Network and Information Security Management May 2021 A

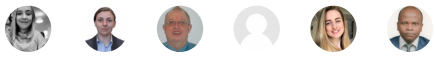
« Collaborative Learning Discussion 3

Jan Küfner

Inital Post

23 days ago

7 replies



Last 10 days ago

Case Study K (2017-8) - „Failure to respond fully to an access request“

This case study is about a person trying to retrieve personal data collected by an organization, as allowed by GDPR Article 15. A request to provide the personal data (surveillance footage) was submitted by the person to further be used in a criminal case. The organization however did not provide all videos. A second request was made to request the remaining video footage, but at that time the request was made, the data was already erased as per standard procedure, which is in line with data deletion as stated in GDPR Article 5 1e. (EUR-Lex, 2016, Data Protection Commission, 2020)

The company was fined for not providing all footage, since they should have provided the footage initially or should have safeguarded personal data in question once a request to obtain such data is made. (Data Protection Commission, 2020)

In general, it can be said, that GDPR processes need sufficient resources such as staff, IT infrastructure and tools. Additionally, training must be provided, and the effectiveness should be monitored on a regular basis by GDPR audits. In this case a process to preserve all records from routine deletion once an access request is received was missing. Once this process is implemented and trained, the likelihood of reoccurrence of a similar issue is considered low.

Data Protection Commission (2020) Pre-GDPR Case Studies. Available from: https://www.dataprotection.ie/en/pre-gdpr/case-studies#201708 [Accessed 23.06.2021]

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 06 2021].

Reply

Maximum rating: (1)

7 replies

1 

Post by **David Luvaha**

19 days ago

Peer Response

As discussed above, this is an absurd case where a subject was denied access to vital information resulting to delayed justice. According to EU GDPR Academy (2021) GDPR gives data subjects right to information which equips them with the ability to request an enterprise for information about their personal data being processed and the rationale for such processing. Secondly, GDPR gives them right to access hence the data subject has the capability to get access to his or her personal data that is being processed which includes viewing their own personal data, as well as to request copies of the same. Last but not least GDPR gives data subjects right for data portability where it give the data subject the right to ask for transfer of his or her personal data. As part of such request, the data subject may ask for his or her personal data to be provided back (to him or her) or transferred to another controller.

References

1. EU GDPR Academy (2021) Data subject rights according to GDPR Available from https://advisera.com/eugdpracademy/knowledgebase/8-data-subject-rights-according-to-gdpr/ [Accessed 27 June 2021].

Reply

2 

Post by **Freya Basey**

18 days ago

Peer Response

Further to Jan's recommendations and as per Article 12, processes should be implemented for staff to record and appropriately action any data subject access request (DSAR) to ensure none are missed (EUR-Lex, 2016). This is particularly important where the data is only available for a set amount of time, as can be seen in this case study (Data Protection Commission, 2020). Furthermore, training regarding DSARs should be completed by all staff as a business has only one month to provide a response to the initial request under the GDPR and this request could go to any member of staff, either verbally or in writing, and they must therefore be able to recognise this type of request (ICO, N.D.).

Under the GDPR, businesses can no longer charge for processing DSARs as was common practice before the directive, therefore Jan's point on funding is particularly poignant and businesses must set aside appropriate funding to conduct this duty under GDPR. Funding should also consider methods for providing the data as this should match the way the data is requested. If it was requested electronically, over email for example, then the data should be provided electronically to ensure that the data subject can access it. With personal data tak-

ing many forms, businesses should ensure they have suitably secure mechanisms in place for sharing these different formats with due consideration for accessibility.

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].

ICO (N.D.) Right of Access. Available from: **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/** [Accessed 28 June 2021].

Reply

3

Post by **Aimalohi Odia**

17 days ago

Peer Response

This is a case of failure to grant a data subject their right of Access. Article 15(1) and (3) of the GDPR give the data subject the right to be provided a copy of any of their personal data undergoing processing. It is now required that organisations respond (In electronic format) as soon as possible and no later than 30 days. (GDPR, 2018)

REFERENCE

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

Available at [Accessed 27 June 2021]

Reply

4 

Post by **Doug Millward**

17 days ago

initial feedback

Jan makes some excellent points, highlighted by both David and Freya. Once again, as Freya notes, training is vital to ensure GDPR is adhered to. But it is

worth noting that the GDPR has potentially increased the responsibilities of companies that operate CCTV or other monitoring equipment and they need to review the. implications of owning and operating such equipment.

Reply

5  Post by **Laura Rivella**

17 days ago

Peer response

Hi Jan,

We agree with your recommendations and analysis. Since you selected a very interesting case, we would like to expand on GDPR regulations and broader regulations when it comes to CCTV surveillance footage. (European Data Protection Supervisor, N.D.)

Video-surveillance footage can be used to identify people either directly or indirectly and it therefore qualifies as personal data.

