

Case Study: Sheldon Investments Limited (trading as River Medical)

Unit 10 Summary post:

In summary, a critical factor that led to the non-compliance of GDPR is poor system design. The case against Sheldon Investments Limited (trading as River Medical) (Data Protection Commission, N.D.) was a clear breach of non-compliance due to the persistent sending of unsolicited marketing emails without consent.

The system's design ultimately led to human error, which the company gave for the reasoning of the non-compliance. As there was no clear cookie disclaimer form on the site (River Medical, 2022), this infringes Articles 6-7 (Intersoft Consulting, N.D.) for processing and conditions for consent. This was supported further by Chan (2022), suggesting that users' consent and opt-out causes a challenging user experience and elevates the risk of potential human error. He continues that the accuracy of the mailing list could be improved and that unsubscribing from mailing lists would need to be performed in writing (Chan, 2022). The supportive point argues the need for a transparent system and policy to achieve consistency from its users. In the original case, the user had not signed up to their newsletter and requested not to; there is a clear issue with the system to record and hold personal data. A solution to this issue could be automation to process such requests (Necat, 2022), which would ease efficiency and lower the risk of GDPR breaches in the future. Following the incident, it was clear that the current system should be reviewed. Chan (2022) also highlighted Newsweaver, the system used to issue emails, had sent out the unsolicited email due to human error. Automation would help solve this issue. Chan (2020) did raise the concern that HIPAA privacy rules could be applied; however, as this is outside of the United States, it would be not be considered, and the privacy rule would fall under the

umbrella of GDPR in Ireland (Venkatesiah, 2017). To conclude, audit and functional system design changes may help comply with GDPR in the future.

- Chan, Y. (2022). Peer Response NISM Collaborative Learning Discussion 3. Available: <https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=292723> [Accessed 3 February 2022].
- Data Protection Commission. (N.D.). Case Studies. Available: <https://dataprotection.ie/en/pre-gdpr/case-studies> [Accessed 22 January 2022].
- Intersoft Consulting. (N.D.). GDPR. Available: <https://gdpr-info.eu/> [Accessed 22 January 2022].
- River Medical. (2022). River Medical. Available: <https://www.rivermedical.ie/> [Accessed 22 January 2022].
- Venkatesiah, K. (2017). GDPR vs. HIPAA - Noting the differences. Available: <https://www.healthitoutcomes.com/doc/gdpr-vs-hipaa-noting-the-differences-0001> [Accessed 3 February 2022].