GDPR Case Study: Biometric Fingerprinting in Poland School

Rebecca Zuo
Brown University

Abstract:

A school in Gdansk, Northern Poland, used biometric fingerprinting to verify student identity for purchasing school lunches. The fingerprints of hundreds of children were processed "without a legal basis", which violates the guidelines of the GDPR. As a result, the school has been fined €4,600. This case raises questions about which forms of identification are deemed necessary within a school system, and what special provisions should be made for data protection of children. In this paper, I will discuss the particularities of the legal violations of this case, as well as its results and implications.

1. Background:

The Polish school required students to use a biometric reader at the front of the cafeteria to verify payment of meals. Poland's Personal Protection Office, which is the responsible data protection agency, has deemed this unlawful. The school and its employees are both the data controllers and processors, while the students are the data subjects. In particular, two people had access to the data: the school administrator and the authorizing website [1].

No images of children's fingerprints were actually collected. Each students' fingerprint was scanned and converted to a sequence of bytes, which was then assigned to each student as a unique identifying number. Once the contract for school lunches was terminated, the data would be deleted from the reader, but a copy of the byte sequence would be archived and stored on a micro Sd card in a secure room [1].

SEWiP was the meal registration system used that takes the information from the reader to identify the registered student. The account is created using the name, surname, class, email address, parent's phone number, and fingerprint data of the student, if there is parental consent. The SEWiP program is installed on the school server. Once a fingerprint is scanned by the biometric reader, the system finds the student assigned to this person and whether the lunch status is paid or unpaid [1].

2. GDPR Violation:

The school's collection of biometric data violated Article 6 of the GDPR that allows data processing only when the task carried out in the public interest or with authority entrusted to the administrator. In this case, acquiring and collection biometric data, which is further prohibited in Article 9, does not meet the criteria. According to the GDPR in Article 9 Sect. 1, the processing of personal data, revealing biometric data to identify a natural person is prohibited. Furthermore, Article 5 states that data processing should be limited and minimized to the purposes for which they are processed

[3]. Other forms of identification with less invasiveness could have been used for cafeteria organization and function, so using biometric data was deemed unnecessary.

Additionally, proper consent of the data subjects according to Art. 4 sec. 11 means a voluntary, specific, informed and unambiguous demonstration of will[3], which in this case could not be achieved because of the clear imbalance between the data subject and the controller. Students who did not opt in to the fingerprinting had to wait until all other students had already gotten their meals, which demonstrates unequal treatment [2].

An ex school official reported this incident of unlawful processing of data to The President of the Personal Data Protection Office, and the school has been asked to change their data processing methods, to erase all personal data and to stop collecting such data [1].

This situation could have been prevented if the school had considered the consequences of collecting biometric data of children. The school did not consider its actions illegal, which demonstrates the lack of evaluation of what could possibly go wrong from collecting personal identifying data. Other methods could have been used to generate unique identifications for the students, such as a randomized id generator.

3. Discussion:

I think that the fine is justifiable in order to prevent schools from following similarly potentially invasive identification methods. In fact, there was a case that happened not too long before this incident that involved a Swedish School using facial scans to track attendance. The usage of these technologies demonstrates a desire for schools to streamline everyday functions, but these systems function at the cost of the privacy of the students from which the data is being collected. Furthermore, the usages of such identifying technologies involve biometric data, which under the GDPR is considered a "special category." It is considered as such because unlike email addresses or other markers, biometric data cannot be easily changed.

In this case, the school was not minimizing the data processing that was taking place. The data subjects were particularly vulnerable, because they were children who can't at the time give proper consent, while biometric data could still be used to identify them later on in their adulthood. The possibility of leakage of such information also present a higher risk to the rights and freedoms of natural persons. I also definitely agree that students should not have received unequal treatment for opting out of fingerprinting.

Ultimately, this case serves a precedent for European schools to minimize the data collected to complete its functions, and to carry out functions in more traditional ways. Perhaps, such regulations would limit the usage of education technology in classrooms. For instance, in an even more extreme case in China, artificial intelligence headbands were used to monitor student's brain-waves in order to improve grades and concentration [4]. This case demonstrates that the advantages of such technologies may be marginal in comparison to the loss of privacy.

References:

[1] Decisions of the President of the Personal Data Protection Office: https://uodo.gov.pl/decyzje/ZSZZS.440.768.2018

[2] Polish School Hit with GDPR Fine for Using Fingerprints to verify student's lunch payments: https://venturebeat.com/2020/03/06/polish-school-hit-with-gdpr-fine

[3] 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

[4] How China is Using Artificial Intelligence in Classrooms: https://www.youtube.com/watch?v=JMLsHI8aV0g