Network and Information Security Management May 2021 A

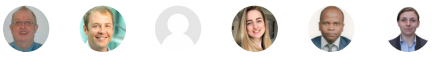
« Collaborative Learning Discussion 3

Charlotte Wilson

Initial Post

23 days ago

8 replies



Last 3 days ago

In the Virgin Media Ireland Limited case study, the aspect of GDPR that is addressed is the “Right to Erasure”. Within the case study, an individual wanted to ensure they were not called for promotion purposes, and although multiple requests had been made changes were not conducted. Part of the “Right to Erasure” includes “Individuals can make a request for erasure verbally or in writing” and “a right for individuals to have personal data erased”, both of which the individual did and should have had in the case study (ICO, 2018). To rectify the situation, Virgin Media Ireland Limited reviewed all requests made within a certain time period and ensured all had been completed correctly, and any manual errors had been rectified.

To avoid these situations in the future, steps can be put in place. For example, automation across systems could ensure that manual error is limited. If for example, when an individual calls, this starts an automated process which removes that individual from any call list, manual intervention could be limited and in turn manual error avoided. Another solution could be to review the process and complete spot checks periodically, to ensure that requests are completed in full and correctly. This would stop individuals having to contact further to ensure their right to be forgotten has been completed.

References

ICO (2018) Right to Erasure. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ [Accessed 23 June 2021]

Reply

8 replies

1 

Post by Laura Rivella

21 days ago

Peer response

Hi Charlotte,

We agree with your analysis and we would like to add to a few of the points you made to broaden the discussion and bring additional trends to light.

The case summary states that Virgin Media Ireland Limited cited human error as the cause for the complainant's account not being updated correctly. (Data Protection Commission, 2017) You rightfully highlighted the fact that automation could ensure that manual error is limited.

Automation appears to be applied in some areas in order to maximise profit by removing humans in call centers and substituting them with chatbots. So while the capability to apply automation is within reach of companies like VMIL, it is not being applied in a way that ensures data security or customer support. This should be kept in mind and revisited at a later date to check if legislation is being drafted around this issue.

To cite human error when presented with legal action, especially in the case of multiple complaints and previous offenses under another name (Data Protection Commission, 2017) is preposterous. The latter being particularly concerning since it means that VMIL, previously trading as UPC Communications Ireland Limited has been exhibiting a good degree recidivism since 2010 at the very least. It is also worth noting that no mechanism to prevent marketing offenses from reoccurring appears to have been put in place between the first recorded offense in 2010 and 2017.

In the case at hand, the local Court proceeded to convict the company on both charges and fining them €1,500 and €1,000 respectively on the charges. (Data Protection Commission, 2017) While it is true that customer turnover is one of the key factors in a competitive market with little margin such as telecommunications and media, it is still hard to justify the aggressiveness of some marketing campaigns. For a company like VMIL with a revenue surpassing 500 million dollars (Libertyglobal, 2021) it is very easy to plead guilty to offenses, pay incredibly low fines and apologise.

This highlights two key issues, the first being the lack of credible dissuasive measures to preempt the behaviour from occurring in the first place. The second being that only a small and negligible percentage of the population will actually notify the data protection authority about a violation.

TLL (Amy, Chris, Laura, Shiraj)

References

Data Protection Commission (2017) Case Studies. Available from: **https://dataprotection.ie/en/pre-gdpr/case-studies#201711** [Accessed 25 June 2021].

Libertyglobal (2021) Virgin Media Ireland Limited Data. Available from: **https://www.libertyglobal.com/operation/ireland/** [Accessed 25 June 2021].

Reply

2  Post by **David Luvaha**

19 days ago

Peer Response

Similarly, 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

3

Post by **Freya Basey**

18 days ago

Peer Response

Further to the contravention of the data subject's right to erasure, Virgin Media Ireland Limited had no justification for utilising the complainant's personal data for continued marketing as consent had been withdrawn (Data Protection Commission, 2020). Whilst it is clear in the case of Virgin Media Ireland Limited that appropriate processes were not in place or followed to make the withdrawal of consent available to the complainant, sometimes the availability of these mechanisms does not translate to usability (Habib et al., 2020). This ultimately leads to the same outcome of rights of the data subject not being exercised in line with the GDPR.

The GDPR focusses on usability and states that "it shall be as easy to withdraw as to give consent" (EUR-Lex, 2016: Article 7). However, in practice opt-out options can be difficult to access and confusing for consumers. This not only breaches Article 7 but it can also lead to reputational damage for the company by frustrating consumers and leading them to report marketing as spam.

References

Data Protection Commission (2020) Pre-GDPR Case Studies. Available from: **https://www.dataprotection.ie/en/pre-gdpr/case-studies#201705** [Accessed 28 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 28 June 2021].

