Case Study of the GDPR Violation by the Skellefteå Municipality School Board

Alexander J. Gaidis
Brown University

Abstract

The Skellefteå municipality high school board in Sweden was found to have violated Article 5 (1) c), Article 9, Article 35, and Article 36 of the GDPR by the Swedish Data Protection Authority in late August, 2019. Anderstorp high school was working with a private company, Tieto, to develop and test a facial recognition system to track student attendance. Despite getting the consent of students and their guardians before starting the pilot program, the data protectorate felt that due to the power imbalanc between the students and school staff as well as the sensitive and excessive nature of data being collected, there was insufficient legal basis for data processing. Additionally, facial recognition is a new, high-risk technology, and thus the school board should have sought consultation with the data protectorate before beginning the tests. The total fine against the school board was € 18,630.

1 Introduction

On August 20th, 2019 a fine of € 18,630 was levied against the High School board in Skellefteå municipality by the Swedish Data Protection Authority [1]. The charge came after the data protectorate saw in Swedish media that Anderstorp high school was conducting a pilot program with Tieto, an IT software and service company, to track student attendance via facial recognition. According to Tieto, logging attendance at the beginning of each class can total 17,280 hours per year at Anderstorp high school alone. Two methods were used to determine the presence of students. The first involved a tag[1] that students brought to the test classroom where a Raspberry Pi would then detect and log their presence. The second method involved facial recognition whereby students entering the test classroom had their photo taken and compared with ones previously acquired and stored at the school [2]. It was this second method that caught the attention of the data protectorate due to the sensitive nature of biometric data and new technology.

On February 19th, 2019 the Swedish Data Protection Authority sent a letter of inquiry to the school board to determine compliance with Sweden's data protection laws. A response from the school board was received March 15th, 2019 with three later additions that year dated April 2nd, August 16th, and August 19th. The school board disputed the claims of the data protectorate contending that consent was provided by the students and their guardians, and students who did not want to participate were not enrolled in the pilot program. While consent was sought, the data protectorate still held the Skellefteå municipality school board accountable for violating the GDPR [1].

2 Background

The Swedish Data Protection Authority (Datainspektionen) was formed in 1973 as a part of Sweden's world-first Data Act [4]. The data protectorate matured as new laws superseded the old to keep up with a changing technological landscape. In the most current legislation that went into effect on September 1st, 2019, the data protectorate's job was stated as protecting the basic freedoms and rights of people in relation to the processing of personal data [5]. Thus, when GDPR went into effect, Sweden was already in a good position to comply with the new regulation as they already had infrastructure in place.

Since the GDPR was passed, the case discussed within this paper is the only violation of Swedish data protection law. However, Anderstorp high school in Skellefteå municipality did not develop the technology they used in the facial recognition pilot program. Rather, a private company Tieto developed the technology. The system worked as follows. After the students provided consent, images of their faces were recorded and stored in a database to provide a baseline for the facial recognition algorithms. When students would enter the test classroom, new images of their face would be captured and compared against the baseline images held in the database. When a match was found, the student's name corresponding

[1] While no formal mention is made, I assume that by "tag" Tieto means RFID tag.

to the baseline images could be resolved and their attendance recorded [2]. The entire system was offline, only authorized personnel could access the data, and any data related to individuals not in the pilot were not persisted [1]. According to the Tieto briefing on the pilot, had it grown any bigger they advised notifying the Swedish Data Protection Authority.

The failure of the school to be GDPR compliant resulted in the letter of inquiry the data protectorate sent the school board as mentioned in §1. This letter and corresponding press releases reveal the following problem setting.

Data Subject: the 22 students participating in the facial recognition pilot program. Biometric data (photographs) were collected, stored, and mapped to names.

Data Controller: the Skellefteå municipality high school board. They got consent of the data subjects, acted as a point of contact for the pilot program, and decided the direction the study went.

Data Processor #1: the Skellefteå municipality high school board. They provided resources to aid in the processing and storage of student data.

Data Processor #2: Tieto. They provided the technology including processing and storage services. Additionally, they helped with oversight in the pilot program.

Though as will become apparent in §3, the data controller fell victim to the GDPR rather than the data processors. Namely, Tieto was entirely left out of the data protectorate's report [1].

3 GDPR Violation

The result of the compliance inquiry was unforgiving to the high school board's excuses. The Swedish Data Protection Authority quoted Article 5 (1) c), Article 9, Article 35, and Article 36 of the GDPR [6] as reason for the violation [1]. Below is a summary of their reasoning.

Article 5 (1) c) the use of facial recognition to keep attendance is superfluous and requires more data collection than the task demands.

Article 9 sensitive biometric data was processed including data that could reveal racial or ethnic origin or religious or philosophical beliefs. Also, the high school board did not qualify for any of the exceptions in paragraph 2.

Article 35 facial recognition is deemed a new, high-risk technology, thus the high school board should have conducted a more in-depth data protection impact assessment before starting the pilot program.

Article 36 the high school board failed to consult the data protectorate as should be done when a new, high-risk technology is used and a data protection impact assessment is (or should be) carried out.

