Decision

Diarienr

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 Data Protection Regulation 2016/679 against the Board of Education in the City of Stockholm

Content

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 violations

The Data Inspectorate states that the Board of Education in the city of Stockholm has

processed personal data in breach of Article 5 (1) (f) of the Data Protection Regulation1

which requires an appropriate security for personal data, including

protection against unauthorized or unauthorized treatment and in breach of Article 32 (1)

which requires the person responsible for personal data to 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 Compulsory school surveillance, during the period 25 May 2018 until

August 27, 2020, had an eligibility award that has been more

more extensive than is necessary in the light of what

each role holder needs to perform their work as well

by unauthorized persons having access to privacy sensitive

personal data concerning students with a protected identity.

in the subsystem Student documentation, 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 been privacy-sensitive / sensitive personal data.

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

in the subsystem Administration interface, during the period 25 May 2018 until 26 August 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 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).

The Data Inspectorate states that the Board of Education in the city of Stockholm, during the period 25 May 2018 until 27 August 2020, has dealt with personal data in the subsystems Compulsory school monitoring, Student documentation,

Home page for guardians and the Administration interface in violation of

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

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

freedoms and rights of persons as it is a matter of large systems, with

many children registered and with both sensitive and privacy sensitive

personal data.

Administrative penalty fee

The Data Inspectorate decides on the basis of Articles 58 (2) and 83

the Data Protection Ordinance and Chapter 6 § 2 of the Data Protection Act2 that

The Board of Education in the City of Stockholm for the violations of Article 5 (1) and

Article 32 (1) of the Data Protection Regulation shall pay an administrative fee

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

Instructions

The Data Inspectorate submits pursuant to Article 58 (2) (d) i

data protection ordinance education board to implement one as soon as possible

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

regarding the subsystems Compulsory school monitoring, Student documentation and

Home page for guardians.

The Data Inspectorate submits pursuant to Article 58 (2) (d) i

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

eligibility assignments in the module Compulsory school monitoring for only those

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

tasks.

2

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

The Data Inspectorate

DI-2019-7024

1. Report on the supervisory matter

The Data Inspectorate has through reports of personal data incidents from

The Board of Education in the city of Stockholm has been made aware of unauthorized persons

access to student information in the School Platform.

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

used in the city of Stockholm, Skolplattformen, is a city-wide

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

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

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

In the light of these reports, the Data Inspectorate has initiated the relevant case

supervision on 24 June 2019 (dnr 2019-7024) by the Board of Education

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

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

Child and student register:

-

Compulsory school surveillance

-

Inter-municipal agreements

After the supervision began, the education committee came in with more

reports of personal data incidents. In the light of the information provided

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

to extend supervision to include a review of security measures

for access to personal data under the subsystems:

-

Student documentation

Home page for guardians (Home page)

The administration interface “Contact information

teacher ”(Administration interface)

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

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

used by a limited number of users. In the module Inter-municipal agreements

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

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

Against this background, the Data Inspectorate has not examined the module in more detail

Inter-municipal agreements.

When it comes to compulsory schooling, it is a module3 in Children and

the student register, which constitutes administrative system support for

the Board of Education must be able to fulfill its obligations under the Education Act

(2010: 800). Of the received reports of personal data incidents, it has

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

classified persons. Against this background, the Data Inspectorate has

reviewed the technical measures that the board has taken to ensure one

appropriate level of security in the module. The inspectorate has also examined

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

The incoming personal data incidents regarding the subsystems

Student documentation, the Home page and the Administration interface have touched
technical deficiencies. The Data Inspectorate has therefore only examined the technical ones
measures that have been taken to ensure an appropriate level of safety in these
three subsystems.

The Data Inspectorate's review also refers to the obligation to perform one
impact assessment pursuant to Article 35 of the Data Protection Regulation in respect of the
current subsystems.

The Board of Education is responsible for 139 compulsory schools, 32 compulsory special schools, 28
upper secondary schools and six upper secondary special schools. The Data Inspectorate's current
review does not refer to adult education or preschool activities.

2. Justification of decision

2.1 Applicable provisions

The person responsible for personal data is as defined in Article 4 i
the Data Protection Regulation a natural or legal person, public authority,
institution or other body alone or together with others
determines the purposes and means of processing personal data; if
the purposes and means of processing are determined by Union law or
national law of the Member States, the controller or

3

The Board of Education has stated that compulsory schooling is both a module and its own
process area.

specific criteria for his appointment are laid down in Union law or in
national law of the Member States.

According to Article 5 (1) (f) of the Data Protection Regulation, personal data shall be processed on

a way of ensuring adequate security of personal data, including

protection against unauthorized or unauthorized treatment 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 provides that

the person responsible for personal data shall - taking into account the latest developments,

implementation costs and the nature, scope, context of the treatment

and purposes and the risks, of varying degrees of probability and severity, for

rights and freedoms of natural persons - take appropriate technical and

organizational measures to ensure an appropriate level of security in

relation to the risk. This includes, in accordance with Article 32 (1), 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, examining and evaluating

the effectiveness of the technical and organizational measures to be ensured

the safety of treatment.

