Network and Information Security Management May 2021 A

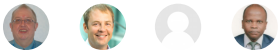
« Collaborative Learning Discussion 3

Dario De Giorgi

Initial Post

19 days ago

5 replies



Last 6 days ago

In this case study, Sheldon Investment Limited failed to comply with the GDPR, notably in the use of email addresses for marketing purposes, even though the person concerned had stated that they did not want to receive marketing emails.

One year later, the individual continued to receive marketing emails, despite complaints made to Sheldon Investement Limited, which resulted in a complaint to the Data Protection Commissioner. The Dublin Metropolitan District Court, therefore, imposed a fine for "marketing email without consent" and costs covering the case study.

Sheldon Investment Limited confirms that this was a human error. A lack of visibility could be responsible for this kind of issue. When a client requests to have their email address deleted, the email address may be stored in many databases, leading to inaccuracy when Sheldon Investment Limited confirms that they have deleted the email from the database.

Manual input can significantly increase errors. In this use case, wishes to withdraw consent to receive marketing emails, it is preferable to automatically update the information for that individual and thus avoid errors. If it is not possible to set up an automated system, thanks to data governance, it is possible to designate specific people to take care of this kind of task (Stephens, N.D).

Stephens, A. (N.D) Could human error cause a data breach under the GDPR? The privacy compliance hub. Available from: https://www.privacycompliancehub.com/gdpr-resources/could-human-error-cause-a-data-breach-under-the-gdpr/ [Accessed 27 June 2021].

Reply

5 replies

Post by **David Luvaha**

1

19 days ago

Peer Response

Similarly, as discussed above, Sheldon Investment Limited failed to obtain consent from the customer to receive emails from the company. This case study addresses an aspect of General Data Protection Regulation (GDPR) Consent. Intersoft consulting (2021) states that:

> 'Processing personal data is generally forbidden, unless permitted by law, or the data subject has consented to the same. Article 7 recital 32 of the GDPR further states that Consent must be freely given, specific, informed and unambiguous. In order to obtain freely given consent, it must be given on a voluntary basis. The element "free" implies a real choice by the data subject. Any element of inappropriate pressure or influence which could affect the outcome of that choice renders the consent invalid.'

Reference

1. Intersoft consulting(2021)GDPR Consent
Available from
https://gdpr-info.eu/issues/consent/
[Accessed 27 June 2021].

Reply

2

Post by **Aimalohi Odia**

17 days ago

Peer Response

In this case, the complainant kept on receiving unsolicited marketing emails even after several complaints had been made to the Data Protection Commissioner. Sheldon Investments Ireland Limited pleaded guilty to two charges of sending unsolicited marketing emails without consent and paid €800 in the form of a charitable donation to Focus Ireland as damages.

The General Data Protection Regulation (GDPR) requires personal data to be processed lawfully, Article 6 defines the scope for what is regarded as lawful and Article 6 (1) (1) in particular states that for processing to be regarded as lawful, consent must be obtained from the data subject for the processing of his or her data. In addition, Art 21(3) and Recital 70 gives the data subject the right to object to processing for direct marketing purposes. (GDPR, 2018)

REFERENCE

GDPR, 2018. *Guide to the General Data Protection Regulation*. [online]GOV.UK.

Available at [Accessed 27 June 2021]

Reply

3  Post by **Doug Millward**

17 days ago

Initial feedback

Dario makes some excellent observations about this case - which is similar to the one reviewed by Charlotte elsewhere. As with Charlotte's observations, it SHOULD be possible to use automation to remove a name 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.

Reply

4  Post by **Jan Küfner**

14 days ago

peer response

I do agree with Doug, that consolidating databases is possible from a technical point of view. To not do this must have other reasons, such as e.g. avoiding costs to do so. Another reason could also be, that the company willingly accepted the fine since this behavior might nonetheless be profitable for the company in the end.

To avoid future potentially higher fines, it is nonetheless recommended to invest in redesign of the database structure and the application. To ensure proper functioning training for staff is necessary. The effectiveness of overall implementation can be checked by regular audits and requirements for CIA as per GDPR article 32 can be verified via pen-testing. (EUR-Lex 2016)

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: (1)

5  Post by **Doug Millward**

6 days ago

Final Summary

Jan as usual makes some very good points in summarising this thread. Often the solutions to GDPR challenges are both social and technical, as Jan highlights above.

Reply

Add your reply

Your subject

Type your post

Dateien auswählen Keine ausgewählt

Submit

Use advanced editor and additional options

OLDER DISCUSSION

Initial post - Department of Justice and Equality case

NEWER DISCUSSION

Initial Post