Decision

Diary no

2020-11-23

DI-2019-7024

City of Stockholm, Board of Education

The Education Administration

Box 22049

104 22 Stockholm

Supervision according to the EU's data protection regulation 2016/679 against the Education Board in the City of Stockholm

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 violations

The Swedish Data Protection Authority states that the Education Board in the City of Stockholm has processed personal data in violation of article 5.1 f of the data protection regulation1 which requires appropriate security for the personal data, including protection against unauthorized or unauthorized processing and in violation of Article 32.1 which requires that the person in charge of personal data take appropriate technical measures and organizational measures to ensure a level of security that is appropriate in relation to the risk to the rights and freedoms of natural persons by:

- in the module School duty monitoring, during the period 25 May 2018 until August 27, 2020, had a permission assignment that has been more extensive than is necessary in light of what respective role holders need to perform their work as well by unauthorized persons having access to privacy-sensitive information

personal data concerning students with protected identity.

- in the Student Documentation subsystem, during the period 26 October 2018 until November 2019, unauthorized persons have had access to personal data concerning a very large number of students, some of whom have have been privacy-sensitive/sensitive personal data.

- in the Home subsystem for guardians, during the period 27 June 2019 until August 24, 2019, unauthorized persons have had access to personal data concerning guardians.

- in the Administration interface subsystem, during the period 25 May 2018 until August 26, 2019, unauthorized persons have had access to privacy-sensitive personal data concerning teachers with protected identity.

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).

The Swedish Data Protection Authority states that the Education Board in the City of Stockholm, during the period 25 May 2018 until 27 August 2020, have processed personal data in the subsystems School obligation monitoring, Student documentation,

Home for guardians and the Administration interface in violation of

Article 35, by not having carried out impact assessments for these

system despite the fact that the treatments likely lead to a high risk of physical

people's freedoms and rights because it is a matter of large systems, with

many children registered and with both sensitive and privacy sensitive

personal data.

Administrative penalty fee

Datainspektionen decides with the support of articles 58.2 and 83

data protection regulation and ch. 6 Section 2 of the Data Protection Act2 that

The Education Board in the City of Stockholm for the violations of Article 5.1 and

Article 32.1 of the Data Protection Regulation must pay an administrative

penalty fee of SEK 4,000,000 (four million).

Orders

Datainspektionen orders with the support of article 58.2 d i

the data protection regulation the education board to implement a

impact assessment in accordance with Article 35 of the Data Protection Regulation

regarding the subsystems School obligation monitoring, Student documentation and

Home page for guardians.

Datainspektionen orders with the support of article 58.2 d i

the data protection regulation The Education Board in the City of Stockholm to limit

authorization assignments in the module School obligation monitoring to only those

persons who have a need to process personal data in order to carry out their

duties.

2

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

The Swedish Data Protection Authority

DI-2019-7024

1. Statement of the supervisory matter

The Swedish Data Protection Authority has through notifications about personal data incidents from

The education board in the city of Stockholm has been alerted to unauthorized persons

access to student data in the School Platform.

From the notifications received, it has emerged that the digital platform

which is used in the city of Stockholm, the School Platform, is a city-wide one

project and the platform consists of six subsystems. It has also emerged that

The Education Board in the City of Stockholm is responsible for personal data for them

personal data processing in the School Platform to which the incidents refer.

Against the background of these notifications, the Data Protection Authority has initiated the current one

the inspection on 24 June 2019 (dnr 2019-7024) by the board of education

processing of personal data, in order to review the security measures for

the access to personal data within the framework of two modules in the subsystem

The child and student register:

-

School duty monitoring

-

Intermunicipal agreements

After the inspection began, the board of education came in with more

notifications of personal data incidents. Against the background of the data which

appeared in these reports, the Data Inspection Authority decided on 18 June 2020

to extend supervision to also include a review of security measures

for the access to personal data within the framework of the subsystems:

-

Student documentation

Home page for guardians (Home page)

The administration interface "Contact information

teacher”(Administrative interface)

With regard to Intermunicipal agreements, it has emerged that it constitutes a module i

The child and student register. This module has not been fully implemented and

used by a limited number of users. In the module Intermunicipal agreements

there have been nine students. The incident in the module did not involve children

protected identity as stated in the notification of the personal data incident.

Against this background, the Swedish Data Protection Authority has not examined the module in more detail

Intermunicipal agreements.

As for the School Duty Monitoring, it is a module 3 in Children and

the student register which constitutes an administrative system support for

the education board must be able to fulfill its obligations according to the Education Act

(2010:800). Of the received notification about the personal data incident, it has

emerged that unauthorized personnel have had the opportunity to see information about

classified persons. Against this background, the Swedish Data Protection Authority has

reviewed the technical measures taken by the board to ensure a

appropriate security level in the module. The inspectorate has also reviewed

organizational measures in the form of authorization assignment in the current module.

The personal data incidents received regarding the subsystems

Student documentation, the Start page and the Administration interface have touched

technical deficiencies. The Swedish Data Protection Authority has therefore only reviewed the technical ones

measures that have been taken to ensure an appropriate level of security in these

three subsystems.

The Data Inspectorate's review also refers to the obligation to carry out a

impact assessment according to article 35 of the data protection regulation regarding the

the relevant subsystems.

The Board of Education is responsible for 139 primary schools, 32 primary special schools, 28

secondary schools and six secondary special schools. The Data Inspectorate's current

review does not refer to adult education or pre-school activities.

2. Justification of decision

2.1 Applicable regulations

Personal data controller is as defined in Article 4 i

data protection regulation a natural or legal person, public authority,

institution or other body as alone or together with others

determines the purposes and means of the processing of personal data; if

the purposes and means of the processing are determined by Union law or

the national law of the Member States may the personal data controller or they

3

The Board of Education has stated that School Duty Monitoring is both a module and a separate module

process area.

the special criteria for how he is to be appointed are prescribed in Union law or in

national law of the Member States.

