GDPR Case Study: Stockholm Public Transport

Richard Abou Chaaya
Brown University

Ishan Sharma
Brown University

Abstract

On June 21, 2021 the Swedish Authority for Privacy Protection (IMY) fined the Stockholm Public Transport (SL) $1,853,504.00 (16 million SEK) for equipping their ticket controller with body camera that would record travellers. Upon investigation, it was found that SL did not have lawful grounds for processing this data, that they did not provide enough information to the travellers about the data collected and that they processed more personal data than necessary thus violating the principle of data minimization.

1 Background

SL operates the public transport in Stockholm. On December 10, 2018 SL started equipping its ticket controllers with body-worn cameras (BWC). On weekdays there are about 55 controllers throughout the transport system and 20 on holidays. These cameras would be used to record the travellers assigned a penalty fare for not having a valid ticket. Fare evasion is a major problem for SL which claims that it accounted for a loss of SEK 280 million ($32,634,609.37) in 2018 [2]. The safety of the ticket controllers is also a concern for SL. Indeed, 62 incidents (verbal attacks, threats of violence and violence) were reported in 2018, 110 in 2019 and 226 in 2020 [2]. Therefore, according to SL, the purpose of the cameras is to:

- Prevent threatening situations related to ticket control (purpose A)
- Document incidents to facilitate subsequent investigations (purpose B)
- Record the identity of the travellers fined for not having a valid ticket to ensure that the right person pays the charge (purpose C)

The goal is twofold: protect ticket controllers and ensure that penalty fares are paid and by the right person.
According to SL, using cameras has had a positive impact. Fewer penalty fares are contested, fewer people try to give a fake identity and ticket inspectors feel safer. Furthemore, while the absolute number of incidents has grown over the years, the number of "serious incidents" (violence) has decreased from 24 in 2018 to 9 in 2019 and 5 in 2020 [2]. SL attributes this evolution to the use of cameras. When the decision to use cameras was taken, the Swedish Authority for Privacy Protection (IMY) started investigating SL's personal data collection and processing.
The cameras are operated by ticket controllers. They continuously record video and audio to a circular memory which has 1 minute worth of storage (it initially had 2 minutes but was reduced during the testing period). When the ticket controller presses a button, the camera starts recording on permanent storage. Furthermore, the 1 minute video in the circular memory is also added to the stored footage(*activated recording*) [2]. This functionality exists in order to show the course of events just before the issuance of a penalty fare or leading to threatening/violent situations.
When the ticket controller finishes a shift, the captured videos are sent to a server for review. Additionally, when a ticket controller issues a penalty fare, a paper is printed giving information about the company's personal data processing. It explains that SL may process the photo and / or film of the travellers [2].

2 GDPR Violations

Overview: In this particular case, IMY decided to supervise the use of BWCs by SL after noticing media reports on SL's test programme for equipping ticket inspectors with BWCs. After investigation, they found that, for all three purposes, SL did not have lawful grounds for processing data (Article 6.1), were against fairness, transparency and legality (Article 5.1(a)) and processed more data than was necessary (Article 5.1(c)). They also violated Article 13 by not providing users with sufficient information before processing their personal information.

In order to deem the lawfulness of processing, each pur-

pose must satisfy at least one of the conditions in Article 6. In this particular case, SL based their grounds for lawful processing under Article 6.1(f). Which states that an entity may process data even without obtaining users explicit consent if it has a legitimate interest and if the interest does not override the fundamental rights and freedom of the data subject [1]. Processing will only be considered lawfull if the entity has a *legitimate interest* and if processing is *necessary* to fulfil that interest.

Purposes A and B: They are related and hence are evaluated together. SL had demonstrated that as a consequence of the use of BWC, there was a significant decrease in serious incidents [2]. Hence, SL stated that they had a legitimate interest in using the BWCs in order to reduce violence against ticket inspectors. SL was also able to demonstrate that the use of BWCs was necessary as they had taken alternative measures - having guards accompany the ticket inspectors - that did not suffice [2].

Based on the facts provided, the IMY believed that there was a legitimate interest and that the use of pre-recording technology was necessary but that *activated recording* was violating GDPR [2]. However, they concluded that pre-recording continuously or in the case of an incident for the period of 1 minute was too invasive from the perspective of people surrounding the perpetrator as they were unaware of being recorded. Hence, in its current state processing was not necessary for A and B as it was unlawful under Article 6.1(b) and against legality and data minimization as stated in articles 5.1(a) and 5.1(c). IMY concluded that if pre-recording was done for a shorter period of time (which it considers 15 seconds) then the purposes could have been deemed necessary [2].

