Decision

Diary no

2019-08-20

DI-2019-2221

Skellefteå Municipality, High School Board

Supervision according to the EU data protection regulation

2016/679 – facial recognition for

attendance control of students

Content

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Telephone: 08-657 61 00

The Swedish Data Protection Authority's decision

The Data Inspectorate states that the upper secondary school board in Skellefteå municipality

by using facial recognition via camera for presence control of

students have processed personal data in violation of

- Article 5 of the Data Protection Regulation1 by processing students'

personal data on a for the personal integrity more intervention

way and included more personal data than is necessary for

the stated purpose (presence control),

- Article 9 by having processed sensitive personal data

(biometric data) without having a valid one for the treatment

exemption from the prohibition to process sensitive personal data and

- articles 35 and 36 by not having met the requirements of a

impact assessment and not have come in with one

prior consultation with the Swedish Data Protection Authority.

The Data Inspection Authority decides with the support of ch. 6. Section 2 of the Data Protection Act2 and

articles 58.2 and 83 of the data protection regulation that the Gymnasienämnden i

Skellefteå municipality must pay an administrative sanction fee of 200,000

crowns.

The Data Inspectorate notes that the High School Board in Skellefteå municipality

likely to breach Articles 5 and 9 if continued use of

facial recognition for presence control.

The Swedish Data Protection Authority therefore decides to give the High School Board in Skellefteå

municipality a warning according to article 58.2 a of the data protection regulation.

Account of the supervisory matter

Through information in the media, the Swedish Data Protection Authority has drawn attention to the fact that

The high school board in Skellefteå municipality (below the high school board) in one

trial project at Anderstorp's high school in Skellefteå has used

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 that

free flow of such data and on the repeal of Directive 95/46/EC (general

data protection regulation).

2 The Act (2018:218) with supplementary provisions to the EU's data protection regulation

facial recognition to register students' presence in a class for some time

weeks.

The purpose of the inspection has been to review the high school board's performance

processing of personal data through facial recognition for

attendance control has been in accordance with data protection regulations.

The Swedish Data Protection Authority has reviewed the personal data processing which the high school board has carried out in the current project and also taken attitude to possible future treatments. The Swedish Data Protection Authority has within the framework of this supervision did not carry out any examination regarding safety or the duty to provide information in connection with the treatments in question.

The review has revealed that the upper secondary school board has for three weeks processed personal data through facial recognition to check the presence of 22 high school students and that the high school board is considering that in the future process personal data through the use of facial recognition for attendance control. The aim has been to in a simpler and more effective way register attendance at classes in secondary school. To register attendance at a traditional way takes, according to the high school board, 10 minutes per lesson and by using facial recognition technology for presence control it would according to the board, save 17,280 hours per year at the school in question.

The secondary school board has stated that the facial recognition has been carried out in that the students were filmed by a camera when they entered a classroom. Images from the camera surveillance have been compared with those registered in advance pictures of each participating student's face. The information that has been registered is biometric data in the form of facial images and first and last names. The data has been stored on a local computer without an internet connection that has been stored in a locked cabinet. Express consents have been obtained from guardians and it has been possible to waive the registration of personal data with biometric data.

The supervisory case was initiated with a supervisory letter on 19 February 2019. Response to the supervisory letter was received on March 15, 2019, with annexes completed on April 2, 2019. Later additions from the high school board came in on the 16th

Justification of decisions

Personal data responsibility

The high school board has stated that the board is responsible for personal data for them personal data processing that has taken place within the framework of the project with facial recognition for attendance control at Anderstorp gymnasium i Skellefteå municipality. The Swedish Data Protection Authority shares this view.

Pilot project

The current personal data processing has taken place within the framework of a pilot project. The Swedish Data Protection Authority notes that the data protection regulation does not contain any exemptions for pilot or experimental activities.

The regulation's requirements therefore also need to be met in order to implement them types of operations.