According to article 5.1 f of the data protection regulation, personal data must be processed on a way that ensures appropriate security for the personal data, including protection against unauthorized or unauthorized processing and against loss, destruction or damage by accident, using appropriate technical or organizational measures (integrity and confidentiality).

Article 32.1 of the data protection regulation stipulates that it personal data controller must - taking into account the latest developments, implementation costs and the nature, extent, context of the processing and purpose as well as the risks, of varying degree of probability and seriousness, for rights and freedoms of natural persons - take appropriate technical and organizational measures to ensure a level of security that is appropriate i relation to the risk. According to Article 32.1, this includes points b and d i the data protection regulation, where appropriate,

- the ability to continuously ensure confidentiality, integrity, availability and resilience of treatment systems and services;

and

- a procedure for regularly testing, investigating and evaluating the effectiveness of the technical and organizational measures to ensure the safety of the treatment.

Recital 74 of the data protection regulation states the following:

Personal data controllers should be held responsible for all processing of personal data that they perform or that are performed on their behalf.

Personal data controllers should in particular be required to take appropriate and effective measures and be able to demonstrate that the treatment is compatible with this regulation, also in terms of the effectiveness of the measures. One should within these measures take into account the nature, scope, context and

purposes and the risk to the rights and freedoms of natural persons.

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. This includes according to Article 35.3

b that an impact assessment according to Article 35.1 shall be specifically required in cases

processing takes place to a large extent of special categories of data such as

referred to in Article 9.1 or of personal data relating to convictions in criminal cases

and violations referred to in Article 10.

2.2 Personal data responsibility

What the Education Board in the City of Stockholm stated during the proceedings

The Education Board in the City of Stockholm is responsible for personal data for them

personal data processing that has taken place in the Child and

the student register (module) School duty monitoring, Student documentation, Start page

and the Administration interface. However, the Board of Education is not

personal data controller for the personal data processing that has taken place in

the latter subsystem within the framework of pre-school activities and

adult education.

The Board of Education today uses a number of systems and e-services as part of

its educational and administrative activities. The committee is responsible for

operation and development of municipal activities within preschool, primary school,

elementary special school, leisure center, upper secondary school and upper secondary special school.

The Board of Education is ultimately responsible for how its own operations are conducted

handles the information. Furthermore, the board is responsible for the information

protected in accordance with the city's information security guidelines and

data protection legislation, such as the Data Protection Regulation. The municipal board

is responsible for ensuring that the system meets the requirements for security and is the system owner.

Following a decision in the council, the entire responsibility for the School Platform was moved to

the education board as of 1 January 2020. This means that

The education board is both system owner and information owner.

The Swedish Data Protection Authority's assessment

Nothing in the case speaks against the education board's finding that the relevant

personal data processing covered by this supervision has taken place for

the purpose of the board of education to conduct municipal school activities.

The same also applies to the education board's opinion that it is

The Board of Education in the City of Stockholm, which is responsible for personal data for them

personal data processing that has taken place in the Child and

the student register (module) School duty monitoring, Student documentation, Start page

and the Administration interface. The current supervision does not include

personal data processing that has taken place within the framework of

pre-school activities and adult education, therefore the question falls on

personal data responsibility for the latter processing outside the current one

supervision.

2.3 Monitoring of compulsory education

What the Education Board in the City of Stockholm stated during the proceedings

General about School Duty Monitoring

The school platform consists of six subsystems and the Child and Student Register forms one of these subsystems. There are 101 modules in the Child and Student Register which are divided into eight process areas. School duty monitoring is one of the eight the process areas in the Child and Student Register. The process area School duty monitoring supports the work with school duty monitoring within municipal primary schools as well as regarding students in independent schools there The city of Stockholm is the home municipality. The function also includes the processes regarding municipal activity responsibility. The administrative system support is used to fulfill the education board's obligations regarding compulsory schooling according to the School Act (2010:800) as well as processing and decisions in connected matters to this (primarily according to ch. 7 of the School Act but also ch. 24 § 23). The administrative responsibility means ensuring that students within a certain geographical area are placed at a school close to home.

In the module School obligation monitoring, information on 1,322 active participants is processed compulsory school supervision (number registered) of which 83 pupils are under the age of seven. Of these 1,322 active school duty supervisions have 60 students protected personal data.

The personal data processed in the current module are, among other things, a. name, address, mother tongue, school placement, guardian and contact details for these (phone number and email address) as well as history of school placement and contact persons. Furthermore, decisions containing personal data are processed regarding a specific student where compulsory schooling has ended, continued monitoring (e.g. imposition of a fine or case with the Tax Agency), consent to fulfill compulsory schooling in another way and deferred compulsory schooling (special reasons).

The module contains information that a student attends a resource school or

elementary special school.

Technical deficiencies

On October 5, 2018, it was discovered that all users who had authorization
to the module School Duty Monitoring had the opportunity to see all of them
privacy marked 4 students without school placement. This deficiency is said to be due to
the system lacked logic to in the functionality for school duty monitoring
restrict the authorization of persons marked as confidential. The reason for that is
unknown. When the module was implemented in July 2017, the education board had
no knowledge of any defects. School duty monitoring at the city's
municipal primary schools start from residential area. Privacy marked
people who are unplaced do not have a residential area in the system. The routine is to
employees at the schools should not be able to see these students during this process
only takes place centrally.

Number of users who could potentially have been mistakenly viewed
persons marked confidential are 1,302. The committee is only aware that
a school administrator mistakenly saw the information about students marked confidential.
This person must have found three students marked confidential in the search results. The
there were a total of 60 students with confidentiality marking in School Duty Monitoring. It has
has not been possible to obtain the exact number of users with log history
which had unauthorized access in practice because there are no specific logs
for the module School duty monitoring.