Recital 74 of the Data Protection Regulation states:

Personal data controllers should be held responsible for all processing of

personal data which they perform or which is performed on their behalf.

Personal data controllers should in particular be required to take appropriate and

effective measures and be able to show that the treatment is compatible with it

Regulation, including the effectiveness of the measures. One should within these

measures take into account the nature, extent, context and

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

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. This includes in accordance with Article 35 (3)

b that an impact assessment pursuant to Article 35 (1) shall be required in particular in cases

processing takes place on a large scale of specific categories of data such as

referred to in Article 9 (1) or of personal data relating to convictions in criminal cases

and infringements referred to in Article 10.

2.2 The responsibility for personal data

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

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

personal data processing that has taken place in the subsystems Children and

student register (module) Compulsory school 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 currently 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 in preschool, primary school,

special primary school, after-school center, upper secondary school and upper secondary special school.

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

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

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

data protection legislation, such as the Data Protection Regulation. The Municipal Board

is responsible for the system meeting the requirements for security and is the system owner.

Following a decision by the council, the entire responsibility for the School Platform was transferred to

the Board of Education from 1 January 2020. This means that

The Board of Education is both a system owner and an information owner.

The Data Inspectorate's assessment

Nothing in the case contradicts the Board of Education's finding that they are relevant

processing of personal data covered by this supervision has taken place

the purpose of the Board of Education's to conduct municipal school activities.

The same also applies to the Board of Education's view 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 subsystems Children and

student register (module) Compulsory school monitoring, Student documentation, Start page

and the Administration Interface. The current supervision does not cover

personal data processing that has taken place within the framework of

preschool activities and adult education, therefore, the question falls on

the personal data responsibility for the latter processing outside the current one

supervision.

2.3 Compulsory school monitoring

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

General information about compulsory schooling

The school platform consists of six subsystems and the Children and Pupils' Register constitutes one of these subsystems. There are 101 modules in the Children and Pupil Register that are divided into eight process areas. Compulsory schooling is one of the eight the process areas in the Children and Pupil Register. The process area Compulsory schooling supports the work with compulsory schooling within municipal primary schools and regarding students in independent schools there The city of Stockholm is a home municipality. The function also includes the processes around the municipal activity responsibility. The administrative system support is used to fulfill the Board of Education's obligations regarding compulsory schooling according to the Education Act (2010: 800) as well as handling and decisions in matters linked to this (mainly according to Chapter 7 of the Education Act but also Chapter 24, Section 23). The Administrative responsibility means ensuring that students within a certain geographical area will be located at a school near the home.

The module Compulsory school monitoring processes data on 1,322 active people compulsory schooling (number of registered) of which 83 students are under seven years of age. Of These 1,322 active compulsory school guards have 60 students protected personal data.

The personal data that is processed in the current module are, among other things. a. name, address, mother tongue, school placement, guardians and contact information for these (telephone number and e-mail address) as well as history of school placement and contacts. Decisions containing personal data are also processed regarding a specific student where compulsory schooling has ceased, continued supervision (eg imposition of a fine or case with the Swedish Tax Agency), consent to fulfill compulsory schooling in another way and deferred compulsory schooling (special reasons).

The module contains information that a student goes to a resource school or

special primary school.

Technical deficiencies

On October 5, 2018, it was discovered that all users who were authorized

to the module Compulsory schooling had the opportunity to see all

classified 4 students without school placement. This deficiency is said to be due to

the system lacked logic to in the functionality of compulsory school monitoring

restrict the authority of classified persons. The reason for that is

unknown. When the module was implemented in July 2017, the Board of Education had

no knowledge of any deficiencies. Compulsory school surveillance in the city

municipal primary and lower secondary schools are based on a residential area. Privacy marked

people who are unplaced do not have a living area in the system. The routine is that

employees at schools should not be able to see these students then this processing

only happens centrally.

Number of users who could potentially have been mistaken

classified persons are 1,302. The Board is only aware that

a school administrator incorrectly viewed the information about students marked with privacy.

This must have produced three students marked with secrecy in the search results. The

there were a total of 60 students with confidentiality marking in compulsory schooling. It has

it has not been possible to obtain the exact number of users with log history

who had unauthorized access in practice because there are no specific logs

for the module Compulsory school monitoring.

When the defect was discovered on October 5, 2018, it was not verified by users

saw more information than they were authorized to see. On 5 November 2018, ie. 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 correction

which went into production on November 9, 2018.

Organizational shortcomings

Regarding the allocation of qualifications in the Compulsory School Surveillance, the board has

stated that there are eight role holders with different qualifications;

4

Gr system administrator Sthlm,

Gr Administrator Remuneration Sthlm,

Gr Look Sthlm,

Gr Administrator Language Center Sthlm,

Gr PMO-responsible Sthlm,

Privacy-marked persons refer to students with protected personal data.

9 (31)

The Data Inspectorate

DI-2019-7024

-

Article Administrator School Sthlm,

Gr Compulsory schooling Central Admin Sthlm

Gr Look Economy Sthlm.