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

Article 6 of the Data Protection Regulation states that processing is only lawful if one of the conditions specified in the article is met.

Consent as a legal basis

The High School Board has in its opinion that came to the Data Inspection Authority that 15 March 2019 p. a. indicated that consent has been given to the treatment that has took place within the framework of attendance management.

In the opinion of the high school board, it is stated, among other things, a. the following.

"I.e. the students' guardians receive information about the project's purpose and which personal data processing will take place and may have its say

explicit and voluntary consent for the processing of personal data.

Students who do not want to participate do not have to participate, attendance is then checked according to previous procedures. Students also receive information that when they preferably can withdraw their consent to the processing of personal data.

(p. 6).”

Article 6.1 a of the data protection regulation states that a processing of personal data is legal if the data subject has provided his consent to his personal data being processed for one or more specific purposes purpose.

Consent by the data subject is defined in Article 4.11 of the Data Protection Regulation such as any kind of voluntary, specific, informed and unambiguous expression of will, by which it registered, either by a statement or by a unambiguous confirmation document, accepts the processing of personal data relating to him or her.

In recital 43 of the data protection regulation, the following is further stated.

“To ensure that consent is given voluntarily, it should not constitute valid legal basis for processing personal data in a particular case where there is significant inequality between the data subject and the personal data controller, especially if the personal data controller is a public authority and it is therefore unlikely that the consent has provided voluntarily in relation to all conditions such as this particular one situation includes.”

This means that the assessment of a consent has been given voluntarily not only

must take place based on what freedom of choice prevails, but also what relationship exists between the registered and the personal data controller.

The space for voluntary consent in the public domain is therefore limited. Within the school area, it is clear that the student is in a dependent position to the school in terms of grades, study funds, education and thus the opportunity to future work or further studies. It is also often a matter of children.

The education data survey made the assessment that it is still possible to for certain personal data processing use consent also in the relationship between a child's guardian and a preschool and a student's guardian or the student himself, depending on age and a school. An example on when consent could be the appropriate basis for personal data processing is for photographing the students for the purpose of creating electronic school catalogs or photography to document activities in preschool and school, not least in order to be able to account for the one for the children's guardians. (SOU 2017:49 EU data protection regulation and the field of education p. 137)

The attendance check is an obligation regulated by public law school activities and attendance reporting are of significant importance to

the student. This treatment is therefore not comparable to it personal data processing that may take place to administer school photography.

During attendance control, the student is in such a dependent position that it prevails significant inequality. The Swedish Data Protection Authority therefore assesses that consent does not may constitute a legal basis for the processing of personal data such as this

supervision includes.

The processing is necessary to perform a task of public interest

The High School Board has also stated that the legal basis for the

personal data processing that has taken place within the framework of the project with

facial recognition is the administrative act's requirement for efficient case management,

The School Act's requirements for measures in case of absence and the obligation for

upper secondary schools to report invalid absences to Centrala

the study funds board (CSN).

According to Article 6.1 e of the Data Protection Regulation, processing is legal if it is

necessary to perform a task of public interest or as part of it

personal data controller's exercise of authority.

Article 6.2 of the data protection regulation states, among other things, that member states may retain or introduce more

specific provisions to adapt

the application of the provisions of the data protection regulation in order to comply

point e of the same article. According to Article 6.3, the information must be of public interest

according to Article 6.1 e be established in accordance with Union or national law

Right.

According to ch. 15 Section 16 first paragraph of the School Act (2010:800) a student must i

secondary school participate in the activities organized to provide the intended

the education, if the student does not have a valid reason for being absent.

If a student in the upper secondary school is absent from that activity without a valid reason

which is organized to provide the intended education, the principal must ensure that

the student's guardian on the same day is informed that the student has been

absent. If there are special reasons, the student's guardian does not have to

are informed on the same day (chapter 15, section 16, second paragraph of the School Act).