When the flaw was discovered on October 5, 2018, it was not verified that users
saw more information than they were authorized to see. On 5 November 2018, i.e. one

month after discovery, the board was able to verify that users saw more

information than they were authorized to see. The supplier worked out a fix

which went into production on November 9, 2018.

Organizational deficiencies

With regard to the allocation of authority in the School Duty Monitoring, the committee has

stated that there are eight role holders with different authorizations;

Gr system manager Sthlm,

Gr Administrator Compensation Sthlm,

Gr Look Sthlm,

Gr Administrator Language Center Sthlm,

Gr PMO Manager Sthlm,

With persons marked confidential are meant students with protected personal data.

-

Gr Administrator School Sthlm,

Gr School Duty Monitoring Central Admin Sthlm

Gr Watch Economics Sthlm.

The board states that four out of the eight role holders listed above do not

need to have the access to School Duty Monitoring that they have. This is because

that the education administration cannot see that these role holders need to have

access to School Obligation Monitoring alternatively that it is not ensured that

the role only has access to tasks required to complete

the work tasks. The administration has therefore requested that this be adjusted.

The Swedish Data Protection Authority's assessment

Nature of personal data and security requirements

The Swedish Data Protection Authority notes initially that in the module
School duty monitoring processes information about students, such as name, address,
social security number, guardian and contact details for these
(phone number and e-mail address), mother tongue, municipality, school location
(school and grade), history of school placement and contact persons (name,
address, social security number, telephone number and e-mail). It is also processed
information about students whose identity is protected. Furthermore, personal data can i
certain decisions are dealt with in the module such as continued monitoring of a specific student
relating to the imposition of a fine or an investigation or case at the Swedish Tax Agency,
consent to fulfill the school obligation in another way (film recording, Nordic
schooling or travel abroad) as well as deferred compulsory schooling (special reasons).
The Swedish Data Protection Authority considers that information about protected identity is a lot
worthy of protection/privacy-sensitive as the risks to the freedoms of the data subjects and
rights are great when processing this personal data. Statement that a
pupil goes to resource school or primary special school which is also treated in
School duty monitoring is a sensitive personal data6 as it reveals information about
health.

In light of the nature and nature of the personal data processing which
has taken place in the School Duty Monitoring as well as the risks to the freedoms of the registered

5

Gr Administrator Remuneration Sthlm, Gr Administrator Språkcentrum Sthlm, Gr PMO responsible Sthlm and Gr Titta Ekonomi
Sthlm.

6 Article 9 of the Data Protection Regulation.

and rights, the Data Inspection Authority believes that high demands are placed on the technical and organizational measures that the board of education had to take in order to ensure an appropriate level of security in accordance with Article 32 i data protection regulation.

Technical deficiencies

From the investigation into the matter, it appears that unauthorized persons have been able to come to privacy-sensitive personal data concerning students with protected identity. Because there is no log tracking in the module School duty monitoring, it is not possible to state the exact number in retrospect users who had actual unauthorized access to this data. The the technical deficiency in School Duty Monitoring which has now been reviewed has meant that 1,302 users potentially had unauthorized access to personal data regarding 60 students with protected identity. The reason for this depends according to the board on weaknesses in the system that made authorization restriction impossible to data on students with protected identity. There is no indication of when the shortfall occurred but the module was implemented in July 2017 and the shortfall discovered on October 5, 2018.

Organizational deficiencies

The Swedish Data Protection Authority's review of the current subsystem concerns both the requirements on technical measures and organizational measures according to article 32. Av the investigation into the case also reveals that the assignment of authority i School compulsory monitoring is more extensive than is necessary in relation to what the respective role holders need to perform theirs duties. The Board of Education has stated that a review of the eight

the authorization roles should be initialized shortly.

Overall assessment

Both the fact that unauthorized persons had access to/have been able to

access privacy-sensitive personal data concerning students with protected

identity and that there is a more comprehensive authorization for data i

The monitoring of mandatory schooling, if necessary, is contrary to Article 32.1

data protection regulation. According to Article 32.1, the education board must

taking into account recent developments, implementation costs and

the nature, scope, context and purpose of the treatment as well as the risks for

rights and freedoms of natural persons, take appropriate technical and

organizational measures to ensure a level of security that is appropriate i

relation to the risk.

The Swedish Data Protection Authority considers that a suitable security in this case includes a

ability to continuously ensure confidentiality of treatment systems

and the services. By the committee having allocated more comprehensive

authorizations and that unauthorized persons have gained access to personal data about

students with a protected identity, it is the Data Inspectorate's assessment that

the education board lacked the ability to continuously ensure

confidentiality of the data processed in the processing systems and services as required by Article 32.1 of the Data Protection Regulation.

The requirement for adequate security also includes having a procedure to

regularly test, investigate and evaluate the effectiveness of the technical and

the organizational measures taken to ensure the security of the processing

which was also not present in this case. The Swedish Data Protection Authority notes that
if the Board of Education had had such a procedure to regularly
test, investigate and evaluate the effectiveness of the measures taken had
the board was able to ensure/discover whether the technical measures are correct
consistent with the organizational measures taken. As for it
the organizational deficiency (the comprehensive authority) is also according to
Datainspektionen's assessment such a shortcoming in the authorization restriction
which should have been discovered if the Board of Education regularly had
checked the authorization. This, too, is a deficiency in the requirements for adequate security
according to article 32.1 of the data protection regulation.

The Education Board in the City of Stockholm has summarized
personal data in the School Duty Monitoring module in the School Platform in violation of
Article 32 of the Data Protection Regulation.

The Swedish Data Protection Authority also assesses that the education board has processed
personal data in violation of article 5.1 f of the data protection regulation in it
current subsystem. This is because the board has not secured a suitable one
security of the personal data, including protection against unauthorized or unauthorized access
treatment through the use of appropriate technical measures.