Purpose C: IMY concluded that although they had a legitimate reason, recording video and sound for identification of the data subject was not necessary [2]. Less privacy-invasive means like asking the traveller to present an identity document or taking a still picture could have been used instead. SL had no legal grounds under Article 6.1(f) and hence was in violation of the principle of legality based on Article 5.1(a) [2].

Violation of Article 13: Upon issuing a surcharge the receipt contained details regarding active recording and relevant contact information for further questions. But this information was provided after the recording had started [2]. Furthermore, other travellers who were in the frame were not being provided with this information. SL had mentioned the use of BWCs on their website but it failed to mention that it recorded sound as well [7]. Hence, it was concluded that SL violated Article 13 which has no exceptions when it comes to providing relevant information to the data subject regarding the collection of personal data. [2]

Fines: In the investigation it was decided that purposes A and B constitute a different infringement from purpose C. Additionally, not disclosing enough information about the data processing constitutes a third infringement. SL was fined USD 460K for purposes A and B and USD 920K for purpose C [2]. It is important to note that the first fine is lower because SL had a legitimate interest for purposes A and B, whereas that was not the case for purpose C. Apart from this, it was also fined USD 460K for violating Article 13 [2]. These fines were imposed in light of the fact that SL is a publicly owned company [6] and the ticket inspection system is not for profit but rather to increase public willingness to pay for tickets [2].

Potential prevention and response: During the supervision, SL did take active measures to increase transparency and address privacy concerns. They reduced the pre-recording time from 2 minutes to 1 minute and the ticket inspectors started wearing badges that indicated that a data subject was being recorded [2]. This did not seem to have an impact on the final decision by IMY. However, SL could certainly have made more effort in letting the customers know that they were being recorded. For instance, they could have printed out relevant information on the tickets as well in addition to displaying it on their website.

After the fine, as of today, SL still makes use of the BWCs [5]. But they have also updated their website to indicated that in addition to video audio is also being recorded [4].

3 Discussion

We feel that the penalty for purposes A and B are too harsh. Especially because of the fact that a precedent had not been established and that IMY did not provide any valid reasoning behind its interpretation of a "shorter time" of 15 seconds. Regarding the 15 second decision, there are two motivations. The first being to reduce the amount of data collected in pre-recording pertaining to an incident and the second is to reduce the amount of data collected during continuous pre-recording. Upon closely inspecting the report, the investigators seemed to have a greater concern regarding the continuous ephemeral recording of 1-minute intervals. The following is a snippet from the report regarding their judgement summary:

"Regarding the severity of the violation, IMY states that the treatment that took place to prevent and document threats and violence was largely legal (the treatment that took place during ongoing threats and violence). The violation in this part, however, consists of SL's excessive use of pre-recording technology through which they continuously recorded with picture and sound, for at least one minute." [2]

This concern has influenced the severity of fines imposed and we believe that this concern is largely baseless. BWCs do not have a screen and data is generally extracted from a docking station. In the case of SL the dock was stored in a locked space. It is highly unlikely that any human could gain access to a 1-minute clip before it gets erased. Therefore, in this context, it doesn't really matter if the camera continuously pre-records for 15 seconds or 1 minute. But we do acknowledge the fact that currently, the very act of recording is considered as "data processing" [8].

A precedent has been established and it will certainly have an impact on future cases that arise pertaining to BWCs. As a consequence of GDPR, firms have also started rolling out "privacy conscious" BWCs that include a host of features like AES encryption, access control, audit logging, custom retention/deletion policies among other things [3].

References

[1] General data protection regulation. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679. Accessed: 2021-09-24.

[2] Imy decision. https://www.imy.se/globalassets/dokument/beslut/2021/2021-06-21-beslut-sl.pdf. Accessed: 2021-09-24, translated to English via Google Translate.

[3] Privacy conscious bwc. https://www.edesix.com/downloads/data-protection/ED-008-001-04-DataProtection-Brochure.pdf. Accessed: 2021-09-24.

[4] Storstockholms lokaltrafik personal data processing. https://sl.se/kundservice/villkor/behandling-av-personuppgifter. Accessed: 2021-09-24, translated to English via Google Translate.

[5] Storstockholms lokaltrafik ticket control. https://sl.se/kundservice/villkor/biljettkontrollen. Accessed: 2021-09-24, translated to English via Google Translate.

[6] Storstockholms lokaltrafik wiki. https://en.wikipedia.org/wiki/SL_(Stockholm. Accessed: 2021-09-24.

[7] Swedish authority for privacy protection news. https://www.imy.se/en/news/unlawful-use-of-body-cams-in-stockholms-public-transport/. Accessed: 2021-09-24.

[8] What constitutes data processing? https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en. Accessed: 2021-09-24.