The personal data processing that usually takes place to administer student data

attendance at school should be considered necessary because of the principals' task

according to ch. 15 Section 16 of the School Act and thus constitutes a task of general interest

according to article 6.1 e of the data protection regulation. In some parts it can

there is a legal obligation according to Article 6.1 c of the data protection regulation.

According to the preparatory work for the Data Protection Act (prop. 2017/18:105 New Data Protection Act s.

51) however, increases the requirements for the supplementary national regulation

regarding precision and predictability when it comes to a more tangible

infringement. It is also stated that if the infringement is significant and involves

monitoring or mapping of the individual's personal circumstances is required

in addition, special statutory support according to ch. 2 §§ 6 and 20 the form of government.

The Swedish Data Protection Authority can state that there is a legal basis for

administer students' attendance at school, but that there is an express lack

team support to carry out the task through the treatment of sensitive

personal data or in other more privacy-infringing ways.

Sensitive personal data (Article 9)

The facial recognition that has taken place in the current case has meant that

the attendance control has taken place by biometric personal information about children

have been processed to uniquely identify these.

According to Article 9.1 of the Data Protection Regulation, a processing of

biometric personal data to uniquely identify a natural person a

processing of special categories of personal data (so-called sensitive

personal data). The starting point is that it is forbidden to treat such

tasks. In order to process sensitive personal data, it is required that a

exemption from the prohibition according to Article 9.2 of the data protection regulation is relevant.

As stated above, the high school board has meant that consent from

the guardians have been given in connection with the current treatments which

the supervision refers.

According to Article 9.2 a of the data protection regulation, processing of sensitive

personal data be permitted if the data subject has expressly provided his

consent to the processing of this personal data for one or more

specific purposes, except then Union law or Member States' national law

law stipulates that the prohibition in paragraph 1 cannot be revoked by the data subject.

As previously reported, there is generally a significant inequality

relationship between the high school board and the students and attendance control is one

unilateral control measure where this inequality prevails. Consent therefore cannot,

as previously established, is considered to be voluntarily provided within the framework of

school activities. Consent is therefore not possible to apply as an exception

from the ban on processing sensitive personal data in the current case.

The High School Board also refers in its opinion to the Administrative Law's rules on

efficient case management and the School Act's rules on handling absences.

It follows from Article 9.2 g of the data protection regulation that the prohibition against processing

sensitive personal data does not apply if the processing is necessary for consideration

to an important public interest, on the basis of Union law or

the national law of the Member States, which must be proportionate to it

pursued purpose, be consistent with the essential content of the right to

data protection and contain provisions on appropriate and specific measures for

to ensure the data subject's fundamental rights and interests.

National supplementary provisions regarding the exception if important

general interest has a. introduced in ch. 3 Section 3 of the Data Protection Act.3

According to ch. 3 Section 3 first paragraph 2 of the Data Protection Act appears to be sensitive

personal data may be processed with the support of Article 9.2 g of the data protection regulation if it is necessary due to an

important public interest

and the processing is necessary for the processing of a case.

In the preliminary works (prop. 2017/18:105 New Data Protection Act) it is stated, among other things, a. the following.

"However, the government's view is that the concept of case in the vast majority of cases

is relatively clear (see prop. 2016/17:180 p. 23–25 and p. 286).

The term is used as a delimitation for the Administrative Law

scope of application and should, in the government's opinion, also be used

3

Individual school principals' processing of sensitive personal data has

regulated in ch. 26 a. Section 4 of the School Act (2010:800) which corresponds to ch. 3 Section 3

the data protection act. As this supervision concerns a municipal school and it is missing

sector-specific regulations regarding the treatment of sensitive

personal data in this type of school activity is ch. 3. Section 3 of the Data Protection Act

applicable.

here. The provision should thus be applicable when handling a

matter. (p. 87)”

Furthermore, the following is evident from the preparatory work for the Administration Act

(prop. 2016/17:180 A modern and legal administration - new administration act).