2.4 The student documentation

What the Education Board in the City of Stockholm stated during the proceedings

General information about the student documentation

The student documentation is one of six subsystems that the School Platform consists of.
In the Student documentation subsystem, there are a total of 464,611 registered, of which

122,699 are pupils in municipal primary and secondary schools. Of these students
has 787 protected personal data. In this subsystem there are 233,066
registered guardians and 34,756 employees (part of these employees
work in child care and adult education that are not covered
supervision).

The personal data that is processed in the current subsystem is, among other things, a. grades, results
on national tests, reporting results to Statistics Norway, Statistics Sweden,
assessment support which involves documentation of the student's level of knowledge,
information that some students need extra adaptations, documentation
regarding investigations and action programs, personal data for work with
development interviews and written reviews.

Technical deficiencies

On August 21, 2019, it was revealed via a thread on Twitter that a guardian
had discovered a data leak in the student documentation. The person behind
The Twitter account has its own access and login via Bank ID analyzed
the traffic and calls between the frontend and backend system.7 The person has
then extracted parts of these calls and manipulated them in order to
come across other people's information.

7

The terms are used by the Education Board in the City of Stockholm and their function can
generally described as follows. The separation of frontend and backend systems simplifies
the data process when it comes to multi-layered development and maintenance of data systems. One
frontend systems are primarily used to send questions and requests and receive data from
the backend system. It allows users to interact and use one
information system. Typically, front-end systems have very limited computational or
business logic processing functions and relies on data and functions from

the backend system. A front-end system can include or consist of a text or graphic system
user interface (GUI) and/or a frontend client application connected to
the backend system. The backend system manages databases and data processing components
and ensures that the responses to the front-end system's requests are retrieved from databases and
computing components.

The board has stated that when logging in to the Student Documentation i
The school platform exposes personal data through an API8. Due to a technical
shortfall in the API could people, with some knowledge of network systems and
programming, monitor calls made from a logged in client mode, copy
and modify them. That way, new calls could be made and personal data
that would not be available to the person became available. This means
that personal data was available depending on which requests an individual
did, regardless of authority. That in turn gave access to personal data without
correct authorization.

This lack has meant that unauthorized persons have been able to gain access
the following information about other students: first name, last name, social security number,
school type (e.g. primary special school), grade, school ID, class, student's assessment from
the development conversation module, whether it is an integrated user or not as well
migrated IUP9 documents from Skolwebben.

All registered guardians in the School Platform have because of it
the current deficiency had the opportunity to gain unauthorized access to information. According to
the education board, one person took advantage of this opportunity and did
searches on 101 unique people. The deficiency has existed since the subsystem

was launched. The module where the deficiency existed has been in operation since October 26 2018. This flaw had not been caught in previous functional and security tests before the feature was put into production.

The deficiency in the subsystem was addressed through code changes that were completed during November 2019. The student documentation was closed after the shortage was discovered until all discovered deficiencies were remedied.

8

An application programming interface (API) is a set of protocols, routines, functions and/or commands that programmers use to develop software or facilitate interaction between different systems. APIs are usually useful for programming GUI (graphical user interface) components, as well such as for one program to request and satisfy services from another program.

9 Individual development plan.

The Swedish Data Protection Authority's assessment

Security requirements

The Swedish Data Protection Authority notes initially that in the subsystem Student documentation in the School Platform is extensive personal data processing concerning thousands of students, guardians and teacher.

According to Article 9 of the Data Protection Regulation, information about health is so-called sensitive personal data according to the data protection regulation. In preliminary work, Processing of personal data in the field of education (prop. 2017/18:218 p.57) the following is stated:

As mentioned above, sensitive personal data is also processed about

health when examining reception in the elementary special school, the special school,

the high school special school, and special education for adults according to 7, 18 and 21

Cape. the school law. Even a statement that a student attends such a school is one

sensitive task.

The Swedish Data Protection Authority further states that in the Student Documentation subsystem

processed data relating to students' health such as data appearing in

various investigations about students, special adaptations, etc. Also information about

the fact that some students go to a special school means treating sensitive people

personal data.

In addition, extensive personal data processing is added in

Student documentation that does not constitute sensitive personal data according to

data protection regulation but are to be considered extra privacy sensitive such as

data relating to reviews and data from development interviews.

In light of the scope of the personal data processing that takes place in

the Pupil Documentation subsystem, the nature and nature of the treatments and

the risks to the freedoms and rights of the data subjects is considered by the Data Inspectorate

that very high requirements must be placed on the technical measures that must be taken in order to

ensure an appropriate level of security in accordance with Article 32 i

data protection regulation.

Assessment of technical measures

The technical deficiency in the student documentation that is now being reviewed has meant

that unauthorized persons have been able to access other people's personal data through

to monitor calls made from a logged in client mode, copy and modify
them. In this way, new calls could be made and personal data that could not
would be available became available. According to the board of education
data could be accessed by unauthorized persons, e.g. a. other people's first names,
surname, social security number, school type (e.g. elementary special school), grade, school ID,
class and students' judgments from the development interview module. This technical
shortage has meant that all registered guardians in the School Platform
has had the opportunity to gain unauthorized access to information about all registered users
students, including sensitive and privacy-sensitive data concerning
the students.

The Swedish Data Protection Authority notes that the technical security measures that have
taken in the Pupil Documentation subsystem in the School Platform has been
deficient as unauthorized persons have been able to gain access in a simple way
extensive sensitive and privacy-sensitive personal data concerning
thousands of students. The Board of Education has thus failed in its obligation
according to article 32.1 of the data protection regulation that with consideration of the latest
the development, implementation costs and the nature, scope,
context and purpose as well as the risks to the rights of natural persons and
freedoms, take appropriate technical measures to ensure a level of security
which is appropriate in relation to the risk.

The current technical deficiency that is now being reviewed in the subsystem
According to the Swedish Data Protection Authority's assessment, the student documentation should have
discovered at an early stage, before the processing of the personal data
was started. The Swedish Data Protection Authority considers that a suitable security in this case
includes an ability to continuously ensure confidentiality of
the treatment systems and services.

