REGULATORY UPDATES

THESEUS REGULATORY UPDATES ON PATCHING

EU Developments

NIS2 Directive Adopted: The EU has officially adopted the NIS2 Directive on 10 November 2022. Member States will have 21 months from its entry into force to incorporate its provisions into their national law. The NIS2 introduces some of the most widespread cybersecurity rules to date, and lays down the first minimum cybersecurity standards, including vulnerability management. Source here

Initial feedback on the CRA: The Czech presidency circulated a first draft of the Cyber Resilience Act (CRA) significantly altering its scope and free movement principles. Primarily, they argue that the scope should extend to software as a service (SaaS), military products and include a national security intervention clause. In addition, there appears to be an overarching call from Member States to clarify the definition of 'critical products' and the interaction of the CRA with other EU regulation. Different opinions on the proposal have also been compiled into a Briefing Report by the EU Parliamentary Research. It is clear however, from the Commission's recent report on the EU Security Strategy, that they view the CRA as imposing a legitimate obligation to 'ensure the availability of patches'. Source here , here and here

EDPB and ENISA Sign Memorandum of Understanding: ENISA and the European Data Protection Board (EDPB) have signed a Memorandum of Understanding on Strategic Cooperation going forwards. The memorandum is intended to serve as a basis for future collaboration on achieving mutual goals, particularly in areas of privacy and security by design. Some of the proposed collaboration will include guidelines and harmonized feedback. Source here

Irish DPA fines Meta 265 Million: The Irish Data Protection Authority has presented Meta with a 265 Million Euro fine, for a failure to upkeep privacy and security by design. In 2018 and 2019 Meta's failure to implement appropriate security measures led to widespread dataset leaks. Following the Irish Data Protection Authority's decision, the EDPB published 3 binding decisions regarding contractual obligation as a legal ground for processing, to be published next month. Source here and here

Polish DPA fines Virgin Mobile: The Polish DPA has fined Virgin Mobile approx. 350.000 euros following a data breach. Notable about the decision is the focus of the DPA on the failure of Virgin to timely detect vulnerabilities, as they failed to run regular tests. Source here

DECEMBER / 2022 / ISSUE #3

HAPPY HOLIDAYS!

HIGHLIGHTS

NIS2 DIRECTIVE ADOPTED

The EU and its Member States have officially adopted the NIS2 Directive.

FIRST ROUND OF CRA FEEDBACK

Initial feedback by Member States on the CRA proposes hefty changes to its scope

META FINED 265 MILLION

Meta has been fined a record-breaking 265 Million Euros for a failure to upkeep security-by-design

US Developments

Personal Data Expiration Dates: Following the FTC's Drizly case, where Drizly's CEO was individually penalized for failing to uphold standards of data security, the FTC has now somewhat introduced the concept of 'expiration dates' for personal data. In essence, under the new CPRA, to be implemented on the 1st of January next year (2023), organisations will be required to present expiration dates of categories of personal data prior to collection. The circumstances of this case also present a stronger incentive to preventatively take cybersecurity and vulnerability mitigation steps, or risk full and personal liability. Source here

Global & Privacy Developments

CJEU bans inaccurate personal data on the web: In an arrest made by the CJEU on 8 December 2022, the Court decided that, under the GDPR, a search engine is required to remove links that could lead to factually inaccurate information, if such is proven by the person requestion the deletion. This arrest could have very interesting implications for the long-ongoing "Fake News" debate. Source here and here (summary in Dutch)

UK First to Adopt Cybersecurity Code of Conduct for Apps: The United Kingdom has introduced the first Code of Conduct for app operators and app platforms. Primarily, the Code introduces stronger requirements for app operators to inform users of their security standards, and allow for usage even if privacy settings are not 'optimal'. Importantly, the Code explicitly requires app operators to reduce security vulnerabilities through patches, and introduces the notion of coordinated vulnerability disclosure mechanisms between the app operators and platforms, aiming to avoid public exploitation. Where the Code is voluntary, the UK DCMS will start checking for compliance in 9 months' time. Source here

Cyberveilig Nederland feedback on NLCS: The Dutch organization, Cyberveilig Nederland, has drafted a letter in response to the new Dutch Cybersecurity Strategy. Where the organisation praises the ambitious stance taken by the strategy, they do call for further specification of the action points and the private scope of the strategy. Source here (in Dutch)

WANT TO CONTRIBUTE YOUR OWN UPDATES AND REGULATORY FINDS?

CONTACT E.M.ROOIJ@TILBURGUNIVERSITY.EDU

THESEUS PROJECT
https://project-theseus.nl/