"The term handling includes all measures taken by an authority

takes place from the time a case is initiated until it is closed. The expression

matter is not defined in the law. Characteristic of what constitutes one

matter is, however, that it is regularly concluded by a statement from

the side of the authority which is intended to have actual effects for one

recipient in the individual case. A case is closed by a decision of

some kind. In assessing the question of whether an authority's

taking a stand is to be considered a decision in this sense it is

the purpose and content of the statement that determine the character of the statement, not its

external form (p. 286).”

The Swedish Data Protection Authority states that the presence control that takes place through

facial recognition does not constitute case management without it being a question

about an actual transaction. The provision in ch. 3 Section 3 first paragraph 2

The Data Protection Act is therefore not applicable to the processing of personal data

which the upper secondary school board has carried out in connection with facial recognition for

attendance control of students.

Of 3 ch. Section 3 first paragraph 1 of the Data Protection Act appears to be sensitive

personal data may be processed by an authority if the data has been provided

to the authority and the processing is required by law. Regarding this one

provision appears, among other things, a. the following of the preliminary works (prop. 2017/18:105 Ny

data protection law).

"The provision makes it clear that it is permissible for authorities to carry out

such processing of sensitive personal data as required in

the authorities' activities as a direct consequence of above all

the provisions of the Publicity and Secrecy Act and the Administration Act

about how public documents are to be handled, for example by requiring

personal data with the support of this point may only be about the data

has been submitted to the authority. (p. 194)”

The Swedish Data Protection Authority states that ch. 3 Section 3 first paragraph 1 of the Data Protection Act

is not relevant to the current processing of personal data.

According to ch. 3 Section 3 first paragraph 3 of the Data Protection Act allows authorities in other areas as well

case process sensitive personal data if the processing is necessary with

consideration of an important public interest and does not constitute an undue intrusion into

the personal integrity of the data subject.

In the preliminary works (prop. 2017/18:105 New Data Protection Act) it is stated, among other things, a. the following.

“The provision is not intended to be applied casually in it

ongoing operations. It is required that the personal data controller, in that

individual case, make an assessment of whether the treatment involves a

undue intrusion into the data subject's personal privacy. If

the processing would involve such an infringement, it must not take place according to

this provision. To determine whether the infringement is improper must

the authority make a proportionality assessment where the need to

carrying out the processing is weighted against the interest of the data subjects in that

the treatment does not take place. The assessment of the interest of the data subjects to

the processing does not take place should be based on the interest in privacy protection which

the registrants typically have. The personal data controller must

thus not making an assessment in relation to each affected individual. At

the assessment of the intrusion into the individual's personal privacy shall be weighted

be added to e.g. the sensitivity of the data, the nature of the processing, the

attitude the data subjects can be assumed to have towards the processing, the dissemination

the data may receive and the risk of further processing for others

purpose than the collection purpose. This means e.g. that the provision

cannot be used as a basis for creating privacy sensitive

compilations of sensitive personal data. (p. 194)".

Attendance management is an extensive and central task in the school system and

takes place casually in the day-to-day operations. The Swedish Data Protection Authority

therefore assesses that ch. 3 Section 3 first paragraph 3 of the Data Protection Act cannot

applied to the personal data processing that takes place for attendance management.

The provision cannot therefore be applied to the processing of personal data

which the upper secondary school board has carried out. In addition, the Swedish Data Protection Authority believes that they

the current processing of personal data has involved an improper intrusion into

they were recorded privacy when the high school board through camera surveillance in

the students' everyday environment has processed sensitive personal data concerning

children who are in a dependent position in relation to

the upper secondary school board for the purpose of attendance management.

Against this background, the Swedish Data Protection Authority finds that the national

supplementary provisions regarding the exception in 9.2 g i

the data protection regulation on important public interest, which has been introduced in ch. 3. 3

§ first paragraph of the Data Protection Act does not apply to them

personal data processing covered by this supervision.

