Swedish Data Protection Authority

Decision	**Ref. no.**
20.08.2019	DI-2019-2221

Skellefteå Municipality, Secondary Education Board
Skellefteå kommun, Gymnasienämnden

Supervision pursuant to the General Data Protection Regulation (EU) 2016/679 – facial recognition used to monitor the attendance of students

Contents

The Swedish Data Protection Authority's decision

The Swedish Data Protection Authority has concluded that, by using facial recognition via a camera to monitor the attendance of students, the Secondary Education Board (*Gymnasienämnden*) in the municipality of Skellefteå (*Skellefteå kommun*) has processed personal data in breach of:

- Article 5 of the General Data Protection Regulation[1] by processing students' personal data in a manner that is more intrusive as regards personal integrity and encompasses more personal data than is necessary for the specified purpose (monitoring of attendance),
- Article 9 by having processed special categories of personal data (biometric data) without having a valid derogation from the prohibition on the processing of special categories of personal data, and
- Articles 35 and 36 by failing to fulfil the requirements for an impact assessment and failing to carry out prior consultation with the Swedish Data Protection Authority.

Pursuant to Chapter 6 Section 2 of the Swedish Data Protection Act[2] and Articles 58.2 and 83 of the General Data Protection Regulation, the Swedish Data Protection Authority concludes that the Secondary Education Board of Skellefteå municipality must pay an administrative fine of SEK 200,000.

The Swedish Data Protection Authority concludes that the Secondary Education Board is likely to breach Articles 5 and 9 if it continues to use facial recognition for monitoring attendance.

The Swedish Data Protection Authority has therefore decided to issue the Secondary Education Board of Skellefteå municipality with a warning pursuant to Article 58.2(a) of the General Data Protection Regulation.

Description of the supervisory case

The Swedish Data Protection Authority became aware through information in the media that the Secondary Education Board in Skellefteå municipality (hereinafter 'the Board') had used facial recognition in a trial project at Anderstorp Secondary School in Skellefteå in order to register the attendance of students in a class over a number of weeks.

The purpose of the supervision was to investigate whether the Board's processing of personal data using facial recognition in order to monitor attendance was compliant with data protection regulations.

The Swedish Data Protection Authority has investigated the processing of personal data by the Board in the project concerned and reached a decision concerning possible future processing. Within the framework of this supervision, the Swedish Data Protection Authority did not carry out any assessment regarding security aspects or the notification obligation relating to the concerned processing.

The investigation revealed that, over a period of three weeks, the Board processed personal data through facial recognition in order to monitor the attendance of 22 secondary school students, and that the Secondary Education Board is considering processing personal data through the use of facial recognition for the monitoring of attendance in the future. The aim was to register attendance at lessons at the secondary school in a easier and more effective manner. According to the Board,

---

[1] 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).

[2] Act (2018:218) and supplementary provisions to the EU's General Data Protection Regulation.

registering attendance in a traditional manner takes ten minutes per lesson, and using facial recognition technology for monitoring attendance would, according to the Board, save 17 280 hours per year at the school concerned.

The Board has stated that the facial recognition involved the students being filmed by a camera when they entered a classroom. Images from the camera surveillance were compared with pre-registered images of the face of each participating student. The data that was recorded consisted of biometric data in the form of facial images, first name and surname. The data was stored on a local computer without any internet connection. The computer was kept in a locked cupboard. An explicit consent of the guardians was obtained and it was possible to opt out of the recording of personal data using biometric data.

The supervisory case was initiated with a letter of supervision dated 19 February 2019. A reply to this letter was received on 15 March 2019, with an addenda being added to appendices on 2 April 2019. Subsequent addenda were received from the Board on 16 August and 19 August 2019.

Justification for the decision

Personal data responsibility

The Board has stated that the Board is the controller regarding the processing of personal data that has taken place within the framework of the project using facial recognition for monitoring attendance at Anderstorp Secondary School in Skellefteå municipality. The Swedish Data Protection Authority shares this opinion.

Trial project

The processing operations concerned took place within the framework of a trial project. The Swedish Data Protection Authority notes that the General Data Protection Regulation does not contain any derogations for pilot or trial activities. The requirements of the Regulation must therefore also be met in order to carry out such types of activity.

Legal basis for the processing of personal data (Article 6)

Article 6 of the General Data Protection Regulation states that processing shall only be lawful if at least one of the stipulated conditions is met.

