formal "admonishment" and must produce a solution to fix the issue which should be implemented within six months.

French Data Protection Authority – GDPR Developers Guide

The French CNIL have produced a "Developer's Guide to GDPR". This shows organisations how they can approach to the main principles of GDPR. It outlines the different things you should consider to ensure that you continue to respect the privacy of users. You will find the guidance here: https://www.cnil.fr/en/gdpr-developers-guide

Spanish Data Protection Authority – New Guidelines

The Spanish DPA have issued guidance on how to achieve "Privacy by Default" while processing personal data. This is particularly useful if you intend to provide services in Spain but may also be of use to developers of processing systems in other countries as a source of information and guidance. The document lists the measures that need to be taken including data minimisation, adequacy, relevance and the need to consider what your purpose of processing is at each phase of processing. Some useful documentation and audit requirements are also included. You can read a translation of this guidance here: https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf

Cyber attackers targeting healtcare sector

The FBI has announced that it has "credible evidence" that US hospitals and health care providers face an "increased and imminent" cybercrime threat. The US agencies have urged healthcare providers to take precautions and make sure that they have robust business conntinuity plans in place. This serves as a warning to other healthcare providers globally that just because we are in the grips of a global pandemic the threat actors are still at work. The damage that they can do at this time could be catestrophic.

Blogs of The Week

Jill Bottomley/Sam Alford – Don't get caught out by GDPR when making redundancies

This week I share a joint Blog that I did with Jill Bottomley this week discussing the potentially crippling risks of data protection obligations in the redundancy process. Jill and I both tackled the issue from our respective fields of HR and GDPR. If you are looking to make redundancies following the end of the Government's furlough scheme you should read our warning of the extra, little-known and costly implications that business owners may face at this challenging time. https://www.hrdept.co.uk/trafford-and-warrington/blog/dont-get-caught-out-by-gdpr-when-making-redundancies

NCSC - Bugs happen, so make sure you're ready to fix them

This Blog by Stuart H at the NCSC discusses why it is unrealistic to expect software to be bug free in new systems such as the NHS COVID-19 app the importance having multiple layers of defence which allow you to respond quickly to bugs and fix the system. He describes 24 hours in the life of the NHS COVID app where their "Vulnerability Disclosure Process" made that the team had triaged, fixed, tested, and approved a patch for the bug which was installed by over 93% of the apps Android users. You can read the blog here: https://www.ncsc.gov.uk/blog-post/bugs-happen-be-ready-to-fix-them