Decision

Diarienr

2019-08-20

DI-2019-2221

Skellefteå Municipality, Upper Secondary School Board

Supervision according to the EU Data Protection Regulation

2016/679 - face recognition for

attendance control of students

Content

The Data Inspectorate's decision …… .. 2

Report on the supervisory matter ……. 2

Grounds for the decision 4 .. 4

Personal data liability …… 4

Experimental project …….. 4

Legal basis for the processing of personal data (Article 6) ……. 4

Consent as a legal basis …….. 4

The treatment is necessary to perform a task of general

Interest …… .. 6

Sensitive personal data (Article 9) …… ... 7

Basic principles for the processing of personal data

(Article 5) …… ..11

Impact assessment and prior consultation (Articles 35, 36) …… 13

Permission according to the Camera Surveillance Act …… ..15

Risk that the regulations will be violated in the event of a planned continuation

treatment …… 16

Choice of intervention …… .. 16

Penalty fee …… 17

Determination of the amount of the penalty …… 18

Warning …… ..19

How to appeal …… .. 20

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Phone: 08-657 61 00

The Data Inspectorate's decision

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

by using face recognition via camera for presence control of

students have processed personal data in violation of

Article 5 of the Data Protection Regulation1 by dealing with pupils

personal data in a more intrusive way for personal privacy

way and included more personal data than is necessary for

the stated purpose (attendance check),

Article 9 by processing sensitive personal data

(biometric data) without a valid treatment

exceptions to the ban on the processing of sensitive personal data and

Articles 35 and 36 by failing to meet the requirements of a

impact assessment and not having submitted one

prior consultation with the Data Inspectorate.

The Data Inspectorate decides on the basis of ch. Section 2 of the Data Protection Act2 and

Articles 58 (2) and 83 of the Data Protection Ordinance that the Upper Secondary School Board in Skellefteå municipality must pay an administrative sanction fee of 200,000 kronor.

The Data Inspectorate states that the Upper Secondary School Board in Skellefteå municipality is likely to infringe Articles 5 and 9 with the continued use of face recognition for presence control.

The Data Inspectorate therefore decides to give the Upper Secondary School Board in Skellefteå municipality a warning under Article 58 (2) (a) of the Data Protection Regulation.

Report on the supervisory matter

The Data Inspectorate has, through information in the media, been made aware that The upper secondary school board in Skellefteå municipality (hereinafter the upper secondary school board) in one pilot project at Anderstorps gymnasium 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 individuals with regard to the processing of personal data and on that free flow of such data and repealing Directive 95/46 / EC (General Data Protection Regulation).

2 The Act (2018: 218) with supplementary provisions to the EU Data Protection Regulation

face recognition to record students' attendance in a class during some weeks.

The purpose of the supervision has been to review the upper secondary school board's processing of personal data by face recognition for attendance control has been in accordance with the data protection rules.

The Data Inspectorate has examined the personal data processing that
the upper secondary school board has carried out in the current project and also taken
position on any future treatments. The Data Inspectorate has within
in the framework of this supervision has not made any assessment 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 face 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 face recognition
for attendance control. The purpose has been to in a simpler and more efficient way
register attendance at high school lessons. To register attendance at
a traditional way takes according to the high school board 10 minutes per lesson and
by using face recognition technology for presence control it would
according to the board save 17,280 hours per year at the current school.
The Upper Secondary School Board has stated that the face recognition has been carried out
in that the students were filmed by a camera as they entered a classroom.
Images from the camera surveillance have been compared with pre-registered ones
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 information
has been stored on a local computer without an internet connection stored in one
locked cabinet. Express approvals have been obtained from guardians and
it has been possible to waive the registration of personal data with
biometric data.
The supervisory case began with a supervisory letter on 19 February 2019. Answer to
The supervisory letter was received on March 15, 2019, with the addition of appendices on
April 2, 2019. Later additions from the high school board came in on the 16th

Justification of decision

The responsibility for personal data

The Upper Secondary 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 face recognition for attendance control at Anderstorps gymnasium in Skellefteå municipality. The Data Inspectorate shares this view.

