

USE OF FACIAL RECOGNITION IN SCHOOLS SANCTIONED UNDER GDPR

Category: Commercial Law, Privacy Law, Infosec, and POPIA, Technology Law
written by Delphine Daversin | September 3, 2019



Biometrics is often presented as the most ergonomic and effective way of organising access control. And this is probably the case! Local Swedish authorities reported that teachers were spending 17,000 hours a year reporting on attendance[\[1\]](#). Given this shocking statistic, facial recognition at the classroom entrance could well be a very attractive option...

The Swedish Data Protection Authority (the “**Swedish DPA**”) has, in its decision dated 21 August 2019[\[2\]](#), reminded us that “convenient” is not “compliant” and that biometric data processed in an environment where data subjects are dependants (such as school, work places, etc) should be considered with extra vigilance.

A school has conducted a pilot using facial recognition technology to record students’ attendance. The trial was conducted with 22 students for only a few weeks.

After investigating the case, the Swedish DPA concluded that the trial is not compliant with the provisions of the GDPR and fined the school an amount of approximately €20,000.00[\[3\]](#). This is the first fine issued by the Swedish DPA and it is quite substantial when compared to the number of data subjects involved and the very limited duration of the trial.

Here are the main take-aways from this decision:

Consent is not (always) enough

Processing of biometric personal data is prohibited, except in certain instances which are exhaustively listed under GDPR[\[4\]](#). One of these exceptions is the explicit consent of the data subject[\[5\]](#). In this case, the school claimed that consent to the processing had been obtained from the students’ legal guardians. The Swedish DPA however opposed that such consent was not adequate: the relationship between the school and the students is unequal and the children are dependent on their school environment. As a consequence, the consent cannot be considered as freely given and cannot be used as a legal exception for processing sensitive personal data.

The data controller should always look for the least intrusive / most proportionate way to achieve its objective (data minimisation principle)

Even though the processing was limited (only 22 students involved over a short period of time), the Swedish DPA stated that this processing was an unnecessary invasion of the students' privacy. Indeed, there are less intrusive ways of registering class attendance than using facial recognition.

A DPIA is required when the processing results in a high risk to the rights and freedoms of data subjects

The school did not conduct a proper Data Protection Impact Assessment ("DPIA") as required by GDPR "*where a type of processing in particular using new technologies (...) is likely to result in a high risk to the rights and freedoms of natural persons*"^[6]. The Swedish DPA decided that the school's risk assessment was too shallow and did not include a risk assessment of the impact of the processing on the data subjects' rights and freedoms. It also did not include an assessment of the proportionality of the processing in relation to its purposes.

It is interesting to note that this decision is in line with a regulation recently issued by the French Data Protection Authority (the "CNIL") regarding Biometrics processed in the work place for the purpose of access control^[7].

For more good, clear and precise advice, please do not hesitate to contact us.

[\[1\] Facial recognition: School ID checks lead to GDPR fine](#) - BBC News

[\[2\]](#)

<https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvaro-kontroll-av-elever-dnr-di-2019-2221.pdf>

[\[3\]](#)

https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en

[\[4\]](#) Article 9 (1) and 9 (2) GDPR.

[\[5\]](#) Article 9 (2) (a) GDPR.

[\[6\]](#) Article 35 GDPR

[\[7\]](#)

<https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-dacces-biometrique.pdf>