In addition, it appears from ch. 3. Section 3 second paragraph of the Data Protection Act that it is

prohibited to carry out searches that take place with the support of ch. 3 Section 3 first paragraph i

purpose of obtaining a selection of people based on sensitive personal data.

Since the purpose of face recognition is to identify students, can

The Swedish Data Protection Authority states that the presence control requires searches

based on sensitive personal data. The latter means that the current

the treatments covered by this supervision have also been in violation of 3

Cape. Section 3, second paragraph of the Data Protection Act.

In summary, the Data Inspectorate assesses that the exception in 9.2 g i

the data protection regulation is not applicable to the current processing of

personal data. Because what has emerged in the case does not either

means that any other of the other exceptions in Article 9.2 i

the data protection regulation may become relevant, the Data Inspectorate believes that

the upper secondary school board has lacked the conditions to process biometrics

personal data to uniquely identify students for attendance management such as

has been. This processing of personal data has therefore taken place in violation of

Article 9 of the Data Protection Regulation.

Basic principles for processing personal data (Article 5)

It can be stated that the personal data controller according to Article 5.2

data protection regulation is responsible for compliance with the regulation and must

be able to demonstrate that the basic principles are followed.

Article 5 of the data protection regulation states, among other things, a. that the personal data shall

are collected for specific, explicitly stated and legitimate purposes and not

later processed in a way that is incompatible with these purposes

(purpose limitation). In addition, personal data processed must be

adequate, relevant and not too extensive in relation to the purposes for

which they are processed (task minimization). It follows from reason 39 that personal data

may only be processed if the purpose of the processing cannot be achieved at once

satisfactorily with other methods.

When asked how the upper secondary school board has made the proportionality assessment

regarding the personal data processing in question, the board has submitted

the following response in its opinion received on March 15, 2019.

"It is important to have a secure identification to know who the students are

present and meet the requirements found in the School Act in order to take action then

students have high absenteeism. The face recognition method is assessed

needed to know for sure that attendance is recorded correctly.

The facial recognition is also a clear improvement in quality compared to

the previous manual handling which was found to have deficiencies during inspection

in such a way that it is not always correct. Of the various alternative methods

that were tested, facial recognition was judged to be the best method

corresponds to the requirements both from the legislation and from the purpose of the project."

The Swedish Data Protection Authority has previously stated that the personal data processing

which this supervision covers has involved the treatment of sensitive

personal data concerning children who are in a dependent position i

relationship with the upper secondary school board and that these treatments have taken place

through camera surveillance in the students' everyday environment. The Swedish Data Protection Authority

considers that these treatments – even if it is a matter of relatively few

students and a relatively limited period of time – has meant a large

breach of student privacy.

The high school board has stated that the purpose of these treatments has been

attendance control. Attendance control can take place in other ways that are smaller

violating the privacy of the students. The Swedish Data Protection Authority therefore considers that

the method, of using facial recognition via camera for presence control, has

been too extensive and carried out for one for the personal integrity too

intrusive way and thereby been disproportionate in relation to

the purpose. The high school board's proceedings have thus been carried out in conflict

with Article 5 of the Data Protection Regulation.

Impact assessment and prior consultation (Articles 35, 36)

According to Article 35, a personal data controller must make an assessment of a

consequences of planned processing for the protection of personal data, in particular

if a treatment is to be carried out using new technology and taking into account its nature,

scope, context and purpose likely lead to a high risk of

rights and freedoms of natural persons.

On the question of whether the upper secondary school board has made a consequence assessment according to

article 35 before the start of the project in question has the upper secondary school board in its

response received on 15 March 2019 referred to a performed risk assessment.

The following is evident from the assessment made.

