Discussion Forum 3: Responses to the initial post

1. Post by Ying Chan

Peer Response

Thanks, Jonathan, the post showed a great understanding of the General Data Protection Regulation (GDPR) focuses on unsolicited marketing emails. Especially provide the findings of no clear cookie disclaimer on the company site.

In order to subscribe to the newsletter on the River Medical company site, the customer is required to tick the checkbox for consent on their GDPR obligations, however, the withdrawal of subscription have to submit in writing (River Medical, N.D.). It is common that the unsuccessful opt-out request was due to human error which this organization occurred. The accuracy of the mailing list and user experience could be improved if the opt-out process was done by the system itself with the provided unsubscribe link within their email. Despite the fact that the GDPR does not define how to unsubscribe, organizations must make it simple for users to alter their views and seek an opt-out (GDPR, N.D.). Moreover, personal data should not disclose to third parties without consent. In the second complaint, River Medical provided an incorrect mailing list to Newsweaver (Data Protection Commission, 2020) who should be defined as a processor in Article 28 (GDPR, N.D.).

Other than GDPR, River Medical as a health care industry, Health Insurance Portability and Accountability Act (HIPAA) privacy rule could be established as well. Individuals have a significant choice over whether and how their protected health information is used and shared for marketing purposes under the HIPAA Privacy Rule. The unsolicited marketing email should be defined as “marketing” under privacy rule 45 CFR 164.501, 164.508(a)(3) with “a communication about a product or service that encourages recipients of the communication to purchase or use the product or service” (HHS, 2003).

References:

Data Protection Commission (2020) Case Study 13: Sheldon Investments Limited (trading as River Medical). *Pre-GDPR*. Available from: https://www.dataprotection.ie/en/pre-gdpr/case-studies#201713 [Accessed 28 January 2022].

GDPR (N.D.) Principles relating to processing of personal data. *Art. 5 GDPR*. Available from: https://gdpr.eu/article-5-how-to-process-personal-data/ [Accessed 28 January 2022].

HHS (April 3, 2003) Marketing. *Guidance Materials.* Available from: https://www.hhs.gov/hipaa/for-

professionals/privacy/guidance/marketing/index.html [Accessed 28 January 2022].

River Medical (N.D.) Enquire Now. Available from: https://www.rivermedical.ie/enquire-now/ [Accessed 28 January 2022].

2. Post by Beran Necat

Re: Initial Post

Hi Jonathan,

It should be possible to use automation to remove a name/links from the system, and if they cannot it reflects (as is the case here) that the system is poorly designed and may put the company at risk of multiple GDPR breaches. This case highlights that good system design is critical for GDPR compliance.

Regards, Beran