Consent as a legal basis

In its statement, which was received by the Swedish Data Protection Authority on 15 March 2019, the Board stated, inter alia, that consent was given for the processing that took place within the framework of the attendance monitoring.

The Board's statement included the following.

> *"I.e. the students' guardians are given information regarding the purpose of the project and the processing of personal data that will take place, and must give their explicit and voluntary consent for the processing. Students do not have to take part if they do not wish to; in such cases, attendance will then be monitored using the previous procedures. Students are also informed that they may withdraw their consent to the processing of personal data at any time. (p. 6)."*

Under Article 6.1(a) of the General Data Protection Regulation, processing will be lawful if the data subject has consented to the processing of his or her personal data for one or more specified purposes.

'Consent' of the data subject is defined in Article 4.11 of the General Data Protection Regulation as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Furthermore, the following is stated in recital 43 of the General Data Protection Regulation:

> *"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 a 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."*

This means that the assessment of whether consent has been freely given should be based not only on the prevailing freedom of choice, but also on the relationship that exists between the data subject and the controller. The scope for voluntary consent within the public sphere is therefore limited. As regards the school sector, it is clear that the students are in a position of dependence with respect to the school both as regards grades, student grants and loans and education, and therefore also as regards the scope to obtain employment in the future or to continue further education. The processing also often involves children's personal data.

The Swedish government's official report of data in the education sector (*Utbildningsdatautredningen*) concluded that it is still possible for certain processing of personal data to be based on consent, including in the relationship between a child's guardians and a pre-school, or a student's guardian or the students themselves (depending on their age) and a school. Examples of situations where consent might provide a suitable basis for the processing of personal data are prior to the photographing of students with the aim of creating electronic school catalogues and the use of photography to document activities at pre-schools or schools, not least with the aim of reporting such activities to the children's guardians. (SOU 2017:49 *EU:s dataskyddsförordning och utbildningsområdet*, p. 137)

The monitoring of attendance is an obligation incumbent on the school sector which is regulated in administrative law, and the reporting of attendance is of considerable importance for the students. This processing is therefore not comparable with the processing of personal data for the purpose of administering school photography. In the case of attendance monitoring, the students are in a position of dependence which results in a substantial imbalance. The Swedish Data Protection Authority therefore believes that consent cannot constitute a legal basis for the processing operations which this supervision regards.

The processing is necessary in order to perform a task in the public interest

The Board has also stated that the legal basis for the processing of personal data that has taken place within the framework of the facial recognition project comprises the requirement stipulated in the Administrative Procedure Act for effective case administration, the requirement of the Education Act for action to be taken in the event of absence, and the obligation incumbent on secondary schools to report cases of unauthorised absence to the Swedish Board of Student Finance (CSN).

Under Article 6.1(e) of the General Data Protection Regulation, processing will be lawful if it is necessary in order to perform a task in the public interest or as part of the controller's exercising of public authority.

Article 6.2 of the General Data Protection Regulation states, inter alia, that Member States may retain or introduce more specific provisions in order to adapt the transposition of the provisions of the General Data Protection Regulation to comply with paragraph (e) of the same article. Under Article 6.3, a task in the public interest under Article 6.1(e) must be established pursuant to Union or Member State law.

Under Chapter 15 Section 16 first paragraph of the Education Act (2010:800), a student at a secondary school must participate in activities that are organised in order to provide the intended education, unless the student has a valid reason for not doing so.

If a student at a secondary school without valid reason does not participate in an activity that is being organised in order to provide the intended education, the head of the school must ensure that the student's guardian is notified on the day that the student is absent. If there are special reasons, the student's guardian need not be informed on the same day (Chapter 15 Section 16 second paragraph of the Education Act).

The processing of personal data that is normally carried out in order to administer student attendance at the school should be deemed to be necessary due to the head's duties under Chapter 15 Section 16 of the Education Act, and therefore constitutes a task in the public interest under Article 6.1(e) of the General Data Protection Regulation. In certain areas, a legal duty may also exist under Article 6.1(c) of the General Data Protection Regulation.

However, according to the preparatory work for the Data Protection Act (prop. 2017/18:105 *Ny dataskyddslag*, p. 51), the requirements imposed on supplementary national regulations become more stringent as regards precision and predictability in the case of more tangible intrusion. It is also noted that if the intrusion is substantial and entails monitoring or surveillance of an individual's personal circumstances, a separate legal basis will also be required under Chapter 2 Sections 6 and 20 of the Swedish Instrument of Government.

