Trends in Interpretation of EU Data Protection Authorities of Cybersecurity Requirements under the GDPR

Larisa GĂBUDEANU
Faculty of Law, University Babes-Bolyai, Cluj-Napoca, Romania
larisa.gabudeanu@ubbcluj.ro

Abstract
One of the main legal requirements for the adopting the GDPR was the technical and organizational security requirements, alongside the transparency and purpose limitation principles. The wide wording mentioned by the GDPR in terms of state-of-the-art security measures has given rise to a series of interpretations both in literature and by the data controllers and data processors. The manner in which national data protection authorities interpret this wording on a case-by-case basis is a good indicator in terms of interpretation, as the authorities look into the specific use case requiring preventive security measures. Thus, this research paper brings additional clarity in the interpretation of this legal requirement in terms of the risks and damages considered relevant for the specific data breach or lack of proper legal requirement implementation, given publicly available information in this respect. Further, the research paper highlights the number of use cases analyzed by different national data protection authorities and the views of each national data protection authority.

Index terms: security by design, data protection, article 32, enforcement, GDPR

References
[7]. ENISA, “Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default,” 2019.