Trial project

The current personal data processing has taken place within the framework of one pilot project. The Data Inspectorate finds that the Data Protection Ordinance does not contain any exceptions for pilot or pilot activities.

The requirements of the regulation therefore also need to be met in order to implement them types of activities.

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 Upper Secondary School Board has in its opinion received by the Swedish Data Inspectorate on March 15, 2019 p. a. stated that consent has been given to the treatment that has occurred within the framework of attendance management.

The upper secondary school board's opinion states, among other things: a. the following.

“Ie. the students' guardians receive information about the project's purpose and which personal data processing will take place and may give its

express and voluntary approval for the processing of personal data.

Students who do not want to participate do not need to participate, attendance is checked then according to previous routines. Students also receive information that they reach as preferably can withdraw their approval for the processing of personal data.

(p. 6). ”

Article 6 (1) (a) of the Data Protection Regulation states that a personal data processing is legal if the data subject has left his consent to the processing of his personal data for one or more specific purpose.

Consent of the data subject is defined in Article 4 (11) of the Data Protection Regulation such as any kind of voluntary, specific, informed and unequivocal expression of will, by which the data subject, either by a statement or by a unequivocal affirmative action, accepts the processing of personal data relating to him or her.

Recital 43 of the Data Protection Regulation further states the following.

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

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

shall take place on the basis of the freedom of choice that prevails, but also the relationship that exists between the registered person and the person responsible for personal data.

The scope for voluntary consent in the public sphere is therefore limited. Within the school area, it is clear that the student is in a position of dependence to the school in terms of grades, study grants, education and thus the opportunity to future work or further studies. It is also often a question of children.

The Education Data Inquiry 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 pupil 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 prior to photographing students for the purpose of creating electronic school catalogs or photography to document the activities in preschool and school, not least for the purpose of being 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)

Attendance control is a public law regulated obligation for school activities and the reporting of attendance are of significant importance for

eleven. This treatment is therefore not comparable to it personal data processing that can be done to administer school photography.

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

supervision includes.

The treatment is necessary to perform a task of general interest

The Upper Secondary 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

face recognition is the administrative law's requirement for efficient case management,

the Education Act's requirements for measures in the event of absence and the obligation for

high schools to report invalid absences to Central

the Student Aid Board (CSN).

According to Article 6 (1) (e) of the Data Protection Regulation, processing is lawful if it is

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

exercise of personal data controllers' authority.

Article 6 (2) of the Data Protection Regulation states, inter alia, that Member States may maintain 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 task shall be of general interest

in accordance with Article 6 (1) (e) be determined in accordance with Union or national law

Right.

According to ch. Section 16, first paragraph of the Education Act (2010: 800) requires a student in

high school participate in the activities organized to provide the intended

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

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

arranged to provide the intended education, the principal shall ensure that

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

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

be informed on the same day (Chapter 15, Section 16, second paragraph of the Education Act).

The personal data processing that usually takes place to administer students

attendance at school should be considered necessary due to the role of the principals according to ch. 15 Section 16 of the Education Act and thus constitutes a task of general interest

pursuant to Article 6 (1) (e) of the Data Protection Regulation. In some parts it can even there is a legal obligation under Article 6 (1) (c) of the Data Protection Regulation. According to the preparatory work for the Data Protection Act (Bill 2017/18: 105 New Data Protection Act p. 51), however, increases the requirements for complementary 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 legal support according to ch. 6 and 20 §§ form of government.

The Data Inspectorate can state that there is a legal basis for that administer students' attendance at school, but that there is no explicit legal support to perform the task through the treatment of sensitive personal data or in any other way that violates privacy.

Sensitive personal data (Article 9)

The facial recognition that has taken place in the case in question has meant that Attendance checks have been done by biometric personal data 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, a

exemption from the prohibition under Article 9 (2) of the Data Protection Regulation is applicable.

As stated above, the upper secondary school board has agreed to consent from

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

supervision refers to.