The Swedish Data Protection Authority notes that, while there is a legal basis for administering student attendance at school, there is no explicit legal basis for performing the task through the processing of special categories of personal data or in any other manner which entails a greater invasion of privacy.

Special categories of personal data (Article 9)

The facial recognition that has been used in the case in question has meant that the monitoring of attendance has taken place through the processing of biometric personal data concerning children in order to unambiguously identify them.

Under Article 9.1 of the General Data Protection Regulation, the processing of biometric personal data in order to unambiguously identify a natural person constitutes the processing of special categories of personal data. The general rule is that it is prohibited to process such data. In order to process special categories of personal data, a derogation from the prohibition under Article 9.2 of the General Data Protection Regulation is required.

As stated above, the Board has stated that guardians gave their consent to the processing that the supervision concerns.

Under Article 9.2(a) of the General Data Protection Regulation, the processing of special categories of personal data may be permissible if the data subject has given explicit consent to the processing concerned for one or more specified purposes, except where Union or Member State law provide that the prohibition in paragraph 1 may not be lifted by the data subject.

As explained previously, the relationship between the Board and students will generally be one of considerable imbalance, and the monitoring of attendance is a unilateral control measure where this inequality exists. As stated previously, consent cannot be considered to have been given freely within the framework of the school's activities. Consent can therefore not be used as a basis for a derogation from the prohibition of the processing of special categories of personal data in the case in question.

In its statement, the Board also refers to the provisions of the Administrative Procedure Act regarding effective case administration and those of the Education Act regarding the administration of absence.

It follows from Article 9.2(g) of the General Data Protection Regulation that the prohibition of the processing of special categories of personal data will not apply if the processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

National supplementary provisions concerning the derogation regarding substantial public interest have been introduced in Chapter 3 Section 3 of the Data Protection Act[3].
According to Chapter 3 Section 3 first paragraph 2 of the Data Protection Act, special categories of personal data may be processed under Article 9.2 of the General Data Protection Regulation if it is necessary out of consideration for a substantial public interest and the processing is necessary in order for a case to be processed.

The preparatory work for the Data Protection Act (prop. 2017/18:105 *Ny dataskyddslag*) states, inter alia, the following.

> *"However, it is the government's opinion that, in the overwhelming majority of cases, the term 'case' is relatively clear (see prop. 2016/17:180 p. 23–25 and p. 286). The term is used to delimit the scope of the Administrative Procedure Act and should, in the opinion of the government, therefore apply to the administration of a case. (p. 87)"*

Moreover, the preparatory work for the Administrative Procedure Act (prop. 2016/17:180 *En modern och rättssäker förvaltning - ny förvaltningslag*) states the following:

> *"The term 'administration' encompasses all measures which an authority carries out from the initiation of a case until it is closed. The term 'case' is not defined in the law. However, characteristic of what constitutes a case is that it is regularly closed through a statement from the authority that is intended to have actual implications for a recipient in the case in question. A case is closed through a decision of some kind. In any assessment of the question of whether or not an authority's stance should be considered to constitute a decision in this sense, it is the purpose and content of the statement which determines the nature of the statement, not its outer form (p. 286)."*

The Swedish Data Protection Authority notes that the attendance monitoring which takes place through facial recognition does not constitute a form of case administration, but an actual action. The provision in Chapter 3 Section 3 first paragraph (2) of the Data Protection Act thus does not apply to the processing of personal data that the Board has performed using facial recognition in order to monitor student attendance.

According to Chapter 3 Section 3 first paragraph (1) of the Data Protection Act, special categories of personal data may be processed by a public authority if the data has been disclosed to the authority and the processing is required by law. The following is stated regarding this provision in the preparatory work for the Data Protection Act (prop.2017/18:105 *Ny dataskyddslag*).

---

[3] Certain processing of special categories of personal data by heads of schools is regulated in Chapter 26(a) Section 4 of the Education Act (2010:800), which corresponds to Chapter 3 Section 3 of the Data Protection Act. As this supervision concerns a municipal school and there are no sector-specific provisions concerning the processing of special categories of personal data in this type of school activity, Chapter 3 Section 3 of the Data Protection Act is applicable.

