Network and Information Security Management May 2021 A

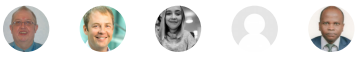
« Collaborative Learning Discussion 3

Freya Basey

Initial Post

23 days ago

7 replies



Last 6 days ago

Case Study H - Disclosure of sensitive personal data by a hospital to a third party

Whilst the General Data Protection Regulation (GDPR) had been adopted by the European Union in 2016, this directive only became enforceable from 25th May 2018 (European Data Protection Supervisor, N.D.). GDPR was not enforceable at the time of this case study in 2017, however the principles of GDPR can still be used to demonstrate the privacy risks involved.

The incident in question involved a hospital disclosing personal health data to a third party and contravenes the GDPR in several ways (Data Protection Commission, 2020). The disclosure occurred due to an incorrect address being used to send documents to the data subject. This breaches Article 5 which states that personal data should be kept accurate and up to date (EUR-Lex, 2016). In a further breach of Article 5, the business did not employ appropriate security measures to protect the personal data in transit, such as using mail tracking. Furthermore, sensitive data categories, such as health data, require an additional lawful basis for processing under Article 9 and this was not met.

The resolution of this case was that the Information Commissioner's Office made a formal decision that the hospital had breached the Data Protection Acts enforced at the time of the incident.

Recommended steps to mitigate these issues in future include implementing clear, documented procedures for managing all personal data processing, including processes for securely sharing personal data with data subjects. In addition, the human error involved in this case suggests that the staff have a lack of awareness of data protection principles. Therefore, GDPR training should be a prerequisite for all staff involved in data processing operations as this is a mandated responsibility of the Data Protection Officer under the GDPR.

References

Data Protection Commission (2020) Pre-GDPR Case Studies. Available from: **https://www.dataprotection.ie/en/pre-gdpr/case-studies#201705** [Accessed 23 June 2021].

EUR-Lex (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council. Available from: **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434** [Accessed 23 June 2021].

European Data Protection Supervisor (N.D.) The History of the General Data Protection Regulation. Available from: **https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en** [Accessed 23 June 2021].

Reply

7 replies

1 

Post by **David Luvaha**

19 days ago

Peer Response

In support of the above case according to Dataguise(2021) as defined in Article 5(1)(f) of the GDPR, integrity and confidentiality is the sixth principle related to the processing of personal data. Additionally, all organizations must take necessary precautions to guarantee the correctness of personal data collected from data subjects. Secondly, they must identify essential steps, depending on the purpose of processing, to erase or rectify inaccurate data without delay. It is because of the above reasons that the Information Commissioner's Office might have made a formal decision that the hospital had breached patient data.

References

Dataguise(2021) That is the GDPR Data Accuracy Principle? Available from https://www.dataguise.com/gdpr-knowledge-center/data-accuracy/ [Accessed 27 June 2021].

Reply

2

Post by **Kin Wong**

18 days ago

Peer response

Again, this can be caused by human error in every circumstance. It is possible that either the employees have overlooked the security of data, or they haven't identified what data they can't share with other third parties.

According to the ICO (2016), “Your employees may have a limited knowledge of cyber security, but they could be your final line of defence against an attack. Accidental disclosure or human error is also a leading cause of breaches of personal data. This can be caused by simply sending an email to the incorrect recipient or opening an email attachment containing malware cyber security awareness. “ Therefore, the following aspects should be included in the training, to prevent and minimise the same incident happens again:

“

1. Employees at all levels need to be aware of what their roles and responsibilities are. They need to be trained, able to recognise threats such as phishing emails and other malware or alerting them to the risks involved in posting information relating to your business activities on social networks.
2. We should encourage our employees to have a general security awareness within our organisation. A security aware culture is likely to identify security risks. Employees should be trained, so that they can keep their cyber security knowledge of threats up-to date.
3. Distribute security bulletins or newsletters from organisations relevant to our business to the employees. This able to keep the cyber security knowledge of employees up to date, but also can maintain the cyber security and GPDR awareness.”

Reference:

ICO (2016) *A practical guide to IT security. Data protection* [Online]. Available at: *https://ico.org.uk/media/fororganisations/documents/1575/it_security_practical_guide.pdf* (Accessed: 28th June 2021).

Reply

3  Post by **Doug Millward**

17 days ago

Initial feedback

Freya makes an excellent point that many of the regulations embodied in the GDPR were still enforceable before the regulation became law in the UK - GDPR in some cases just consolidated various regulations, added additional clauses, and made the penalties clearer and more severe. Nonetheless, the mitigations mentioned in other posts - user training, education, and additional processes are core actions that should be applied.

Reply

4  Post by **Charlotte Wilson**

17 days ago

Peer Response

I agree with the potential mitigations proposed within this post, especially ensuring that clear processes are not only documented, but followed. It is unfortunate that human error can cause an incident of this level; however, from experience this is something that occurs more often than not. Hence why it is necessary that the processes are simple for any individual to follow, whilst also ensuring specific checkpoints are met and fulfilled. Given that medical information is considered to be sensitive personal data under the guidance of GDPR, it is expected to be handled with greater care and further precautions (ICO, 2018). Within Section 1, condition 2, it is stated that “you must be able to justify why process of this specific data is ‘necessary’” (ICO, 2018). This relates well to this particular case study and it would be required by the hospital to provide that justification.