According to Article 9 (2) (a) of the Data Protection Regulation, the processing of sensitive data

personal data may 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 in the case of Union or national law

the law provides that the prohibition in paragraph 1 may not be lifted 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 can therefore not,

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

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

from the ban on the processing of sensitive personal data in the present case.

The Upper Secondary School Board also refers in its opinion to the rules of the Public Administration Act

efficient case management and the school law's rules on handling absence.

It follows from Article 9 (2) (g) of the Data Protection Regulation that the prohibition on processing

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

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

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

sought 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 concerning the exemption if important

public interest has i.a. a. introduced in ch. § 3 of the Data Protection Act.3

According to ch. Section 3, first paragraph 2 of the Data Protection Act states that sensitive

personal data may be processed in accordance with Article 9 (2) (g) of the Data Protection Regulation if this is necessary in

the interests of the public interest;

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

In the preparatory work (Bill 2017/18: 105 New Data Protection Act) it is stated, among other things. a. the following.

“The Government's view, however, is that the concept of the case in most cases

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

The term is used as a delimitation for the Public Administration Act

scope and should, in the Government's view, also be used

3

Individual school principals' processing of sensitive personal data has

regulated in Chapter 26 a. Section 4 of the Education Act (2010: 800), which corresponds to Chapter 3 § 3

the Data Protection Act. As this supervision refers to a municipal school and it is missing

sector-specific rules regarding the treatment of sensitive

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

applicable.

here. The provision should therefore be applicable in the handling of a

matter. (p. 87) ”

Furthermore, the following is stated in the preparatory work for the Public Administration Act

(Bill 2016/17: 180 A modern and legally secure administration - new administrative law).

The term processing includes all measures taken by an authority
takes from the time a case is initiated until it is closed. The expression
case is not defined in the law. Characteristic of what constitutes a
case is, however, that it is regularly concluded by a statement from
the side of the authority intended to have actual effects on one
recipient in the individual case. A case is closed by a decision of
some kind. In assessing the question of whether an authority
position is to be regarded as a decision in this sense it is
the purpose and content of the statement that determines the nature of the statement, not its
external form (p. 286). "

The Data Inspectorate states that the attendance check that takes place through
facial recognition does not constitute a case handling without it being a question
about an actual action. The provision in ch. § 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 face recognition
attendance control of students.

Of ch. 3 Section 3, first paragraph 1 of the Data Protection Act states that 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
provision appears, among other things. a. the following of the preparatory work (prop.2017 / 18: 105 New
data protection law).

“The provision clarifies that it is permitted for authorities to perform
such processing of sensitive personal data as is required in
the activities of the authorities as a direct consequence of, above all
the provisions of the Public Access and Secrecy Act and the Administrative Procedure Act
on how public documents are to be handled, for example by requiring

record keeping and obligation to receive e-mail. Treatment of sensitive

personal data on the basis of this paragraph may only be made about the data

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

The Data Inspectorate states that ch. Section 3, first paragraph 1 of the Data Protection Act

is not relevant for the current processing of personal data.

According to ch. Section 3, first paragraph 3 of the Data Protection Act, authorities may also in other respects

case process sensitive personal data if the processing is necessary with

consideration of an important public interest and does not unduly infringe

the personal integrity of the data subject.

In the preparatory work (Bill 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 data controller, in it

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

undue invasion of the data subject's privacy. If

the treatment would involve such an infringement, it may not take place in accordance with

this provision. To determine if the intrusion is improper must

the authority to make a proportionality assessment where the need to

carry out the processing is weighted against the data subjects' interest in

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

the treatment does not take place should be based on the interest of privacy protection that

the registrants typically have. The personal data controller must

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

the assessment of the invasion of the individual's personal integrity shall be important

added to i.a. the sensitivity of the data, the nature of the processing, the

attitude the data subjects can be assumed to have to the processing, the spread

the information may be obtained and the risk of further processing for others

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

can not be used as a basis for creating privacy-sensitive

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

Attendance management is a comprehensive and central task in the school system and

takes place casually in the day-to-day operations. The Data Inspectorate

therefore considers that ch. § 3 first paragraph 3 of the Data Protection Act can not