3.1 Responsibility

To fully understand the decision made by the Swedish Data Protection Authority, consideration must first be given to the ecosystem in which the problem arose. Per the Swedish Education Act chapter 15 section 16, attendance control is mandated by law [3] and can have a significant effect on a student's progress through school. This contributes to an imbalance of power between students and school staff; where students are relient on teachers for grades, funding, and future opportunities [1]. Thus, even though the high school board received consent from the students and their guardians, they were subject to general provision 43 of the GDPR: "In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation." [6] No longer having the protection of students' consent left the high school board susceptible to GDPR violations and unable to argue via the GDPR's exceptions, such as those in Article 9 (2).

Notably, Tieto was not held responsible for any GDPR violations. As a data processor, they are held to different standards than data controllers. The responsibility of the data controller, as per Article 24 of the GDPR, spans the entirety of the violations noted by the data protectorate [6]. Namely, the Skellefteå municipality high school board failed to implement the appropriate technical and organizational measures to ensure processing of the data subjects' data was in-line with the GDPR.

3.2 Prevention

There are two measures the high school board could have taken to avoid a violation. First, had they notified the data protectorate before the pilot program started and not waited, the incident may have been avoided. When dealing with sensitive data, new technology, and the GDPR it is easier to ask for permission rather than forgiveness. Second, altering the security concept of *least privilege* for the GDPR to be *least technology* or *least data* would help prevent future fines as it plays into the data minimization described in Article 5 (1) c) [6]. Additionally, the less data collected to get a task done, the smaller the probability of a GDPR violation.

An example of a data and technology minimizing solution could be a small RFID tag, similar to Tieto's idea, but made more ergonomic so students wouldn't forget it at home. By making it into a backpack clip, say, the students will always bring it to class with them. When the students enter the classroom, a sensor could relay their presence to a computer which would mark it in a database. Alternatively, a smart tablet could be mounted at the front of the classroom. When students enter,

they could press the screen to check their name off. However, the problem with these two approaches is both can be made to believe there are more people present in the class than there are. Without approval to process more sensitive data for authentication, the means with which to combat false positives are limited.

It seems one of the only ways to navigate consent in an unequal relationship between data subject and data controller is to have valid justification that is pre-approved by the data protectorate. Articles that may allow one to develop preliminary judgement on this matter are Article 6 (1) b-f), Article 9 (2), and Article 17 (3) a-e) of the GDPR [6]. Ultimately seeking guidance from the data protectorate can help provide an unbiased view of the case.

4 Discussion

The data protectorate's choice to fine a public entity is significant as it sets the precedent that no one is above the GDPR in Sweden. Per Article 83 (7): "Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58 (2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State." [6] Thus, the data protectorate had the option to waive or lessen the fine, but since they didn't, their decision reflected a want to uphold the rights of their citizens in the face of government misconduct.

This decision comes at an interesting time as the spread of facial recognition in countries such as China has been rapid [7]. Certain sensitive information about an individual can be gleaned from the images captured by facial recognition systems that can be used to discriminate, such as religious beliefs and race. Further, facial recognition can be invasive, for example, if someone is wearing a hijab they would most likely have to remove it for the algorithm to work. There are many small nuances in this case that the forward-thinking data protectorate drew attention to. As a result, this is a landmark GDPR case in the use of facial recognition and could act to draw a clear line between policy differences of GDPR-following nations and non-GDPR-following nations.

5 Conclusion

Since the decision of the data protectorate in late August of 2019, the Skellefteå municipality high school board has remained quiet about the incident. The magnitude of time spent taking attendance will surely motivate the school board to continue investigating ways to automate this process other than facial recognition. The alternative method of taking attendance that Tieto explored with Anderstorp high school, using tags to register students, was less invasive but was impractical since the students forgot to bring their tags to school a large amount of the time. Thus, the problem is still without a satisfactory answer. This case has made it clear that GDPR is shaping how technological progress is made and who the technology is working for.

References

[1] Swedish Data Protection Authority. Supervision in accordance with the EU data protection regulation (2016/679) - facial recognition for attendance control of students, 2019. https://tinyurl.com/y65mn8qb.

[2] Tieto Corporation. Future classroom - summary, 2018. https://tinyurl.com/yyg3rcph.

[3] Swedish Ministry of Education. School act (2010: 800), 2010. https://tinyurl.com/y4va7p2m.

[4] Swedish Ministry of Justice. Regulation (2007: 975) with instructions for the data inspectorate, 2007. *Note: this document superseded an older document that formed the Data Protection Authority.* https://tinyurl.com/y57hdyn3.

[5] Swedish Ministry of Justice. Act (2018: 218) with supplementing provisions to the EU data protection regulation, 2018. https://tinyurl.com/yxdcan83.

[6] European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation), 2016. https://tinyurl.com/y4hu4m7h.

[7] Rob Schmitz. Facial recognition in china is big business as local governments boost surveillance, Apr 2018. https://tinyurl.com/y77pkcws.