> *"The provision makes it clear that it is permissible for public authorities to process special categories of personal data which forms an essential part of the authorities' activities as a direct result of, above all, the provisions of the Public Access to Information and Secrecy Act and the Administrative Procedure Act concerning the way in which general actions are to be handled, e.g. through requirements concerning record-keeping and an obligation to accept e-mail. The processing of special categories of personal data pursuant to this paragraph may therefore only take place if the data has been disclosed to the public authority. (p. 194)"*

The Swedish Data Protection Authority notes that Chapter 3 Section 3 first paragraph (1) of the Data Protection Act is not relevant to the processing of personal data in question.

Under Chapter 3 Section 3 first paragraph (3) of the Data Protection Act, public authorities may also process special categories of personal data in other cases if the processing is necessary out of consideration for a substantial public interest and does not entail undue infringement of the data subject's personal integrity.

The preparatory work for the Data Protection Act (prop. 2017/18:105 *Ny dataskyddslag*) states, inter alia, the following.

> *"The provision is not intended to be applied routinely during ongoing operations. It is a requirement that the controller in each individual case assesses whether the processing will entail undue infringement of the data subject's personal integrity. If the processing would entail such infringement, it may not take place under this provision. In order to determine whether the infringement is undue, the public authority must carry out a proportionality assessment, where the necessity of performing the processing is weighed against the interest of the data subject in the processing not taking place. The assessment of the data subject's interest in the processing not taking place should be based on the interest of integrity protection which is normally afforded to data subjects. The controller must therefore carry out an assessment in relation to each individual concerned. When assessing infringement of an individual's personal integrity, emphasis should be placed on factors such as the sensitivity of the data, the nature of the processing, the setting that the data subjects can be expected to have towards the processing, the degree to which the data will be disseminated, and the risk of further processing for purposes other than that for which it was collected. This means for example that the provision cannot be used as a basis for collating integrity-sensitive personal data. (p. 194)"*.

Attendance monitoring is an extensive and important task within the school sector and is routinely carried out as part of the day-to-day running of schools. The Swedish Data Protection Authority is therefore of the opinion that Chapter 3 Section 3 first paragraph (3) of the Data Protection Act can be applied to the processing of personal data for the purpose of attendance monitoring. The provision can thus not be applied to the processing that the Board has carried out. Moreover, the Swedish Data Protection Authority believes that the processing in question has resulted in undue infringement of the data subjects' integrity, as the Board has processed special categories of personal data concerning children who are in a position of dependence in relation to the Board for the purpose of attendance monitoring through camera surveillance in the student's everyday environment.

Accordingly, the Swedish Data Protection Authority concludes that the national supplementary provisions concerning the derogation in Article 9.2(g) of the General Data Protection Regulation concerning a *substantial public interest* which have been introduced in Chapter 3 Section 3 first paragraph of the Data Protection Act do not apply to the processing of personal data that is covered by this supervision.

Moreover, it is apparent from Chapter 3 Section 3 second paragraph of the Data Protection Act that it is prohibited to carry out searches with the support of Chapter 3 Section 3 first paragraph with the aim of obtaining a sample of persons based on special categories of personal data. As the purpose of facial recognition is to identify students, the Swedish Data Protection Authority notes that the process of

attendance monitoring presupposes searches based on special categories of personal data. The latter means that the processing covered by this supervision was also in breach of Chapter 3 Section 3 second paragraph of the Data Protection Act.

In summary, the Swedish Data Protection Authority considers that the derogation in Article 9.2(g) of the General Data Protection Regulation does not apply to the processing of personal data in question. As the information that has emerged in the case also precludes the possibility that any of the other derogations in Article 9.2 of the General Data Protection Regulation might apply, the Swedish Data Protection Authority considers that the Board lacked the prerequisites necessary to process biometric personal data in order to unambiguously identify students for attendance monitoring purposes, as has occurred. This processing of personal data therefore took place in breach of Article 9 of the General Data Protection Regulation.

Fundamental principles for the processing of personal data (Article 5)

Under Article 5.2 of the General Data Protection Regulation, the controller is responsible for compliance with the Regulation and must be able to demonstrate that the fundamental principles are being followed.

Under Article 5 of the General Data Protection Regulation, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitations). Furthermore, personal data that is processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation). It follows from recital 39 that personal data may only be processed if the purpose of the processing cannot be achieved in a satisfactory manner using other methods.