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

The provision can thus not be applied to the personal data processing

which the upper secondary school board has carried out. In addition, the Data Inspectorate considers that they

the current personal data processing has entailed an undue invasion of

the privacy of the registered as 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 Data Inspectorate finds that the national

supplementary provisions concerning the exemption in 9.2 g i

the Data Protection Ordinance on important public interest which has been introduced in ch. 3

§ first paragraph of the Data Protection Act are not applicable to those

personal data processing covered by this supervision.

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

prohibited from performing searches that take place on the basis of ch. § 3 first paragraph in

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

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

The Data Inspectorate states that the attendance check presupposes searches

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

the treatments covered by this supervision have also been in breach 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 in

the Data Protection Regulation does not apply to the current processing of

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

means that any of the other exceptions in Article 9 (2) (i)

the Data Protection Ordinance may become relevant, the Data Inspectorate considers 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. These personal data processing has thus taken place in violation of

Article 9 of the Data Protection Regulation.

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

It can be stated that the personal data controller according to Article 5 (2)

the Data Protection Regulation is responsible for compliance with the Regulation and shall

be able to show that the basic principles are followed.

Article 5 of the Data Protection Regulation states, among other things: a. that the personal data shall

collected for specific, explicit and justified purposes and not

later treated in a manner incompatible with those purposes

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

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

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

may be treated only if the purpose of the treatment can not be achieved on one

satisfactorily with other methods.

On the question of how the upper secondary school board has made the proportionality assessment

regarding the current personal data processing, the board has provided

following response in its opinion received on 15 March 2019.

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

present and meet the requirements contained in the Education Act for action then

students have high absenteeism. The method of face recognition is assessed

needed to know for sure that the presence is registered correctly.

Face recognition is also a clear increase in quality compared to

the previous manual handling which on inspection proved to have deficiencies

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

tested, facial recognition was judged to be the best method

meets the requirements both from the legislation and from the purpose of the project. "

The Data Inspectorate has previously found that the personal data processing

which this supervision covers has involved the treatment of sensitive

personal data concerning children who are dependent on i

relation to the upper secondary school board and that these treatments have taken place

through camera surveillance in the students' everyday environment. The Data Inspectorate

assess that these treatments - even if it is a question of relatively few

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

invasion of student integrity.

The Upper Secondary School Board has stated that the purpose of these treatments has been

attendance control. Attendance control can be done in other ways that are smaller

violating the privacy of students. The Data Inspectorate therefore considers that

the method, to use face recognition via camera for presence control, has

been too extensive and implemented for one for the privacy of

intervening manner and thereby been disproportionate to

the purpose. The Upper Secondary School Board's proceedings have thus been carried out in combat

with Article 5 of the Data Protection Regulation.

Impact assessment and prior consultation (Articles 35, 36)

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

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

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

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

rights and freedoms of natural persons.

On the question of whether the upper secondary school board has made an impact assessment according to

Article 35 prior to the start of the project in question, the upper secondary school board has in its

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

The following is clear from the assessment made.

“Face recognition is admittedly biometric data and according to

the Data Protection Regulation sensitive personal data which requires special

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

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

the processing of personal data and there is legal support for

the treatment both in the Public Administration Act and in the Education Act. The handling

described by the provider for handling the sensitive data

such as that there is no mains connection of the equipment that handles

information that only authorized staff have access to

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

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 framework of

the Data Protection Regulation. Overall, no special is required

risk assessment to handle sensitive personal data without what

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

the handling of biometric data and also the entry of a

reason to use the data. Head of Administration for

the upper secondary school office has a delegation to make decisions on approval of

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

In its response, the Board also referred to the appendix “Skellefteå municipality -

The classroom of the future ”. The appendix (p. 5) states that an advantage of

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

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

solution that requires relatively many pictures of each individual as well as that 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 shall:

included 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 treatment in relation to the purposes, a assessment of the risks to data subjects' rights and freedoms referred to in paragraph 1, and the measures planned to address the risks, including: safeguards, security measures and procedures to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account to the rights and entitlements of data subjects and other persons concerned interests.

