Bird & Bird

Legal SASIG 2022

Legal and regulatory updates in cybersecurity and data protection

What you need to know: Legal and regulatory updates in cybersecurity and data protection

Bird & Bird LLP had the honour of hosting an annual event with the Security Awareness Special Interest Group ('SASIG') on November, 15 2022. The session was attended by cyber security and data protection experts which led to insightful, future focused, and industry specific discussions. The main theme centred on international data transfers and data security measures, the latest insights on data protection enforcement activity and the upcoming EU Regulation Digital Operational Resilience Act (DORA) and the Network and Information Security Directive II (NIS II).

The opening discussion presented by a leading silk outlined litigation trends and class action distinctions. Great attention was paid to the fact that the era of class action lawsuits is not over for data protection. If anything, *Lloyd v Google [2020] QB 747* placed more pressure on the ICO to act on errant controllers. Although non-compliance may not be heavily monitored, the reputational damages to the business can, in some ways, be just as detrimental. The risk landscape for data controllers is seemingly unlimited in regulatory action. The 'threshold of seriousness' has been reached in cases, and in some cases a misuse of private information tortious claim will and has succeeded alongside a GDPR claim.

Looking forward, the high court decision on Talk Talk's future implications of allowing the claimant to claim on *'other circumstances the client did not yet know about.'* reiterates that the balance of information asymmetry may be shifting to the claimants favour in the courts which can be quite auspicious for the data controllers.

The subsequent panel discussion focussed on the recent Interserve fine from the ICO, (£4.4m monetary penalty imposed after the data of 113,000 employees was breached due to a phishing email.) This case was recognised as a crucial warning for companies. If companies are not compliant with data protection and do not have appropriate technical and organisational measures in place within their own companies, they can and will be held liable for any potential consequences.

The panel of experts (including representation from DCMS) also recognised that the baseline controls of security are not acceptable, and most breaches are due to a failure of basic cyber hygiene. The panel recommended that the nexus of legal expertise and cybersecurity specialisation needs to align, not only at an operational level within a company, but also in senior management. A great emphasise was placed on the practical steps companies can take to protect themselves from phishing attacks and general malware which included encryption, patching, updating systems regularly, and most importantly, training, in a bid to keep staff informed and engaged in protecting the company, their colleagues, and clients. Fundamentally, the panel of experts debated the current adequacy arrangements and decisions for cross border data transfers– there was an acknowledgement that the UK are focusing on how to maintain and not undermine UK data subject rights whilst also respecting and not dictating to other countries how to run their systems. Ultimately, the UK adequacy decision relies on working with the country at hand, in a proportionate way which offers realistic protection to individuals. It was further agreed that collaboration and engagement with data protection is crucial, and a focus must be placed on the sustainability of these decisions and the scalability of them as well.

As the SASIG event progressed onto the next session, discussions focussed on the importance of consent. The many requirements, needs and clarifications which qualify consent can be cumbersome, unclear and detrimental to some companies and individuals. Some businesses heavily rely on consent and do not fully appreciate the consequences of GDPR standard consent such as, the right to withdraw consent at any time, which is a mistake, and can have a material impact on the company as a result. The speaker explained the alternatives to seeking to rely on consent including, necessity for performance of contracts, legitimate interest, legal obligation public interest orvital interest. The common trend for many companies as an alternative to relying on consent is relying on legitimate interest as a legal basis for processing personal data. That said, companies need to complete a legitimate interest assessment (LIA) as a balancing test to weigh up the risks to the individual when processing their personal data.

Latter sessions on the day focussed on the Digital Operational Resilience Act ('DORA'). Of course, one might assume DORA is only applicable for financial services but it was confirmed that the upcoming legislation changes have broadened the scope. The influx of legislation and guidance in this space has tripled nearly since 2020. DORA has expanded on the responsibilities of ICT risk management, vendor management, digital operational resilience testing, ICT related incident reporting and information sharing. Crucially, vendors are subject to these regulations. Cyber-attacks and data breaches are usually targeted on the weaker third parties, such as vendors, especially given that the supply chain is most vulnerable and it is therefore just as important to ensure that they are just as protected as the larger more sophisticated companies. DP22/3 is in Parliament currently and will inevitably follow suit of EU regulations currently. The Network and Security Information Directive 2 (NIS 2) has brought into scope more trades and businesses which will become regulated under the new statute. The updates will hopefully future proof the companies to consider their cyber security in the upcoming decades.

Last but not least, the event also featured a discussion on how companies, especially charities, need to marry intelligence with information. Alarming statistics were presented (55% of crime is cybersecurity related, which in turn has less than a 3% reporting rate, and even more concerning a 0.007% conviction rate. Source: Coalition, Inc.). Teamwork with individuals, companies, the police and students will aim to help raise awareness, educate and protect individuals and companies from future cyberattacks. Cyber resilience, supply chain vulnerability, and data storage policies were all identified as the three most strategic focal points for companies in the coming months and years.

As the session drew to a close, it was recognised that as much as data is an asset, it is also a liability which one must treat with caution, integrity, and respect.

As a truly global law firm, Bird & Bird's Privacy and Data Protection team is here to help you navigate the complex landscape of compliance. If you'd like to keep up-to-date with Bird & Bird data protection events and legal alerts, please do sign up **here**. We would like to thank the SASIG for their partnership and collaboration and we look forward to working together at future events.

SASIG is a free networking forum for the cybersecurity industry. Its mission is to improve trust and confidence in the online environment through regular masterclasses. Further information is available at www.thesasig.com.

twobirds.com

Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai • Dublin • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Luxembourg • Lyon • Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Singapore • Stockholm • Sydney • Warsaw