The main issues with it are: (European Data Protection Supervisor, N.D.)

- Data quality - Cameras should only target specifically identified security problems thus minimising the gathering of irrelevant footage (data minimisation).
- The right of information - signs that inform about monitoring, purpose, length of time and purpose of the footage must be installed.
- Retention period - the timely and automatic deletion of footage is essential.

All of the above have cybersecurity ramifications as well since the footage must be safely stored, retrieved if needed and destroyed within the time frame dictated by the law.

It's worth noting that while the GDPR does play a role in laying out privacy safeguards when it comes to video surveillance, it does not account for everything. National legislation must be taken into account since every country has a different regulatory body in charge of enforcing GDPR and it may do a poor job at it. (Bischoff, 2021)

In the UK, additional laws covering CCTV are the Data Protection Act (DPA), the Freedom of Information Act (FOI), the Protection of Freedoms Act (POFA) and the Human Rights Act (HRA). The adherence to the data protection laws, in this case falls under the Information Commissioner's Office (ICO), which also issued a specific code of practice for data controllers to follow. (

Last but not least, it's always a good idea to check criminal law in one's own country to assess the case under examination since not every country enables the same methods of collecting evidence to be presented in court.

TLL (Amy, Chris, Laura, Shiraj)

References

Bischoff, P. (2019) Data privacy laws & government surveillance by country: Which countries best protect their citizens? Available from: **https://www.comparitech.com/blog/vpn-privacy/surveillance-states/** [Accessed 28 June 2021].

Information Commissioner's Office (N.D.) CCTV. Available from: **https://ico.org.uk/for-organisations/guide-to-data-protection-1998/encryption/scenarios/cctv/** [Accessed 28 June 2021].

European Data Protection Supervisor (N.D.) Video-surveillance. Available from: **https://edps.europa.eu/data-protection/data-protection/reference-library/video-surveillance_en** [Accessed 28 June 2021].

Reply

6  Post by **Charlotte Wilson**

17 days ago

Peer Response

To further your point Jan regarding GDPR processes needing sufficient resources, I believe this to be necessary within implementation. As you have mentioned, this could include training of staff so that they understand all requirements and necessary steps when receiving a note of an access request. I agree that when an access request is received, preventative measures should be put in place to ensure all data requested is available to the individual.

It is imperative that processes are documented to ensure that this work is in line with the GDPR standard. For example, within the guidance, one of the key principles is storage limitation. This ensures that personal data is not kept any longer than is deemed reasonable and required. If a process was to potentially increase the amount of time the data was stored for, this would need to be documented and stringent measures in place to ensure that once used, it was deleted as per the original process (ICO, 2018).

One other thing to note would be if there were any implications on other individuals within the CCTV footage and if extended storage is required, technology would be used to anonymise any other individuals within the footage. Depending on how frequently the requests for this information are, this could come at a cost that outweighs the potential fines - something organisations unfortunately have to consider.

References

ICO (2018) Principle (e). Storage Limitation. Available from: **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/** [Accessed 29 June 2021]

Reply

7  Post by **Jan Küfner**

10 days ago

Summary Post

In this case a company having video surveillance was discussed, many contributions of my fellow peers helped me to identify the specific GDPR challenges companies face, that have video surveillance. (Data Protection Commission, 2020)

As any data needs to be deleted after a certain amount of time as per GDPR and as video surveillance data must in most cases be looked at to verify that this section of the tape is showing the person sending in a data subject access request (DSAR), it can be said that a good DSAR process is especially important for companies having video surveillance. Since GDPR compliant storage of data and handling of such data in case of e.g., DSAR request costs a lot of money, companies must ask themselves, if they can reduce their surveillance / minimize the data to reduce costs. (EUR-Lex, 2016)

During the discussion there was wide agreement that GDPR processes need sufficient resources such as staff, IT infrastructure and tools. The fact that training is key to ensure GDPR compliance was also agreed by all. To check the overall implementation, it is essential to have GDPR audits on a regular basis. GDPR specific grey box pen-tests trying to e.g., disclose information also should be conducted.

If a company also learns from procedural failures in a way that they integrate e.g., missing steps into their processes or correct certain process steps to remediate the issue, the system will continue to improve to an ideal state. To further avoid human error and to make the overall system more robust against failure, it can also be said that a technical solution should be favored over an organizational solution to mitigate issues. It needs to be stated, though, that for some e.g., smaller companies it is simply cheaper to implement a solution that relies on human paying attention rather than coding algorithms, that e.g., ensures, that important process steps are not missed.

Data Protection Commission (2020) Pre-GDPR Case Studies. Available from: https://www.dataprotection.ie/en/pre-gdpr/case-studies#201708 [Accessed 23.06.2021]

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 06 2021].

Reply

Maximum rating: -

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

Summary Post