The requirement for adequate security also includes having a procedure to

regularly test, investigate and evaluate the effectiveness of the technical

the measures taken to ensure the safety of the treatment. That it

the current technical deficiency was discovered by a guardian long after that

The student documentation subsystem was launched, shows that the board of education

neither has taken care to continuously ensure confidentiality thereof

subsystem or had a procedure to regularly test, investigate and

evaluate the effectiveness of the technical measures taken in a way that

meets the requirements of the data protection regulation. The Swedish Data Protection Authority notes that

this too is a deficiency in the requirements for adequate security according to Article 32.1 i

data protection regulation.

In summary, the Board of Education in the City of Stockholm has dealt with

personal data in the Student Documentation which is part of the School Platform i

contrary to Article 32 of the Data Protection Regulation.

The Swedish Data Protection Authority also assesses that the education board has processed

personal data in the subsystem in question in violation of Article 5.1 f i

data protection regulation. This is because the board has not secured one

appropriate security for the personal data, including protection against unauthorized or

unauthorized processing through the use of appropriate technical measures.

2.5 Home page

What the Board of Education in the City of Stockholm has stated during the proceedings

General about the Start page

The start page is one of the six subsystems that the School Platform consists of. A module

in the subsystem Startsidan it is called "contacts" where personal data from School
The Data Sync Database (SDS DB) is processed, which in turn retrieves information
from the child and student register subsystem. Personal data is processed to
ensure guardians' access to information about the right school and class
based on the connection between guardian and child/pupil and child/pupil
connection to classes/groups. This is controlled based on information in Barn- and
the student register.

Among the personal data that is processed on the Home page are those of students and teachers
name, e-mail address, school connection, connection to groups, connection to
departments, mentor groups and courses. Information about is also processed
guardian's name, social security number, address, e-mail address, telephone number
and connection to children.

In the subsystem Startsidan there are a total of 440,695 registered, of which 31,847 are
employees, 233,062 guardians and 122,699 pupils in municipal primary schools
and high school.

Technical deficiency

On June 27, 2019, a new functionality was introduced on the Start page there
guardians could search for other guardians with children in the same class
provided that the guardians have consented to it. The 24th of August
In 2019, it was discovered that the technical measures have broken down
guardians by changing calls in the developer tool in their browser
with the help of social security number could search for other guardians who
were registered on the Start page. The shortage has meant that everyone registered

guardians in the School Platform have had the opportunity to take part in unauthorized information. This shortcoming has existed since the new functionality was introduced in June 2019. The Board of Education has identified a guardian who has accessed unauthorized information about seven unique people. None of the victims had protected identity.

The technical flaw was fixed the same day it was discovered, August 24 2019, through a code amendment that was produced.

The Swedish Data Protection Authority's assessment

Security requirements

The Data Inspectorate notes initially that in the subsystem Startsidan i The school platform carries out extensive processing of personal data relating to thousands of students, guardians and teachers. It is treated differently information such as guardian's social security number, address, e-mail address, telephone number and connection to children.

In light of the scope of the personal data processing that takes place in subsystem Start side, the nature and character of the treatments and the risks associated with them freedoms and rights of data subjects, the Data Inspectorate believes that high requirements must be placed on the technical measures to be taken to ensure a suitable security level in accordance with Article 32 of the Data Protection Regulation.

The assessment of technical measures

The technical deficiency in the Start page that is now being reviewed has meant that guardians by changing calls in the developer tool in their browser with the help of social security number could search for other guardians who are registered on the Start page. This means that guardians have on one easily able to gain unauthorized access to other custodians personal data. The Board of Education has thus failed in its obligation

according to article 32.1 of the data protection regulation that with consideration of the latest the development, implementation costs and the nature, scope, context and purpose as well as the risks to the rights of natural persons and freedoms, take appropriate technical measures to ensure a level of security which is appropriate in relation to the risk in the relevant subsystem.

The Swedish Data Protection Authority considers that a suitable security in this case includes a ability to continuously ensure confidentiality of treatment systems and the services. The current technical deficiency should according to The Data Inspectorate's assessment has been discovered at an early stage before the processing of the personal data began. That the current shortage was discovered by a guardian after the Home subsystem was launched, shows that the education board also did not have a procedure that satisfies the requirements of the data protection regulation to regularly test, investigate and evaluate the effectiveness of the technical measures taken. Even this is lack of requirements for appropriate security according to Article 32.1 of the Data Protection Regulation.

The Board of Education in the City of Stockholm has thus processed personal data in the subsystem in question in violation of Article 32 i data protection regulation.

The Swedish Data Protection Authority further assesses that the Education Board in the City of Stockholm has processed the personal data in the relevant subsystem in violation of Article 5.1 f of the data protection regulation because the board has not secured one appropriate security for the personal data, including protection against unauthorized or unauthorized treatment.

2.6 The Administration Interface

What the Board of Education in the City of Stockholm has stated during the proceedings

General about the Administration interface

The administration interface was common to the two subsystems

Absence/Presence and Schedule in the School Platform, where settings for these

subsystem is performed. The system read data from the Child and Student Register which is

the source system for basic data in the current subsystem. The data was administered in

this interface and then displayed to the users in different interfaces

based on the role in the system and depending on the settings that were made.

The administration interface was not intended for guardians. People with

a combination of roles such as, for example, teacher or clerk who are also

guardians did not have access to the data associated with the role

guardian when logging into this interface. People who only had

however, the role of guardian was given when logging in to the Administration interface

access to data linked to own children.

Among the personal data handled are name, social security number, e-mail,

telephone number, department or group/class affiliation, teacher's connection

to group/class/department, lesson information (group/class/subject/course, hall

and time), absence data (presence/absence, reason for absence,

valid/invalid) and application for leave.