"Face recognition is admittedly biometric data and according to

data protection regulation sensitive personal data, which requires special

decision to be handled. However, the information is not confidential either

if they are sensitive. The students' guardians also give their consent to

the processing of the personal data and there is legal support for

the treatment both in the Administration Act and in the School Act. The handling

as described by the provider for handling the sensitive data

such as that there is no network connection of the handling equipment

the information that only authorized personnel have access to

the personal data that only the target group is handled, that those who

is registered gives his consent and that the data will be deleted after

the test period means that the handling is judged to be within the scope of

data protection regulation. Overall, no special is required

risk assessment for handling sensitive personal data without that which

is needed is that the upper secondary school board approves in its register list

the handling of biometric data and also that a

reason for using the data. Head of Administration for

the high school office has delegation to make decisions on approval of

handling of personal data and also sensitive personal data. (p. 4)".

In its response, the board has also referred to the appendix "Skellefteå municipality -

The classroom of the future". In the appendix (p. 5) it is stated that an advantage with

facial recognition is that it is easy to mass register a large group

as a class. The disadvantages are said to be that it is technically advanced

solution that requires relatively many images of each individual as well as the camera

must have a clear view of all students present and that any headgear/shawl

may cause identification to fail.

Article 35.7 of the data protection regulation states that at least the following must

is taken up in an impact assessment. A systematic description of it

planned treatment and the purposes of the treatment, an assessment of the need

of and the proportionality of the processing in relation to the purposes, a
assessment of the risks for the rights and freedoms of the data subjects referred to in
paragraph 1, and the measures planned to manage the risks, including
safeguards, security measures and routines to ensure the protection of
the personal data and to demonstrate compliance with this regulation, with consideration
to the rights and entitlements of the data subjects and other affected persons
interests.

The Swedish Data Protection Authority states that the upper secondary school board has made a
risk assessment. In the risk assessment, the conclusion has been drawn that the legal support
one refers to and the security the processing is covered by means that no one
special risk assessment needs to be done regarding the sensitive
the personal data.

According to the Danish Data Protection Authority's assessment, the current treatments have
included a number of factors that suggest that an impact assessment according to
article 35 would have been done before the treatments began. The treatments have
happened with camera surveillance which is a systematic surveillance and they have
covered sensitive personal data about children in an environment in which they are located
dependency status. Facial recognition is also a new technology. Requirement for one
impact assessment according to Article 35 can therefore be placed on those assessments
that preceded the current use.

The Swedish Data Protection Authority assesses that the risk assessment of the upper secondary school board has
accounted for lacks an assessment of the risks that exist for them
data subject's rights and freedoms as well as an account of
the proportionality of the processing in relation to its purposes and therefore the requirements
in Article 35 cannot be considered fulfilled.

According to Article 36 of the Data Protection Regulation, a personal data controller must

consult with the supervisory authority about an impact assessment regarding

data protection according to Article 35 shows that the processing would lead to a high risk

unless the controller takes measures to reduce the risk.

Based on what has emerged in the case, the high school board has not

submitted with a prior consultation to the Data Inspectorate. The inspection

assesses that there have been a number of factors that cause it to be high

risk to the rights and freedoms of individuals with the treatments. For example

these treatments include new technology relating to sensitive personal data

concerning children who are dependent on the upper secondary school board

and that these treatments have taken place through camera surveillance in the students' rooms

everyday environment. Because the risk assessment the high school board has left

in lacks an assessment of current risks for the rights of the data subjects and

liberties with the treatments, the high school board has also not been able to show

that the high risk according to Article 36 has been lowered. The Swedish Data Protection Authority states

because the current treatments should have caused one

prior consultation with the Data Protection Authority according to Article 36 before processing

was initiated. The processing has thus also taken place in violation of Article 36.

Permission according to the Camera Surveillance Act

The Camera Surveillance Act contains national regulations regarding camera surveillance which, according to § 1, supplement

the Data Protection Ordinance. Of § 2

the camera surveillance act states that the purpose of the act is to meet the need

of camera surveillance for legitimate purposes and to protect natural persons

against undue intrusion into personal integrity during such monitoring.

