Peer Response in Collaborative Discussion 1

My peer response to Anda Ziemele

by George Koridze - Sunday, 3 November 2024, 7:57 PM

Your description of cryptographic failures is insightful and the flowchart effectively highlights how insufficient planning and a lack of proper encryption protocols can lead to security risks, especially in the context of GDPR compliance (Allen, 2023).

For further strengthening the prevention of cryptographic failures, data assessment action can be added to the flowchart for assessing each attribute during the planning stage to identify specific personal information that require encryption and the encryption type, per GDPR, to ensure data compliance.

Your point on using secure internet protocols (like HTTPS) during the transmission phase is spot on. Regarding your note on encryption algorithm selection, you're absolutely correct in emphasising SHA-256 over MD5 due to MD5's vulnerabilities to collision attacks (Stec, 2024), but I would also update this in the Flowchart.

Your flowchart illustrates at which stage the encryption-related risks may arise and where the secure data transmission protocols should be implemented within the SDLC process, making it easier to visualise and mitigate cryptographic vulnerabilities during planning and design phases.

References:

Allen, C. (2023) Encryption For GDPR Compliance. *Cryptomathic*. Available from: **https://www.cryptomathic.com/blog/encryption-for-gdpr-compliance** [Accessed 3 November 2024]

Stec, A. (2024) MD5 vs. SHA Algorithms. *Baeldung*. Available from: **https://www.baeldung.com/cs/md5-vs-sha-algorithms** [Accessed 3 November 2024]