Technical deficiencies

On August 26, 2019, it was discovered that guardians via search on Google

found links for login to the Administration interface there

guardians should not be able to log in. The current shortage has meant that

guardians have been able to produce reports for "Teacher contact details"

where name, e-mail address and work phone number are displayed. Furthermore, have

the interface has not proven to be adapted for handling confidential information

tasks. Individuals with protected identity have not had a mark as

reveals this. This means that people with protected identity can have

covered by the deficiency in question, but that these cannot be distinguished from the others

registered.

The flaw has existed since the feature was launched, likely since August 2017.

It was discovered internally on 19 November 2018 and was then assessed by

the board of education be trivial because the investigation then claimed that

no data that guardians could not see in another interface

was shown. The differences that existed e.g. access to "Contact details-Teacher",

was then said to only show the student's current teachers and which subjects they have

the student. It was also said that no contact details were shown. The deficiency would be resolved

with a code merge that was then planned in 2019. The release which

the correction was to be covered by early 2019, however, it was deferred to the future.

The personal data that was shown as a result of the current deficiency is

contact details for teachers, such as name, class, school, subject/course, e-mail address (both work and private address) and

telephone number (both work and private number).

It is not possible to determine how many guardians have logged into this

interface and wrongly accessed data. It is also not possible to obtain

how many of the teachers covered by the reports also had their private e-mail address entered in the Child and Student

Register and could therefore be shown to

unauthorized. The Board of Education cannot state the number of registered as

was affected by this technical deficiency. There are currently between 50 and 60 teachers

which has protected identity in this subsystem. The Board of Education cannot

rather estimate what the current shortcoming meant for the registered

because the committee has not received indications of consequences.

After the vulnerability was discovered and could be confirmed, Stockholms requested

city on August 26, 2019 that the provider would close access for

caregiver. The subsystem was shut down and is no longer in operation.

The Swedish Data Protection Authority's assessment

Security requirements

The Swedish Data Protection Authority notes initially that in the Administration interface

was processed data concerning teachers, such as e-mail address (both work and

private address) and telephone number (both work and private numbers). The

data concerning teachers whose identity is protected was also processed.

As previously mentioned, the Swedish Data Protection Authority considers that information relating to persons

with protected identities are highly protective/privacy-sensitive as the risks

because the freedoms and rights of the data subjects are great when processing them

personal data. In light of the nature and nature of the

personal data processing that has taken place in the Administration interface as well as

the risks to the freedoms and rights of the data subjects is considered by the Data Inspectorate

that high demands must be placed on the technical measures that must be taken in order to

ensure an appropriate level of security in accordance with Article 32 i

data protection regulation.

The assessment of technical measures

In the Administration interface, guardians have via search on Google

able to find links for logging in to the Administration interface there
guardians should not be able to log in. In this interface, guardians have
was able to produce information about a. teachers' private contact details such as
e-mail address and private telephone number. This interface has also been shown
not be adapted for handling information about individuals with protected

identity. This means that unauthorized persons have been able to gain access
information about persons with protected identity.
Because the current deficiency has meant that unauthorized persons have had
possibility to access information about persons with protected identity
the education board failed in its obligation according to article 32.1 i
data protection regulation that, taking into account the latest developments,
implementation costs and the nature, extent, context of the processing
and purpose as well as the risks to the rights and freedoms of natural persons take
appropriate technical measures to ensure a level of security that is appropriate i
relation to the risk.
The Swedish Data Protection Authority considers that a suitable security in this case includes a
ability to continuously ensure confidentiality of treatment systems
and the services. The current technical deficiency should according to
The Data Inspectorate's assessment has been discovered at an early stage before
the processing of the personal data began. The mentioned shortcoming has
existed for a long period since the system was launched.
The Board of Education was made aware of the deficiency in November 2018,
but chose not to fix it until the flaw was rediscovered in August

2019. The Board of Education has thus failed in the necessity to

continuously ensure confidentiality in the current interface. The requirement of

appropriate security also includes having a procedure to regularly

test, examine and evaluate the effectiveness of the technical measures taken

the measures to ensure the safety of the treatment, which also has not

present in this case against the background of what was stated above.

The Board of Education in the City of Stockholm has thus processed

personal data in the subsystem in question in violation of Article 32 i

data protection regulation.

The Swedish Data Protection Authority also assesses in this part that the education board has

processed personal data in the relevant interface in violation of Article 5.1 f i

data protection regulation because the board has not secured a suitable one

security of personal data.

2.7 The impact assessment

What the Education Board in the City of Stockholm stated during the proceedings

The Board of Education states that because the Child and Student Register

put into production before May 25, 2018 has no comprehensive coverage

impact assessment according to Article 35 of the Data Protection Regulation yet

carried out. However, impact assessments have been carried out continuously

as new functionalities have been added.

The committee believes that an impact assessment needs to be done and work with

this is ongoing and should be completed in December 2020. The vulnerabilities that have

discovered during penetration tests has been quickly remedied.

The Board of Education has further stated that it is working with a

risk management plan, where what is discovered during risk and impact analyses

are addressed systematically in accordance with the city's risk matrix and that the objective

is that there will soon be active risk management for the whole

The school platform. The Board of Education has a developed process to

ensure adequate information security which means that risk and

impact analyzes must be carried out

Regarding the administration interface, there will be no impact assessment

to be done for this part as the interface has been deprecated and is no longer in

use.

The Swedish Data Protection Authority's assessment

In the subsystems and modules that have been the subject of the Data Inspectorate

review is processed that of students, school staff and guardians

personal data of varying degrees of sensitivity. The relevant subsystems covered

of the current supervision involves the treatment of a large number

personal data of a large number of registered persons, who are largely children, who i

the data protection regulation is highlighted as vulnerable natural persons10.

The Swedish Data Protection Authority states that in the subsystems in question extensive

personal data processing with different types of personal data such as grades,

investigations about students, development interviews, special adaptations, children's and

adults with protected identity. Furthermore, sensitive ones are also treated

personal data to a certain extent, i.e. particular categories of data such as

referred to in Article 9.1 as health data. It is thus a matter of one

10

See recital 75 of the data protection regulation.

extensive personal data processing on a large number of registered i

the system.