The definition of camera surveillance in Section 3 of the Camera Surveillance Act means among other things, that it must be a question of equipment that is used on such means that involve long-term or regularly repeated personal surveillance.

According to Section 7 of the Camera Surveillance Act, permission is required for camera surveillance by a place to which the public has access, if the surveillance is to be carried out by one authority.

The Swedish Data Protection Authority notes that it was a question of lasting and regular repeated personal surveillance when the upper secondary school board used camera surveillance with facial recognition technology in connection with its attendance control project over a three-week period.

The high school board is an authority and must therefore have as its starting point permit for camera surveillance of a place to which the public has access. The question is then if the public is considered to have access to the place that the high school board

camera surveillance through the use of facial recognition technology i connection with attendance registration of students. From practice it appears that the concept "place to which the public has access" shall be interpreted broadly (see Högsta the administrative court's decision RÅ 2000 ref. 52).

In general, a school is considered a place where the public does not have access, however, there are certain areas of a school where the public is considered to have access. Examples of such areas are main entrances and corridors such as leads up to the rector's office. The investigation shows that the students were registered using facial recognition every time they entered one classroom. A classroom is not to be considered a place where the public has

access.

In the light of what has emerged about the location of the surveillance assesses

Datainspektionen that it is not a question of a place where the public has

access. There is therefore no requirement to apply for a permit. To

the camera surveillance is permit-free, however, does not necessarily mean that it is a

permitted surveillance. If camera surveillance includes

personal data processing, the data protection rules must be followed, e.g. the obligation to

clearly inform about the camera surveillance.

Risk that the regulations are violated in the event of planned continued treatment

Based on what has emerged in the case, the high school board has considered

to process personal data again in the future through facial recognition

for attendance control of students. The Swedish Data Protection Authority has found above that

the high school board's treatment has been in violation of articles 5 and 9

data protection regulation. The Swedish Data Protection Authority therefore notes that

the high school board runs the risk of breaching the aforementioned regulations even when

planned treatments.

Choice of intervention

In article 58 of the data protection regulation, all powers are specified as

The Swedish Data Protection Authority has According to Article 58.2, the Data Inspectorate has a number

corrective powers, i.a. a. warnings, reprimands or restrictions

of treatment.

According to Article 58.2 (i) of the data protection regulation, it appears that

the supervisory authority shall impose administrative penalty fees in accordance

with Article 83. According to Article 83.2, administrative penalty fees,
depending on the circumstances of the individual case, imposed in addition to or in
instead of the measures referred to in article 58.2 a–h and j. Furthermore, it appears from
article 83.2 n which factors must be taken into account when deciding on administrative
penalty fees at all shall be imposed and upon determination of
the amount of the fee.
Instead of penalty fees, in certain cases according to reason 148 to
data protection regulation a reprimand is issued instead of penalty fees
if it is a question of a minor violation. However, consideration must be given
circumstances such as the nature of the breach, severity and
duration.
For authorities, according to Article 83.7, national supplementary
regulations are introduced regarding administrative penalty fees. Of ch. 6 Section 2
the data protection act states that the supervisory authority may levy a penalty fee
by an authority in the event of violations referred to in Article 83.4, 83.5 and 83.6 of
data protection regulation. Then article 83.1, 83.2 and 83.3 of the regulation
apply.
Penalty fee
The Swedish Data Protection Authority has assessed above that the upper secondary school board in the cases in question
the processing of personal data has violated Article 5, Article 9, Article 35
and Article 36 of the Data Protection Regulation. These articles are covered by article
83.4 and 83.5 and in the event of a breach of these, the supervisory authority shall
consider imposing an administrative penalty charge in addition to, or instead of,
other corrective actions.
In view of the personal data processing as this supervision
includes the processing of sensitive personal data concerning children

who are in a dependent relationship with the upper secondary school board and that

these treatments have taken place through camera surveillance in the students' everyday life

environment, it is not a question of a minor violation. There is thus no reason

to replace the sanction fee with a reprimand.