Habib, H. et al. (2020) 'It's a scavenger hunt: Usability of Websites' Opt-Out and Data Deletion Choices', *CHI Conference on Human Factors in Computing Systems*. New York, USA, 25-30 April. Association for Computing Machinery. 1-12.

Reply

4 Post by **Aimalohi Odia**

17 days ago

Peer Response

This case is concerned with making unsolicited marketing telephone calls to customers, in this case, Virgin Media Ireland Limited pleaded guilty to two charges of making unsolicited marketing telephone calls to its customer even after she notified the company that she did not wish to receive such calls.

Article 5 requires personal data collected to be processed to be adequate, relevant and limited to what is necessary, processed lawfully and kept no longer than is needed. Article 6 and recital 46 define the scope of 'Lawfulness of processing'. One very important pre-requisite for lawfulness is consent which is defined in Article 4(11) of the GDPR. Consent of the data subject was absent in this scenario thus making it unlawful. (GDPR, 2018)

Article 18(1)2 gives a data subject the right to request that the use of their personal data be restricted, in circumstances where the data subject has not requested for a total erasure of personal data like in this scenario. Article 12(2) on the other hand puts the data controller under an obligation to facilitate the exercise of data subject rights under articles 15-22. In addition, Article 21(3) gives data subjects 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

5  Post by **Doug Millward**

17 days ago

Initial feedback

Charlotte makes some very interesting observations about this case, with some excellent recommendations on how to mitigate the issue. Laura in addition provides some very interesting insights. It is worth noting that technology could be used to resolve these types of issues but as Laura notes some corporations would rather pay relatively small fines and continue to annoy ex-customers.

Reply

6 

Post by **Jan Küfner**

15 days ago

Peer response

As others already suggested, the company might willingly ignore current laws to make more profit. It was however not yet mentioned that the height of the fine is subject to a court decision, since GDPR is a European law and disputes are clarified in trials. As judges give the verdict, it can be assumed, that with a reoc-curring GDPR breach, the fines will increase. Chances are therefore, that the company did change their current practice already since they might fear higher future fines.

To accomplish avoiding future fines a system including database, that collects initial consent and let's a user revoke this consent via multiple interfaces should be implemented. Employees of the call center should be also able to access the database to alter the consent data entry. The effectiveness of the system should be tested on a regular basis in GDPR audits. Pen-tests should additionally be conducted to ensure requirements of article 32 (EUR-Lex 2016) Since running a call center is prone to human error, continuous awareness trainings are highly recommended.

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)

7 

Post by **Doug Millward**

6 days ago

Final Feedback

Again, an insightful and well-constructed post from Jan. In situations such as these, not only should fines be imposed that will make the companies change their approach and comply with both the spirit and letter of the GDPR regula-tions, there also needs to be some principles that ensure the privacy and rights of individuals is respected.

Reply

8  Post by **Charlotte Wilson**

3 days ago

Summary Post

The Virgin Media Ireland Limited case study is an interesting one, with a focus on Right to Erasure from a GDPR perspective. It was agreed that human error can be the cause of many GDPR related incidents, including that of Virgin Media. It was also agreed that the use of automation may alleviate some of these issues as processes can be followed in a clearer and more concise way, without need for human interaction or error (Rivella, L., 2021). An additional point was made regarding companies “taking the hit” of the fine as this can be a smaller price to pay, both noted by Laura and Jan. This is something to highlight as unfortunately, it is known that companies will choose this option rather than making the necessary changes. For some organisations, it is actually more cost effective to take the risk than it is to invest in new security tools or controls.

A mitigation that was suggested by Jan was to implement a system to hold a user's consent status, allowing them to update this themselves via a Web Interface (Kufner, J., 2021). This level of automation, although costly to begin with, will ultimately be more cost effective and in line with GDPR requirements, as well as ensuring the reputation of VML is seen as being held to a higher standard. For many consumers, the ability to exercise this right to their personal data and to stop potentially unwanted notifications is expected and without it, many will also exercise their right to report it. (Jan)

Overall, this case study could have been avoided if automation was in place and a checking process implemented. To further enrich both mitigations, training of employees on the GDPR requirements and potential consequences can help avoid these incidents from happening to begin with, but also escalating any further than necessary (and ultimately resulting in larger fines and consequences.)

Kufner, J. (2021) Discussion Forum post by Charlotte Wilson, 2 July

Rivella, L. (2021) Discussion Forum post by Charlotte Wilson, 26 June

Reply

Add your reply

Your subject

Type your post

Dateien auswählen Keine ausgewählt

Submit

Use advanced editor and additional options

Older discussion

Initial Post