Something to consider as well would be the level of assurance understood by the hospital with their third parties. As organisations, it is down to them to ensure their data is protected even if utilised by a third party, the responsibility is still with the organisation. It is important for organisations to choose third parties that will design with data protection in mind, and follow the same standards and controls as deemed required (ICO, 2020). Albeit this data never should have been shared with the third party, it is necessary that third parties are chosen who practice good data protection controls and would have the tools in place to report this type of incident before it reaches the individual.

REFERENCES

ICO (2018) What are the conditions for processing? Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions8 [Accessed 29 June 2021]

ICO (2020) Third-party products and services. Available from: https://ico.org.uk/for-organisations/accountability-framework/contracts-and-data-sharing/third-party-products-and-services/ Accessed 29 June 2021]

Reply

5  Post by **Jan Küfner**

15 days ago

peer response

Another element to ensure GDPR compliance is checking correct implementation of GDPR processes from time to time. This in fact is also a GDPR requirement described in article 32 (d), which might also likely be violated by the hospital at that time. A good way of verifying GDPR compliance are audits combined with specific pen-tests, that target obligations for data security as laid out in article 32 (b)

The process was handled on an organizational level. Operators were instructed to send this sensitive health data to the right recipient. A technical mitigation to this risk, being more expensive, can fix the issue however definitely. If the patient for example would need to authenticate by e.g. username & password in a hospital to sign of his consent for data storage, this mechanism could also be used to provide data, he / she requests in a later point of time for download on a secure web app.

Reply

Maximum rating: -

6  New Post by **Freya Basey**

7 days ago

Summary Post

This discussion was based on a case study of a hospital incorrectly disclosing a patient's data to a third party. Several recommendations for controls that can be used to mitigate the risk of this type of breach were shared. It is important to note that human error is identified as the root cause of the majority of data breaches, with 95% of breaches shown to have human factors involved (Wong, 2021; Nobles, 2018). The General Data Protection Regulation (GDPR) mandates security controls across people, process, and technology in order to effectively protect personal data from being breached.

Wong (2021) suggests a personnel solution of staff training, not just on data protection, but on security too in order to embed a security culture. Building a strong security culture is a continuous process and ensures staff at all levels of an organisation take responsibility for protecting data.

To build on process controls, Wilson (2021) recommends implementing mechanisms for checking adherence to documented processes and Kufner (2021) offers the solution of completing audits to measure effectiveness. Both internal and external audits can be conducted to ensure processes meet compliance requirements (RSM, 2020). In addition, sufficient due diligence should be done on the practices of third parties that will be acting as data processors in order to ensure data is protected throughout its lifecycle (Wilson, 2021).

Furthermore, Kufner (2021) suggests utilising technical solutions to solve the challenge of human error. Using technology to automate data processing tasks can boost GDPR compliance through reducing errors (Ryan et al., 2020). However, Kufner (2021) does highlight that these solutions can be more costly.

The GDPR was introduced to create a clear central regulation to cover the protection of personal data and has incentivised businesses by administering large fines for breaches (Millward, 2021). This has been effective in getting companies to adopt holistic security measures in order to protect the confidentiality, integrity, and availability of data (RSM, 2020).

References

Kufner, J. (2021) Initial Post. Available from: **https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=262576** [Accessed 9 July 2021].

Millward, D. (2021) Initial Post. Available from: **https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=262576** [Accessed 9 July 2021].

Nobles, C. (2018) Botching Human Factors in Cybersecurity in Business Organizations. *Holistica Journal of Business and Public Administration* 9(3): 71-88.

RSM (2020) Impact of the GDPR on Cyber Security Outcomes. Available from: **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/906691/Impact_of_GDPR_on_cyber_security_out**

comes.pdf [Accessed 9 July 2021].

Ryan, P., Crane, M. & Brennan, R. (2021) 'GDPR Compliance Tools: Best Practice from RegTech', *International Conference on Enterprise Information Systems*. Virtual, 5-7 May. Springer, Cham. 905-929.

Wilson, C. (2021) Initial Post. Available from: **https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=262576** [Accessed 9 July 2021].

Wong, K. (2021) Initial Post. Available from: **https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=262576** [Accessed 8 July 2021].

Reply

7  New Post by **Doug Millward**

6 days ago

Final Feedback

Hi Freya
this is an excellent summary of the arguments made in this thread - my only recommendation for improvement would be to validate the comments made by your colleagues - are they using reliable sources? Do any published, peer-reviewed papers contradict or challenge any of the opinions expressed in this thread? Nonetheless an excellent summary.

Reply

Add your reply

Your subject

Type your post

Dateien auswählen Keine ausgewählt

Submit Use advanced editor and additional options

OLDER DISCUSSION Summary Post

NEWER DISCUSSION Initial Post