A Case Study of Violating GDPR by Installing Surveillance Cameras

Zeling Feng
Brown University

Abstract

At least since 05/15/2018, Mr. Rudolf in Austria has installed surveillance cameras around his own apartment. [1] However, those cameras also recorded the areas that surrounded his apartment, which were originally intended for the general use of the residents in the residential complex. Thus, the person who installed those surveillance cameras has become the controller of the video surveillance data, whose subjects included all other residents in his residential complex. It was even worse that the surveillance cameras were being operated under no notice from Mr. Rudolf and other residents never gave Mr. Rudolf their consent for their image data being collected. This certainly violated several articles of GDPR. Austrian Data Protection Authority ordered a fine of €2200 to Mr. Rudolf regarding to this reported incident because of Mr. Rudolf's lack of legal basis for his data processing.

1 Background

Video-surveillance footage often contains images of people. As this information can be used to identify these people either directly or indirectly (i.e. combined with other pieces of information), it qualifies as personal data (also known as personal information). [6] A data subject [3] is any natural person whose personal data is being collected, held or processed. In this incident, The data subjects were those people who lived in the same residence building as Mr. Rudolf. The data controller in this case was Mr. Rudolf himself because he defined the surveillance purposes and means of the processing of the personal data of the data subjects. The data processor in this specific case happened to be the same as the controller because the personal data was not processed by someone else, Mr. Rudolf, the surveillance camera installer exclusively controlled the surveillance data and processed the surveillance data all by himself.

2 GDPR Violation

2.1 The Incident

The incident was reported by the residents in Mr. Rudolf's residencial complex. Mr. Rudolf has violated several GDPR articles by installing those surveillance cameras as he controlled the personal data, images of the residents, and processed those data without any explicit consent from the data subjects, which is unlawful. More specifically, Mr. Rudolf's installed survaillance cameras not only recorded what happened in his own apartment, but also recorded the area intended for the general use of the residents of the multi-party residential property, namely: Parking lots, sidewalks, courtyard, garden and access areas to the residential complex. What's more, the video surveillance recorded garden areas of an adjacent property. [1] The video surveillance deployed by Mr. Rudolf also filmed his roommates entering and leaving the surrounding apartments. [1] The image data captured by video surveillance were thus not restricted to Mr. Rudolf's own apartment alone.

However, all these collection was not indicated anywhere and the data subjects gave consent to neither the collection nor the processing. Thus, Mr. Rudolf's practice was against the Article 5 1 (a) and 1 (c). [3] and the processing was not lawful since Mr. Rudolf has not minimised the data collection. Mr. Rudolf's processing of the image data collected by his surveillance cameras was unlawful because he had not received the consent from his data subjects, which violated Article 6, [3]. There is no information of the surveillance data being collected provided by Mr. Rudolf which violated Article 13. [3] It was reported to Austrian Data Protection Authority. Mr. Rudolf was fined €2,200.

2.2 The Cause

Mr. Rudolf was solely responsible for the GDPR violation because he as a natural person was the exclusive controller and processor of the image data collected from the residents so he should be responsible for the violation. If the video surveillance *only* covered the private area of Mr. Rudolf's apartment, then it should be fine because all the surveillance data were now only Mr. Rudolf's personal data and processing his own personal data is lawful. The violation occurred because Mr. Rudolf didn't make sure the monitored area was restricted to be only in his own apartment. The technical difficulty here is that if the surveillance camera is deployed near the window, chances are that the surveillance camera can record what is happening outside the window, which probably will involve other residents. The human factor of the violation is that Mr. Rudolf might not be aware of GDPR or may not understand collecting other residents' image in his video surveillance is also regulated under GDPR so he must give a lawful ground to his collection and processing.

2.3 Prevention

This violation, of course can be avoided. The most easiest way is to only install the surveillance cameras inside Mr. Rudolf's room. This will prevent the cameras from accidentally filming the public area and thus collecting the image data from other residents. However, this is still not enough to be GDPR compliant, since there are still chances that Mr. Rudolf's may meet with his guests in his apartment. If this is the case, it is hard to not collect the image of his guests in the video surveillance, so Mr. Rudolf must ask for consent from his guests. If his guests refuse to give consent to the collection of their image data, then Mr. Rudolf must turn off his surveillance cameras to ensure he is not unlawfully collecting his guests' image data without consent. If Mr. Rudolf is paranoid about getting surveillance video surrounding his own apartment, then he must ask for consent from everyone that could be possibly captured by his surveillance cameras. He must ask for consent from all of the residents because they all have a chance to be captured. But I think this is probably not enough, because non-residents' image data could also be collected during visit and it will be extremely hard to get consent from everyone.

3 Discussion

This case is a special one as the controller was a natual person rather than a big company. When talking about data privacy, we always first think of big companies who have a lot of data and they must respect the GDPR. However, we as ordinary people can still violate the GDPR and be fined for quite amount of money. This case really reminds us that we are not only data subjects but also we can be data controllers as well. So understanding GDPR not only lets us know what rights do we have as a subject but also lets us avoid violation and fines.

This case interested me not only because an individual was fined instead of a big tech company, it is also interesting in term of how much Mr. Rudolf was fined. Let's take a look at a high-profile case where the tech giant, Google, violated GDPR and was fined €50,000,000 by CNIL in 2019. [4] Google is responsible for the violation because Android's onboarding process is not GDPR compliant. Now there is an interesting question, how many data subjects were affected by the Google violation. There is not much public figures showing how many Android users there are in Europe, so the best we can do is to estimate. Some source [2] says the number of smartphone users in West Europe in 2016 is about 240.3 million and another source [5] says Android took up to 68% of the mobile operating systems market in Europe in 2016. Given these two figures, we can do a rough esitimation that back in 2016, there were approximately 164.2 million Android users in Europe. That said Google was fined €1 for every 3.28 data subjects. However, in Mr. Rudolf's case, I would doubt if there were 7200 residents living in the same residential building. I understand this might be an unaccurate way to compare these two cases, because a). The numbers are not accurate, b). Both cases violated very different articles, but at least from the perspective of how many people were affected in the violation, I would like to argue Mr. Rudolf might be fined too much.

Most organizations and possibly individuals were aware that GDPR applied to text-based data – name, email and physical addresses, etc. However, static and video images also represent personal information to which GDPR applies. This case is thus an important one to us because this reminds us that surveillance data is also regulated by GDPR.

References

[1] Austrian Data Protection Authority. DSB-D550.037/0003-DSB/2018. "https://www.ris.bka.gv.at/Dokument.wxe".

[2] Statista Research Department. Number of Smartphone Users in West Europe. "https://www.statista.com/statistics/494554/smartphone-users-in-western-europe/", 2015. "online; accessed 18-Sept-2019".

[3] EU. Regulation (eu) 2016/679 of the european parliament and of the council. "https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1797-1-1", 4 2016. "oneline; accessed 18-Sept-2019".

[4] Commission nationale de l'informatique et des libertés. The cnil's restricted committee imposes a financial penalty of 50 million euros against google llc. "https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-5 2019. "online; accessed on 18-Sept-2019".

[5] StatCounter. Mobile Operating System Market Share Europe. "https://gs.statcounter.com/os-market-share/mobile/europe/2016", 2016. "online; accessed 18-Sept-2019".

[6] European Data Protection Supervisor. Video-surveillance. "https://edps.europa.eu/data-protection/data-protection/reference-library/video-surveillance_en", 2019. "online; accessed 18-Sept-2019".