The Swedish Data Protection Authority states that it is a question of processing that includes consideration of its nature, scope, context and purpose likely leads to a high risk for the rights and freedoms of natural persons in such a way which requires that the Board of Education should have conducted a impact assessment according to Article 35 of the Data Protection Regulation. Of article 35.3 (b) further states that an impact assessment according to paragraph 1 in particular shall be required when it comes to processing on a large scale of special categories of data referred to in Article 9.1. The Swedish Data Protection Authority states that the processing of the personal data in the relevant subsystems is by it the nature specified in Article 35.3 b of the Data Protection Regulation, which is a circumstance that particularly requires an impact assessment.

The Swedish Data Protection Authority has, guided by guidelines from the Article 29 working group and the criteria developed by the group11, adopted a list of when an impact assessment must be carried out.12

In addition to the situations specified in Article 35.3 of the Data Protection Regulation, and taking into account the exception in Article 35.10, an impact assessment shall regarding data protection is made if the planned processing meets the minimum two of the nine criteria mentioned in the list.

In this case, sensitive data or data is processed by a lot personal nature, data to a large extent and data relating to vulnerable people registered which are three of nine criteria which, according to the list, suggest that an impact assessment must be carried out.

Furthermore, the list indicates when an impact assessment is not required. The

no impact assessment is required for treatments that have

checked by a supervisory authority or a data protection officer in accordance

11

Guidelines on impact assessment regarding data protection and determining whether

the processing is "likely to lead to a high risk" in the sense referred to in the regulation

2016/679, last revised and adopted on 4 October 2017, WP 248 rev. 01.

2 (6) http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236. The

The European Data Protection Board (EDPB) has approved the guidelines on 25 May 2018

https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents.pdf.

12 List according to Article 35.4 of the Data Protection Ordinance, dnr DI-2018-13200

2 4 (31)

The Swedish Data Protection Authority

DI-2019-7024

with Article 20 of Directive 95/46/EC and whose implementation has not been changed

since the previous check. As a good practice, however, one should

impact assessment is continuously reviewed and evaluated regularly.

The Swedish Data Protection Authority states that there is no circumstance which

suggests that an impact assessment is not required. In the 29-group guidelines

specified that although an impact assessment is not required on 25 May

In 2018, it is necessary for the personal data controller to carry out such

impact assessment, at the appropriate time and as part of it

general responsibilities.13

The Swedish Data Protection Authority notes that the processing of personal data that takes place

in the current subsystems in the School Platform likely lead to a high risk of

rights and freedoms of natural persons in such a way that a

impact assessment according to Article 35 of the Data Protection Regulation needs carried out in the respective subsystems covered by this supervision, in order to assess the consequences of the planned processing for the protection of personal data in accordance with Article 35.

The fact that the system was launched before May 25, 2018 does not affect the inspection's assessment. The Board of Education states that the reason for that the current deficiencies that caused the incidents that occurred in the respective subsystem not discovered before is that no comprehensive impact assessment has been carried out.

In the current review, the Swedish Data Protection Authority has assessed that there has been technical deficiencies in several subsystems covered by the inspection. The inspection has also assessed that the authority allocations have been more extensive in it the module in which the question has been reviewed (School obligation monitoring). Against the background of the education board's own information that has emerged in the case applies impact assessment, the Swedish Data Protection Authority believes that the board of education, during the period 25 May 2018 until 27 August 2020, has not completed a impact assessment covering the subsystems School duty monitoring, Student documentation, the Start page and the Administration interface in its whole. If the committee would have made a full impact assessment then so the identified deficiencies could probably have been avoided. The Board of Education has thus not carried out an impact assessment that meets the requirements of Guidelines on impact assessment regarding data protection and determining whether the processing is "likely to lead to a high risk" in the sense referred to in the regulation 2016/679, last revised and adopted on 4 October 2017, WP 248 rev. 01. 2 (6) p. 1516 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

article 35 of the subsystems in question and has thus treated

personal data in violation of the current provision.

3. Choice of intervention

3.1 Possible intervention measures

The Swedish Data Protection Authority has a number of corrective powers to access according to

article 58.2 a–j of the data protection regulation, among other things to order it

personal data controller to ensure that the processing takes place in accordance with

the regulation and if required in a specific manner and within a specific period.

From point (i) of Article 58.2 and Article 83.2 of the Data Protection Regulation

it appears that the Data Protection Authority has the authority to impose administrative

penalty charges in accordance with Article 83. Depending on the circumstances i

the individual case, administrative penalty fees shall be imposed in addition to or in

instead of the other measures referred to in Article 58.2.

Furthermore, article 83.2 states which factors must be taken into account when deciding whether

administrative penalty fees shall be imposed and upon determination of

the amount of the fee.

If it is a question of a minor violation, the Data Protection Authority receives according to what

as set out in Recital 148 of the Data Protection Regulation instead of imposing a

penalty fee issue a reprimand according to article 58.2 b i

data protection regulation. Consideration must be given to aggravating and mitigating circumstances

circumstances of the case, such as the nature of the offence, its severity and

duration as well as previous violations of relevance.

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.

3.2 Injunction

The Swedish Data Protection Authority has found that the Education Board in the City of Stockholm,
by having more extensive authority allocation than necessary i
the subsystem/module School obligation monitoring, has processed personal data in
violation of articles 5.1 f and 32.1 of the data protection regulation.
Furthermore, it has been established that the Board of Education, although
impact assessments have been carried out on an ongoing basis when new functionalities have
added, have not met the requirements to complete an impact assessment i
in accordance with Article 35 of the Data Protection Regulation.
The Education Board in the City of Stockholm must therefore be instructed to ensure that
the processing in these parts takes place in accordance with the data protection regulation according to
following.
The Swedish Data Protection Authority instructs the education board, with the support of article 58.2 d
in the data protection regulation, to limit authorization assignments in the module
The compulsory school supervision for the people who have a need to treat
the personal data to perform their tasks in the relevant module.
The Swedish Data Protection Authority further instructs the education board, with the support of article
58.2 d of the data protection regulation, to implement a

impact assessment in the School Duty Monitoring subsystems,

The student documentation and the Home page for guardians who comply

the requirements of Article 35 of the Data Protection Regulation.