The Data Inspectorate states that the upper secondary school board has made one risk assessment. In the risk assessment, it has been concluded that the legal aid one refers to and the security the treatment is covered by means that no one special risk assessment needs to be made regarding the sensitive ones personal data.

According to the Data Inspectorate's assessment, the current treatments have included a number of factors that suggest that an impact assessment according to Article 35 should have been done before the proceedings began. The treatments have happened with camera surveillance which is a systematic surveillance and they have included sensitive personal data about children in an environment in which they are dependency. Face recognition is also a new technology. Requirements for one impact assessment under Article 35 can therefore be based on those assessments which preceded the current use.

The Data Inspectorate assesses that the high school board's risk assessment reported lacks an assessment of the risks that exist for them registered rights and freedoms as well as a statement of the proportionality of the treatment in relation to its purposes why the requirements in Article 35 can not be considered fulfilled.

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

consult with the regulatory authority on an impact assessment

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

unless the data controller takes measures to reduce the risk.

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

submitted a prior consultation to the Data Inspectorate. The inspection

assesses that there have been a number of factors that make it high

risk to individuals' rights and freedoms 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'

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

lacks an assessment of current risks to data subjects' rights and

freedoms with the treatments, the upper secondary school board has also not been able to show

that the high risk provided for in Article 36 has been reduced. The Data Inspectorate states

because the current treatments should have caused one

prior consultation with the Data Inspectorate in accordance with Article 36 before processing

initiated. The proceedings have thus also taken place in breach of Article 36.

Permit according to the Camera Surveillance Act

The Camera Surveillance Act contains national provisions regarding camera surveillance which, in accordance with section 1,

supplement the Data Protection Ordinance. Of § 2

The Camera Surveillance Act states that the purpose of the law is to meet the need

of camera surveillance for legitimate purposes and to protect natural persons

against undue invasion of privacy during such surveillance.

The definition of camera surveillance in section 3 of the Camera Surveillance Act entails among other things that it must be a question of equipment used on such means involving permanent or regular repeated personal surveillance.

According to section 7 of the Camera Surveillance Act, a permit for camera surveillance of a person is required place to which the public has access, if the surveillance is to be conducted by one authority.

The Data Inspectorate states that this has been a permanent and regular issue repeated personal surveillance when the upper secondary school board has used camera surveillance with face recognition technology in conjunction with its attendance control projects over a three-week period.

The Upper Secondary School Board is an authority and must therefore be based on it permission to camera-monitor a place to which the public has access. The question is then if the public is considered to have access to the place provided by the upper secondary school board

camera-monitored using facial recognition technology in in connection with the registration of students' attendance. Practice shows that the concept "Place where the public has access" must be interpreted broadly (see Högsta the decision of the Administrative Court RÅ 2000 ref. 52).

In general, a school is considered a place to which the public does not have access, however, there are certain areas of a school where it is believed that the public has access. Examples of such areas are main entrances and corridors such as leads to the principal's office. The investigation shows that the students were registered using face recognition each 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 assess

The Data Inspectorate that it is not a question of a place where the public has

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

However, the camera surveillance is unlicensed does not have to mean that it is one

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 will be violated in the event of planned further treatment

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

to re-process personal data in the future through face recognition

for attendance control of students. The Data Inspectorate has found above that

the upper secondary school board's proceedings have been in violation of Articles 5 and 9

the Data Protection Regulation. The Data Inspectorate therefore finds that

the upper secondary school board risks violating the said provisions even at

planned treatments.

Choice of intervention

Article 58 of the Data Protection Regulation lists all the powers that:

The Data Inspectorate has. According to Article 58 (2), the Data Inspectorate has a number

corrective powers, e.g. a. warnings, reprimands or restrictions

of treatment.