As regards the question of how the Board carried out the proportionality assessment concerning the processing in question, the Board gave the following response in its statement which was received on 15 March 2019.

> *"Secure identification is important in order to know which students are present and to fulfil the requirement stipulated in the Education Act to take action when students have high levels of absence. The method used for facial recognition is considered to be necessary in order to verify that attendance is being correctly registered. The facial recognition method also offers a marked improvement in quality compared to the manual method that was previously used, where, when investigated, deficiencies have been found where the processing has been incorrect. Of the various methods that were tested, facial recognition is considered to be the method which best meets the requirements imposed by both the legislation and the purpose of the project."*

The Swedish Data Protection Authority has previously stated that the processing that this supervision concerns has resulted in the processing of special categories of personal data concerning children who are in a position of dependence in relation to the Board, and that this processing has involved the use of camera surveillance in the students' everyday environment. The Swedish Data Protection Authority believes that this processing has resulted in a substantial infringement of the students' integrity, even if it only concerns a relatively small number of students and a relatively limited period of time.

The Board has stated that the purpose of this processing was to monitor attendance. Attendance monitoring can be carried out in other ways which involve less infringement of the students' integrity. The Swedish Data Protection Authority therefore considers that the method of using facial recognition via a camera for attendance monitoring was disproportionate and carried out in a manner that excessively infringed on personal integrity, and was therefore disproportionate in relation to the purpose. The processing carried out by the Board was therefore in breach of Article 5 of the General Data Protection Regulation.

Impact assessment and prior consultation (Article 35, 36)

Under Article 35, the controller must carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, particularly if the processing uses new technologies, and, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.

As regards the question of whether the Board carried out an impact assessment purpose to Article 35 prior to commencement of the project in question, the Board referred in its response, which was received on 15 March 2019, to a risk assessment that had been carried out. The following can be read in the assessment.

> *"Facial recognition is undoubtedly biometric data, and under the General Data Protection Regulation constitutes special categories of personal data which necessitates specific decisions in order to be used. However, although the data is sensitive, it is not secret. The parents of the students also give their consent to the processing of the personal data and there is a legal basis for the processing in both the Administrative Procedure Act and the Education Act. The requirements described by the supplier concerning the processing of the special categories of data, such as the requirement for there to be no internet connection on the equipment that is used to process the data, that only authorised personnel must be given access to the personal data, that only data concerning the target group must be processed, and that the data must be erased at the end of the trial period, means that the processing is considered to fall within the framework of the General Data Protection Regulation. Overall, no specific risk assessment is required in order to process special categories of personal data, but the Board must approve the processing of biometric data in its register list and a reason for using the data must be entered. The school's head of administration is authorised to take decisions concerning approval of the processing of personal data, and special categories of personal data in particular. (p. 4)".*

In its response, the Board referred to the appendix entitled *Skellefteå kommun – Framtidens klassrum* (Skellefteå municipality – The classroom of the future). In the appendix (p. 5), it is stated that one advantage of facial recognition is that it is easy to register a large group such as a class in bulk. The disadvantages mentioned include that it is a technically advanced solution which requires a relatively large number of images of each individual, that the camera must have a free line of sight to all students who are present, and that any headdress/shawls may cause the identification process to fail.

Under Article 35.7 of the General Data Protection Regulation, at least the following factors must be taken into account in any impact assessment. A systematic description of the envisaged processing operations and the purposes of the processing, an assessment of the necessity and proportionality of the processing in relation to the purposes, an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1, and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

The Swedish Data Protection Authority recognises that the Board has conducted a risk assessment. This risk assessment concludes that the cited legal basis and the security measures that have been implemented for the processing means that no specific risk assessment is necessary regarding the personal data.

In the opinion of the Swedish Data Protection Authority, the processing operations concerned encompassed a number of factors which indicate that an impact assessment pursuant to Article 35 should have been carried out before the processing operations were commenced. The processing operations were carried out using camera surveillance, which is a systematic method of surveillance, and the operations covered special categories of personal data concerning children in an environment

where they are in a position of dependence. Furthermore, facial recognition is also a new technology. The requirement for an impact assessment pursuant to Article 35 can therefore be imposed on the assessments that preceded the use concerned.