No other corrective action is applicable for that treatment either

that happened. The upper secondary school board must therefore be imposed administrative

penalty fees.

Determining the size of the sanction amount

According to Article 83.1 of the Data Protection Regulation, each supervisory authority must

ensure that the imposition of administrative penalty charges in each individual

case is effective, proportionate and dissuasive.

According to Article 83.3, the administrative sanction fee may not exceed

the amount of the most serious violation if it is one or the same

data processing or connected data processing.

For authorities, according to ch. 6, § 2 second paragraph of the Data Protection Act that

the penalty fees shall be set at a maximum of SEK 5,000,000 at

violations referred to in Article 83.4 of the Data Protection Ordinance and to a maximum

SEK 10,000,000 for violations referred to in Article 83.5 and 83.6.

Violations of Article 5 and 9 are subject to the higher penalty fee

under Article 83(5), while violations of Articles 35 and 36 are covered by it

lower maximum amount according to article 83.4. In this case, it is the question of the same

data processing, which is why the amount must not exceed SEK 10 million.

In article 83. 2 of the data protection regulation, all factors that must

taken into account when determining the size of the penalty fee. In the assessment of

the size of the penalty fee must, among other things, a. Article 83.2 a. is taken into account

(nature, severity and duration of the offence), b (intent or

negligence), g (categories of personal data), h (how the breach came about

Datainspektionen's knowledge) and k (other aggravating or mitigating

factor such as direct or indirect financial gain)

data protection regulation.

In the Data Inspectorate's assessment of penalty fees, consideration has been given to the fact that

there have been violations concerning several articles in the data protection regulation,

whereby violation of articles 5 and 9 is to be judged as more serious and

covered by the higher penalty fee. Furthermore, consideration has been given to

the breach has concerned sensitive personal data, concerning children who have been

in a dependent position in relation to the upper secondary school board. The treatments have

has taken place to streamline operations, the processing has thus taken place

intentionally. These circumstances are aggravating.

Consideration has also been given to the fact that the treatment has come about

Datainspektionen's knowledge via information in the media.

As mitigating circumstances, it is taken into account that the treatment has taken place during

a limited period of three weeks and has only included 22 students.

The Data Inspectorate decides based on an overall assessment that

The high school board in Skellefteå municipality must pay an administrative fee

penalty fee of SEK 200,000.

Warning

According to Article 58.2 a, the Data Inspection Authority has the authority to issue warnings to a personal data controller or personal data assistant if planned treatments are likely to violate the provisions of this regulation.

The high school board in Skellefteå municipality has indicated that they intend to continue use facial recognition for attendance control of students. These treatments will correspondingly violate the provisions of data protection regulation. Because of the risk of future violations i In connection with the planned treatments, a warning is now given in accordance with article 58.2 a of the data protection regulation.

This decision has been made by the director general Lena Lindgren Schelin after presentation by lawyers Ranja Bunni and Jenny Bård. At the final Chief legal officer Hans-Olof Lindblom and the unit managers are in charge Katarina Tullstedt and Charlotte Waller Dahlberg and the lawyer Jeanette Bladh Gustafson participated.

Lena Lindgren Schelin, 2019-08-20 (This is an electronic signature)

Appendices

Appendix 1 – How to pay penalty fee

Copy for the attention of:

Data protection officer for the high school board in Skellefteå Municipality

How to appeal

If you want to appeal the decision, you must write to the Swedish Data Protection Authority. Enter in the letter which decision you are appealing and the change you are requesting.

The appeal must have been received by the Swedish Data Protection Authority no later than three weeks from the day the decision was announced. If the appeal has been received in time the Swedish Data Protection Authority forwards it to the Administrative Court in Stockholm for examination.

You can e-mail the appeal to the Swedish Data Protection Authority if it does not contain any privacy-sensitive personal data or information that may be covered by secrecy. The authority's contact details appear on the first page of the decision.