Network and Information Security Management May 2021 A

« Collaborative Learning Discussion 3

Laura Rivella

Initial post - Department of Justice and Equality case

24 days ago

5 replies

Last 6 days ago

We believe this to be a relevant case to our field of study since it has to do with the disclosure of sensitive personal data through a failure to apply proper permissions in a database. Additionally, the complainant's sensitive personal data was processed without the required consent or another valid legal basis for doing so. (Data Protection Commission, 2017)

The specific GDPR aspect addressed is the unauthorized disclosure of sensitive personal data to third parties. In particular, we can refer to article 4, 5, 12, 13, 32. (European Parliament & European Council, 2016)

After the complainant declined an amicable resolution offer by the Department, which consisted of an apology and removal of the document from the database, the case escalated to a formal decision by the Commissioner.

More than any other aspect relating to Information Security Management, the mitigation for this sort of issue should come in the form of regular audits and reviews of the databases to address the presence of confidential information and assess permissions. Furthermore, an adequate system of training for staff managers should be implemented to educate them on data protection.

TLL (Amy, Chris, Laura, Shiraj)

References

Data Protection Commission (2017) Case Studies. Case 11 of 2017 "Failure by the Department of Justice and Equality to impose the correct access restrictions on access to medical data of an employee". Available from: **https://dataprotection.ie/en/pre-gdpr/case-studies#201711** [Accessed 19 June 2021].

European Parliament & European Council (2016) General Data Protection Regulation. Available from: **https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1404-1-1** [Accessed 19 June 2021].

Reply

5 replies

1  Post by **Yibeltal Mengesha**

18 days ago

Peer Response

In support of the above case

Unauthorized disclosure means to disclose, release, transfer, disseminate, or otherwise communicate all or any part of any record orally, in writing, or by electronic or any other means to any person or entity. Recommended Practices for Individual All confidential information must be cared for with the appropriate level of physical and electronic (logical) security. When working with confidential information we take on the custodial responsibilities for that information. Thus, each person who access this information has the responsibility to: identify, protect, communicate and maintain. As technology develops, each of these lists should be expanded to cover additional techniques and devices as appropriate.

Reference

Unauthorized Disclosure. Available from: **https://www.csusb.edu/its/support/it-knowledge** base/detail?id=9459598f98f1174e5d7cb447cc95050915699f018 [Accessed 28 June 2021]

Reply

2  Post by **Doug Millward**

17 days ago

Initial feedback

An excellent post, Laura. As observed elsewhere mitigations for GDPR issues consist of user training and education plus good system design and implementation. Pertinent questions can be raised around what could/ should be done with systems designed and built before the legislation, but as Laura observes a good regime of auditing - although staff intensive - can still mitigate issues.

Reply

3 Post by **Jan Küfner**

15 days ago

Peer response

Since this data is undoubtably special category personal data as per GDPR article 9, due diligence in the handling of this type of data would have been necessary, unfortunately this was not the case. (EUR-Lex 2016)

A good way of dealing with special category data is to label it, with tags such as public, confidential, and strictly confidential. By implementing such tags within a company and by scanning databases and data storages for data put in places where it shouldn't be e.g. a strictly confidential employee health record within the departments shared folder, this can easily be avoided. It needs to be said, that the implementation of this approach costs money initially. I however believe, that in the long run, a company will benefit from data labelling incl. check of proper storage location of such data.

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 01.07.2021].

Reply

Maximum rating: -

4

Post by **Laura Rivella**

12 days ago

Summary Post

As usual, this discussion forum highlighted current trends and issues related to GDPR and its ramifications.

It is not entirely clear to us what point Yibetal's response addresses, however, a very good contribution was made nudging the discussion towards the responsibility to updating security standards as technology advances.

In order for this to work, we must once again state the importance of regular system audits and reviews.

From most of the posts by our peers, reflecting most cases, it would appear that there is still a severe lack of training and sensibility when it comes to applying data security. It was indeed discussed in seminar 4 as well, where we brought up real life scenarios from our experiences on the job.

We believe there are two further aspects worth bringing up once more: a lack of attention on the part of the human, and a lack of intelligent implementation of automation. The latter being particularly evident in all the cases about the right to erasure that our peers examined. We have examined and made further contributions on Charlotte's

case in particular. By lack of attention we mean a laissez-faire approach to data security, motivated either by a lack of resources available, or by a negligent attitude and lack of enforcement. This point was also discussed thoroughly in Seminar 4 as data insecurity is still a pervasive issue.

TLL (Amy, Chris, Laura, Shiraj)

Reply

5  Post by **Doug Millward**

6 days ago

Final Feedback

An excellent summary Laura, but kudos to Jan for an insightful post as well. As you both mention there are a variety of social and technical measures that can be put into place to address the GDPR challenges raised but at the moment it is the responsibility of individual companies to select and implement such measures - the next challenge is for national or international bodies to produce guidance around the best such measures for common challenges.

Reply

Add your reply

Your subject

Type your post

Dateien auswählen Keine ausgewählt

Submit

Use advanced editor and additional options

OLDER DISCUSSION

Initial Post

NEWER DISCUSSION

Initial Post