The Swedish Data Protection Authority considers that the risk assessment that was carried out by the Board lacks any assessment of the risks to the rights and freedoms of the data subjects, or an account of the proportionality of the processing in relation to its purposes; hence the requirements of Article 35 cannot be deemed to be fulfilled.

According to Article 36 of the General Data Protection Regulation, the controller must consult the supervisory authority if an impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

Based on the information that has emerged in the case, it is apparent that the Board did not submit a prior consultation to the Swedish Data Protection Authority. The Authority considers that a number of factors indicated that the processing operations posed a high risk to the rights and freedoms of the individuals concerned. For example, the processing operations involved the use of new technology which concerns special categories of personal data relating to children who are in a position of dependence with respect to the Board. The processing operations involved camera surveillance in the students' everyday environment. As the risk assessment submitted by the Board does not include an assessment of relevant risks to the rights and freedoms of the data subjects associated with the processing operations, the Board has not demonstrated that the high risk pursuant to Article 36 has been reduced. The Swedish Data Protection Authority therefore concludes that the processing operations in question here should have led to a prior consultation with the Swedish Data Protection Authority pursuant to Article 36 before the processing was commenced. The processing operations were therefore carried out in breach of Article 36.

Permit under the Camera Surveillance Act

The Camera Surveillance Act contains national provisions regarding camera surveillance which, pursuant to Section 1, supplement the General Data Protection Regulation. According to Section 2 of the Camera Surveillance Act, the purpose of the Act is to satisfy the need for camera surveillance for legitimate purposes and to protect natural persons from undue infringement of their personal integrity as a result of such surveillance.

Amongst other things, the definition of camera surveillance in Section 3 of the Camera Surveillance means that the equipment in question must be used in a way which results in the prolonged or repetitive surveillance of persons.

According to Section 7 of the Camera Surveillance Act, a permit is required in order for public authorities to use camera surveillance in areas to which the public has access.

The Swedish Data Protection Authority notes that the Board did indeed use prolonged and repetitive surveillance of persons involving the use of facial recognition technology in connection with its project for monitoring attendance over a three-week period.

The Board is a public authority and will therefore normally be required to have a permit to use camera surveillance in places to which the public has access. The question is therefore whether the public is considered to have access to where the Board used camera surveillance using facial recognition technology in connection with the monitoring of student attendance. According to case law, the term "place to which the public have access" must be interpreted broadly (see the Supreme Administrative Court's judgement RÅ 2000 ref. 52).

Schools are not normally considered to be places to which the public has access, although there are certain areas in schools to which the public are considered to have access. Examples of such areas

include main entrances and corridors which lead to the head's office. The investigation indicated that the students were registered using facial recognition on each occasion they entered a classroom. A classroom is not considered to be a place to which the public has access.

Based on the information that has emerged concerning the place where the surveillance took place, the Swedish Data Protection Authority has concluded that it is not a place to which the public has access. There is therefore no requirement to apply for a permit. However, the fact that the camera surveillance does not require a permit need not mean that the surveillance is permissible. If camera surveillance involves the processing of personal data, the data protection regulations must be followed, including the obligation to provide clear information concerning the camera surveillance.

Risk of the provisions being infringed in the event of planned further processing

Based on the information that has emerged in the case, the Board has been considering processing personal data through facial recognition in order to monitor student attendance again in the future. In the foregoing, the Swedish Data Protection Authority has concluded that the processing operations carried out by the Board were in breach of Articles 5 and 9 of the General Data Protection Regulation. The Swedish Data Protection Authority therefore notes that the Board risks breaching the aforementioned provisions again through the planned processing operations.

Choice of intervention

Article 58 of the General Data Protection Regulation sets out all the powers that the Swedish Data Protection Authority has at its disposal. According to Article 58.2, the Swedish Data Protection Authority has a number of corrective powers, including warnings, reprimands and restrictions on processing.

According to Article 58.2(i) of the General Data Protection Regulation, the supervisory authority shall impose administrative fines pursuant to Article 83. Under Article 83.2, administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in Article 58.2 (a)–(h) and (j). Moreover, Article 83.2(n) sets out the factors that must be taken into account in connection with decisions as to whether administrative fines should be imposed at all and concerning the amount of the fine.

Instead of fines, under recital 148 of the General Data Protection Regulation, a reprimand may be issued instead of fines in some cases when the breach is minor in nature. However, consideration must be given to the circumstances, such as the nature, gravity and duration of the breach.

