**Peer Response 1**

Context: <https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=296433#p1033296>

Hi Ian,

I enjoyed reading your detailed analysis of the scenario. Although the root cause of the breach in GDPR regulations is that the complainant's address was added to a mailing list when no consent was given for this, attempts to rectify the situation were poorly executed. Further details weren't given by River Medical, but based on the evidence available, it could be argued that their first attempt to delete the complainant's information wasn't fully completed- they likely missed an area of their data where it still existed (which is also alluded to by the fact that their second infringement was due to using an incorrect mailing list).

GDPR is still a relatively new concept and adjustment to the new concepts is a challenge. Automated data deletion relative to time periods has not been a business requirement and considering how unique and disparate systems can be inside a business, there is no easy, universal fix. This is also exacerbated by modern IT practices, which favour data replication across backups and servers for redundancy and safety, in addition to modern software engineering practices which encourage data caching, making rapid data deletion hard to achieve in the real world (Shastri et al., 2019).

Automation is a key area to focus on with GDPR because the rules are strict and manual enforcement is hard to scale- some companies (e.g. dataprivacymanager) are attempting to address this. GDPR implementations are still being ironed out and one could argue that service providers should take responsibility for implementing data standards- in this case, it would mean that River Medical's email system (Newsweaver) should handle this responsibility. In the meantime, what do you think would be the best way of ensuring manual data deletion is thorough enough to guarantee compliance?

**References**

Shastri, S., Wasserman, M. & Chidambaram, V. (2019) 'The seven sins of personal-data processing systems under GDPR', Proceedings of the 11th USENIX Conference on Hot Topics in Cloud Computing (HotCloud'19). Renton, Washington, 8 July. California: USENIX Association. 1-7.

**Peer Response 2**

Context: <https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=293038#p1033302>

Hi Michael,

I found the point on using security frameworks to continuously improve information security, and thereby GDPR compliance, quite interesting. There is a fair amount of research available which takes this perspective: Lopes et al. (2019) did some content analysis and found that overall, organisations that have enforced ISO/IEC:27001 are in a much better position to comply with GDPR requirements, because both GDPR and ISO/IEC:27001 prioritise safe storage and retrieval of sensitive data. Tzolov (2018) also found that ISO 9001 standards (a set of standards which guarantee a high quality of output and customer satisfaction), could have its steps mapped to the processes necessary to achieve GDPR compliance. The author noted that this mapping could be used in different ways- to create a methodology for achieving compliance, as a means of completing specific steps, or merely to prove that the business also complies with the ISO 27000 family of standards.

In addition, other standards and frameworks have also been introduced to help businesses in achieving GDPR compliance. One such example is PDP4E: a set of tools aimed at helping software and systems engineers integrate privacy and GDPR compliance with standard development practices (PDP4E, 2021). In light of the above, would you say that standards and practical frameworks should be given greater attention, as a means of helping businesses reach GDPR compliance faster, and maintain it in a more reliable way?

**References**

ISO. (n.d.) ISO 9001 Family. Available from: https://www.iso.org/iso-9001-quality-management.html [Accessed 20 February 2022].

Lopes, I., Guarda, T. & Oliveira, P. (2019) Implementation of ISO 27001 Standards as GDPR Compliance Facilitator. Journal of Information Systems Engineering & Management, 4(2): 1-8.

PDP4E. (2021) PDP4E: Methods and Tools for GDPR Compliance through Privacy and Data Protection Engineering. Available from: https://www.pdp4e-project.eu/ [Accessed 20 February 2022].

Tzolov, T. (2018) 'One Model For Implementation GDPR Based On ISO Standards', 2018 International Conference on Information Technologies (InfoTech). Varna, Bulgaria, 20-21 September. New Jersey: IEEE.1-3.