According to Article 58 (2) (i) of the Data Protection Regulation,

the supervisory authority shall impose administrative penalty fees in accordance with

with Article 83. Pursuant to Article 83 (2), administrative penalty fees,
depending on the circumstances of the individual case, applied in addition to or in
instead of the measures referred to in Article 58 (2) (a) to (h) and (j)
Article 83 (2) (n) the factors to be taken into account in administrative decisions
penalty fees in general shall be imposed and in determining
the size of the fee.
Instead of penalty fees, in certain cases according to recital 148 to
data protection regulation a reprimand is issued instead of penalty fees
if it is a matter of a minor infringement. However, consideration must be given
circumstances such as the nature of the infringement, the severity and
duration.
For authorities under Article 83 (7), national supplementary
provisions are introduced regarding administrative sanction fees. Of ch. 6 § 2
The Data Protection Act states that the supervisory authority may charge a penalty fee
by an authority in the event of infringements referred to in Article 83 (4), 83 (5) and 83 (6) i
the Data Protection Regulation. In that case, Article 83 (1), (2) and (3) of the Regulation shall apply
apply.
Penalty fee
The Data Inspectorate has above assessed that the upper secondary school board in the relevant
the processing of personal data has infringed 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 violation of these, the supervisory authority shall
consider imposing an administrative penalty fee in addition to, or instead of,
other corrective actions.
In view of the fact that the personal data processing provided by this supervision
has involved the processing of sensitive personal data concerning children

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

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

environment, it is not a matter of a minor infringement. There is thus no reason

to replace the penalty fee with a reprimand.

No other corrective action is relevant for that treatment either

as happened. The Upper Secondary School Board must thus be charged with administrative

penalty fees.

Determination of the amount of the sanction

According to Article 83 (1) of the Data Protection Regulation, each supervisory authority shall:

ensure that the imposition of administrative penalty fees in each individual

cases are effective, proportionate and dissuasive.

According to Article 83 (3), the administrative penalty fee may not exceed

the amount of the most serious infringement in the case of one or the same

data processing or interconnected 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

infringements referred to in Article 83 (4) of the Data Protection Regulation and up to

SEK 10,000,000 in the event of infringements referred to in Article 83 (5) and (6).

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

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

lower maximum amount in accordance with Article 83 (4). In this case, it is a question of the same

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

Article 83. 2 of the Data Protection Regulation sets out all the factors that must

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

the size of the penalty fee shall include a. account is taken of Article 83 (2) (a)

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

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

The Data Inspectorate's knowledge) and k (other aggravating or mitigating

factor such as direct or indirect financial gain)

the Data Protection Regulation.

In the Data Inspectorate's assessment of the penalty fee, account has been taken of the fact that

there have been infringements concerning several articles of the Data Protection Regulation,

whereby infringement of Articles 5 and 9 is to be judged as more serious and

covered by the higher penalty fee. Furthermore, it has been taken into account that

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

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

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

intentionally. These circumstances are aggravating.

Account has also been taken of the fact that the treatment has taken place

The Data Inspectorate's knowledge via information in the media.

Mitigating circumstances take into account that the treatment has been ongoing during

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

The Data Inspectorate decides on the basis of an overall assessment that

The upper secondary 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 Inspectorate has the power to issue warnings to

a personal data controller or personal data assistant if planned

treatments are likely to violate its provisions

Regulation.

The upper secondary school board in Skellefteå municipality has stated that they intend to continue

use face recognition for student attendance. These

treatments will similarly violate the provisions of

the Data Protection Regulation. Due to the risk of future violations in

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 was made by the Director General Lena Lindgren Schelin after

presentation by lawyers Ranja Bunni and Jenny Bård. At the final

The case is handled by Hans-Olof Lindblom, General Counsel, and the Heads of Unit

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 a penalty fee

Copy for information to:

Data protection representative for the upper secondary school board in Skellefteå Municipality

How to appeal

If you want to appeal the decision, you must write to the Data Inspectorate. Enter i

the letter which decision you are appealing and the change you are requesting.

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

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