As regards public authorities, Article 83.7 provides for the introduction of national supplementary provisions concerning administrative fines. According to Chapter 6 Section 2 of the Data Protection Act, the supervisory authority may impose a fine on a public authority for infringements referred to in Articles 83.4, 83.5 and 83.6 of the General Data Protection Regulation. Articles 83.1, 83.2 and 83.3 of the Regulation must then be applied.

Fine

In the foregoing, the Swedish Data Protection Authority has concluded that, in the processing operations concerned, the Board breached Article 5, Article 9, Article 35 and Article 36 of the General Data Protection Regulation. These articles are covered by Articles 83.4 and 83.5, and in the event of a breach of these articles, the supervisory authority shall consider imposing an administrative fine in addition to, or instead of, other corrective measures.

Given that the processing operations that this supervision concerns entailed the processing of special categories of personal data concerning children who are in a position of dependence in relation to the Board, and that these processing operations involved the use of camera surveillance in the students'

everyday environment, the infringement is not minor in nature. There is therefore no reason to replace the fine with a reprimand. No corrective measures would be appropriate for the processing that has taken place either. Administrative fines must therefore be imposed on the Board.

The magnitude of the administrative fine

According to Article 83.1 of the General Data Protection Regulation, each supervisory authority must ensure that the imposition of administrative fines is effective, proportionate and dissuasive in each individual case.

According to Article 83.3, administrative fines may not exceed the amount specified for the gravest infringement for the same or linked processing operations.

Regarding public authorities, Chapter 6 Section 2 second paragraph of the Data Protection Act states that fines that are imposed must not exceed SEK 5,000,000 in the case of infringements referred to in Article 83.4 of the General Data Protection Regulation, or SEK 10,000,000 in the case of infringements referred to in Article 83.5 and 83.6. Infringements of Articles 5 and 9 are covered by the higher fine under Article 83.5, whilst infringements of Articles 35 and 36 are covered by the lower maximum amount under Article 83.4. This case concerns the same processing operations and the fine must therefore not exceed SEK 10 million.

Article 83.2 of the General Data Protection Regulation sets out all the factors that must be taken into account when determining the magnitude of the fine. When deciding on a fine, consideration must be given to, inter alia, Article 83.2(a) (the infringement's nature, gravity and duration), (b) (intentional or negligent character), (g) (categories of personal data), (h) (the manner in which the infringement became known to the Swedish Data Protection Authority), and (k) (any other aggravating or mitigating factors, such as financial benefits gained, directly or indirectly) of the General Data Protection Regulation.

In the Swedish Data Protection Authority's assessment, consideration was given to the fact that the case involves the infringement of several articles of the General Data Protection Regulation, with the infringement of Articles 5 and 9 being considered to be more serious and covered by the higher fine. Furthermore, consideration was also given to the fact that the infringement involves special categories of personal data concerning children who were in a position of dependence in relation to the Board. The processing operations were intended to improve the effectiveness of the activity and the processing was therefore carried out intentionally. These circumstances constitute aggravating factors.

Consideration was also given to the fact that the processing became known to the Swedish Data Protection Authority via information in the media.

As mitigating circumstances, consideration was given to the fact that the processing took place during a limited period of three weeks and only concerned 22 students.

Based on an overall assessment, the Swedish Data Protection Authority has decided that the Secondary Education Board in Skellefteå municipality must pay an administrative fine of SEK 200,000.

Warning

According to Article 58.2(a), the Swedish Data Protection Authority has the power to issue a warning to controllers or processors' representatives that intended processing operations are likely to infringe the provisions of the Regulation.

The Secondary Education Board of Skellefteå municipality has stated that it intends to continue using facial recognition to monitor student attendance. These processing operations will similarly breach the provisions of the General Data Protection Regulation. Because of the risk of future infringements in

connection with planned processing operations, a warning is now being issued pursuant to Article 58.2(a) of the General Data Protection Regulation.

This decision was taken by Director General Lena Lindgren Schelin following a presentation by lawyers Ranja Bunni and Jenny Bård. Chief Legal Office Hans-Olof Lindblom and Heads of Unit Katarina Tullstedt and Charlotte Waller Dahlberg and lawyer Jeanette Bladh Gustafson took part in the concluding administrative process.

Lena Lindgren Schelin, 20.08.2019 (This is an electronic signature)