Hi all,

This is our first edition of the proposed periodic update on regulatory changes in security requirements including patching and liability relating to security breaches.

EU:

- Draft Cyber Resilience Act (CRA): The EU Commission has published its draft of the Cyber Resilience Act. The proposed regulation creates cybersecurity conditions for the development and market placement of hardware and software products, to remain effective during the whole lifecycle of the product. The Act introduces an EU cybersecurity certification scheme to ensure minimum standards of cybersecurity and increase information available to consumers. No explicit timeline for patching is proposed, but a solid patching plan is referenced as a necessary part of the corporate cybersecurity plan, as well as an essential for certification. Article 10(6) imposes a direct obligation on the entire supply chain of producers, modificators, importers, distributors and authorised representatives to ensure vulnerabilities are handled effectively (and accompanied by a procedure for vulnerability handling) for the entire lifecycle of the hardware or software product on the market, essentially representing a requirement to patch. With the extended liability in the regulation from manufacturers to all organisations involved in the supply chain and direct liability for management, a well-established patching procedure is critical. The CRA is the latest addition to the proposed EU cybersecurity harmonization package and is open for feedback until the 5th of December 2022. *We note that we see a shift in narrative in recent trends of regulation and governance, where patching is presented as a part of the integral business structure and interests, rather than an annoyance or a sub-task of internal IT departments.* Source: here
- Draft AI Liability Directive: The proposed AI Liability Directive bundle imposes liability on producers (including organisations which substantially modify products) of IoT products and OS service providers if they fail to address cybersecurity vulnerabilities. This indirectly poses an obligation for effective patch management. Additionally, this liability expands to the requirement in both the CRA and ARES to keep OS or IoT products up-to-date and free of cybersecurity vulnerabilities for their entire lifecycle on the market (or a minimum period of 5 years in the case of OS services). Source: here and here
- Draft Delegated Act to the Radio Equipment Directive: This draft is currently undergoing revision based on the feedback period. The proposed amendments to article 3 expand the scope to IoT products and impose an obligation to maintain network functioning and safeguard privacy. Where this text is left relatively broad, it implies a certain standard of cyber resilience (in which patching plays a substantial part) to be further codified by the European Standards Organizations before their entry into force in 2024. Source: here

NL: Release Cybersecurity strategy 22-28: On 10 October, the National Coordinator for Counterterrorism and Security published the Dutch Cybersecurity strategy for the upcoming 6 years. The strategy document outlines new approaches to cybersecurity at the national level, and aims to expand responsibility of governments and large companies. Additionally, the NCSC and national CSIRTs will be absorbed into one central organisation. Source: here

US: Uber CSO Convicted over Failed Breach Disclosure: On October 5th Uber's former CSO was convicted for his failure to disclose a serious data breach back in 2016 to the FTC. This is the first time a company executive has been held personally criminally liable for the handling of a data breach. Source: here

Germany: BSI Breach Detection Systems guide: The German Federal Office for Information Security (BSI) has published guidance on the use of breach detection systems for providers of critical services. The guide recommends approaches to the implementation of legal obligations of appropriate organisational/technical measures and timely detection. Source: here

Privacy & data security:

- ECJ AG Opinion: The Advocate General of the ECJ has published their opinion on the request for a preliminary ruling by the Austrian Supreme Court on *Case C-300/21 UI v Österreichische Post AG* regarding article 82 of the GDPR. The AG contends that a mere breach of GDPR rules or upset feelings are insufficient to constitute actual damages to the individual under article 82. Source: here
- EDPB Updated Guidelines on Breach Notification: The EDPB plans to update their guidelines on breach notification this October. The guidelines are expected to consider the EU's new regulatory proposals. Source: here

We appreciate any contribution to this newsletter based on your own research or internal enterprise discussions.

Best,

Lokke Moerel & Lisa Rooij

E.M. (Lisa) Rooij
(she/her)
TILT, Tilburg University
E.M.Rooij@tilburguniversity.edu