3.3 A penalty fee must be imposed

The Swedish Data Protection Authority has assessed above that the education board in the relevant

the subsystems have violated Article 5 and Article 32 of the Data Protection Regulation.

These articles are covered by article 83.4 and 83.5 respectively and in the event of a breach

of these, the supervisory authority shall consider imposing administrative

penalty fee in addition to, or in lieu of, other corrective measures.

In light of the fact that they found the violations in the subsystems

School duty monitoring, Student documentation, the Administration interface and

The start page has touched a very large number of registrants including children and

students, as well as covered shortcomings in the handling of sensitive and privacy sensitive

personal data including information about persons with protected identity,

information about health, grades, etc. it is not a question of a minor violation.

There is thus no reason to replace the sanction fee with a reprimand.

The Board of Education must therefore be subject to administrative penalty fees.

3.4 Determining the amount of the penalty fee

General provisions

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.

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 of 10

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

Violations of Article 5 are subject to the higher penalty fee according to

article 83(5), while violations of articles 32 and 35 are covered by the lower

the maximum amount according to article 83.4.

In article 83.2 of the data protection regulation, the factors to be taken into account are stated

determining the size of the penalty fee. When assessing the size of

sanction fee must, among other things, a. Article 83.2 a. is taken into account (the nature of the offence,

severity and duration), b (intent or negligence), g (categories of

personal data), h (how the violation came to the Data Inspectorate

familiarity) and k (other aggravating or mitigating factor for example

direct or indirect financial gain) in the data protection regulation.

Assessment of mitigating and aggravating circumstances

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 Article 5 is to be assessed as more serious and covered by

the higher penalty fee. For penalty fees to be effective and

deterrence, a proportionality assessment must be made in each individual case.

A personal data controller must ensure before launching a new system

appropriate security. The requirements for the personal data controller and the measures that

taken to ensure adequate safety must be set high when it is the question

about a large amount of data subjects and especially when it comes to information about

for example health and protected personal data, which means that sensitive and

privacy-sensitive personal data processing takes place.

In the current case, particular consideration has been given to the fact that the Education Board in the City of Stockholm has processed an extensive amount of personal data in the digital platform which is used in the city of Stockholm, the School Platform, and that the violations have affected data on a very large number of registered users, in any case over hundred thousand registered. The violations in question have included both privacy-sensitive and sensitive personal data concerning children that are extra worthy of protection. The violations have also resulted in unauthorized persons being able to obtain access to information about persons with protected identity. This is personal data which by its nature has a high protection value as it can get a lot serious consequences for the individual natural person if unauthorized access part of the data.

Furthermore, the following aggravating and mitigating circumstances have been considered the various subsystems that have been reviewed.

School duty monitoring

Aggravating circumstances in the module School obligation monitoring are the risks for individuals' lives caused by unauthorized persons having access to privacy-sensitive personal data concerning approximately 60 students with protected identity. Another aggravating circumstance that the inspection has taken into account is that the education board still has not fixed the authorizations in the module so that each user only has access to the data that he needs to perform his duties.

The student documentation

What have been aggravating circumstances regarding the shortcomings that have existed in the student documentation is that the technical deficiencies that this supervision

includes has allowed unauthorized access to sensitive and much

privacy-sensitive personal data concerning at least one hundred thousand students.

All registered guardians have, by in a relatively simple way

way to manipulate the system, had the opportunity to access data such as

social security number, information about students attending special schools and students' grades and

reviews. The technical deficiencies in the student documentation have from outside

the investigation in the case has been in place for a period longer than six months and

was discovered by a guardian.

As a mitigating circumstance, the Board of Education's action has to

remedy the deficiencies after the discovery has been weighed into the assessment of

the amount of the penalty fee.

Home page

The technical deficiency in the subsystem Startsidan has arisen in connection with

launch of a new functionality. What has been aggravating

circumstances are that the deficiency was discovered by a guardian and not by

the board of education. This suggests that the Board of Education has not

sufficient test procedures when launching new functionalities. As

mitigating circumstance, the inspection has taken into account that the relevant

the deficiency has existed for a short period and that the education board

rectified the defect promptly after discovery.

The administration interface

What has been aggravating is the shortcomings that existed in the subsystem

The administration interface is that the shortcomings have been able to lead to unauthorized

had access to data on approximately 50-60 employees with protected identities,

which can have very serious consequences for the individual individuals.

Other aggravating circumstances that have been weighed in the assessment of

the penalty fee is that the technical defects have existed for a period

which exceeds one year and that the education board as during November 2018

became aware that there were deficiencies in the Administration interface,

did not take action until the deficiencies were discovered again in August 2019.

Overall assessment of the size of the penalty fee

The Data Inspectorate decides based on an overall assessment that

The education board in the city of Stockholm must pay an administrative fee

sanction fee of SEK 4,000,000 (four million) for those found

the violations in the subsystems School duty monitoring, Student documentation,

The administration interface and the Start page for guardians.

This decision has been made by the director general Lena Lindgren Schelin after

presentation by lawyers Salli Fanaei and Ranja Bunni. At the final

Chief legal officer Hans-Olof Lindblom, the head of the unit, is also handling the case

Malin Blixt and the information security specialist Adolf Slama participated.

Lena Lindgren Schelin, 2020-11-23 (This is an electronic signature)

Appendix

How to pay penalty fee.

Copy for the attention of:

The Data Protection Officer for the Education Board in Stockholm City.

4. 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.