The committee states that four5 of the eight above-mentioned role holders do not

need to have the access to compulsory schooling that they have. This is because

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

access to compulsory schooling or that it is not guaranteed that

the role only has access to the tasks required to perform

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

The Data Inspectorate's assessment

The nature of the personal data and requirements for security

The Data Inspectorate initially states that in the module

Compulsory school monitoring processes information about students, such as name, address,

social security numbers, guardians and contact information for these

(telephone 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 treated

information about students who have a protected identity. Furthermore, personal data in

some decisions are treated in the module as continued monitoring of a specific student

relating to the imposition of a fine or investigation or matter with the Swedish Tax Agency,

consent to fulfill compulsory schooling in another way (filming, Nordic

schooling or travel abroad) and deferred compulsory schooling (special reasons).

The Data Inspectorate considers that information on protected identity is extensive

worthy of protection / privacy as the risks to the data subjects' freedoms and

rights are great in the processing of this personal data. Information that a

student attends resource school or special primary school which is also treated in

Compulsory school surveillance is a sensitive personal task6 as it reveals information about

health.

In view of the nature and nature of the personal data processing which

has taken place in the compulsory schooling and the risks to the data subjects' freedoms

5

Gr Administrator Remuneration Sthlm, Gr Administrator Language Center Sthlm, Gr PMO responsible Sthlm and Gr Look Finance Sthlm.

Article 9 of the Data Protection Regulation.

and rights, the Data Inspectorate considers that high demands are placed on the technical ones and organizational measures that the Board of Education had to take to ensure an appropriate level of safety in accordance with Article 32 i the Data Protection Regulation.

Technical deficiencies

The investigation in the case shows that unauthorized persons have been able to come to privacy-sensitive personal data concerning students with protected identities. Because there is no log follow-up in the module Compulsory schooling is not possible to state the exact number afterwards users who have had unauthorized access to this data. The The technical shortage in compulsory schooling that has now been examined has meant that Potentially 1,302 users have been able to access personal data without authorization regarding 60 students with a protected identity. The reason for this depends on the board on weaknesses in the system that made the restriction of eligibility impossible to information about students with protected identities. There is no information on when the shortage occurred but the module was implemented in July 2017 and the shortage was discovered on October 5, 2018.

Organizational shortcomings

The Data Inspectorate's examination of the subsystem in question concerns both the requirements on technical and organizational measures in accordance with Article 32. Av the investigation in the case also shows that the allocation of competence in Compulsory schooling is more extensive than what is necessary in in relation to what each role holder needs to perform theirs tasks. The Board of Education has stated that a review of the eight

the eligibility roles will be initiated 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 extensive access to data in

Compulsory schooling than necessary is contrary to Article 32 (1)

the Data Protection Regulation. According to Article 32 (1), the Board of Education shall include

taking into account recent developments, implementation costs and

the nature, scope, context and purpose of the treatment and the risks of

rights and freedoms of natural persons, take appropriate technical and

organizational measures to ensure an appropriate level of security in

relation to the risk.

The Data Inspectorate assesses that an appropriate security in this case includes one

ability to continuously ensure the confidentiality of treatment systems

and services. By the board has allocated more extensive

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 Board of Education has failed in its 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 of adequate security also includes having a procedure for

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

organizational measures taken to ensure the safety of treatment

which has not been the case here either. The Data Inspectorate finds that

if the Board of Education had had such a procedure to regularly

test, examine and evaluate the effectiveness of the measures taken

the board was able to ensure / discover whether the technical measures are correct

in accordance with the organizational measures taken. As for it

the lack of organization (the extensive competence) is also according to

The Data Inspectorate's assessment of such a deficiency in the restriction of competence

which should have been discovered if the Board of Education had regularly

checked the authorization. This too is a shortcoming in the requirements for appropriate security

pursuant to Article 32 (1) of the Data Protection Regulation.

The Board of Education in the City of Stockholm has summarized

personal data in the module Compulsory school monitoring in the School Platform in violation of

Article 32 of the Data Protection Regulation.

The Data Inspectorate also assesses that the Board of Education has processed

personal data in breach of Article 5 (1) (f) of the Data Protection Regulation thereof

current subsystem. This is because the board has not ensured a suitable one

security of personal data, including protection against unauthorized or unauthorized use

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.

There are a total of 464,611 registered in the Student Documentation subsystem, of which

122,699 are students in municipal primary and secondary school. Of these students
has 787 protected personal data. There are 233,066 in this subsystem
registered guardians and 34,756 employees (some of these employees
works in childcare and adult education not covered by
supervision).

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

Technical deficiencies

On August 21, 2019, it was discovered via a thread on Twitter that a guardian
had discovered a data leak in the Student Documentation. The person behind
The Twitter account has analyzed with its own access and login via Bank ID
the traffic and calls between the front-end and back-end systems.7 The person has
then took out parts of these calls and manipulated them in order to do so
get over other people's information.

7

The terms are used by the Board of Education in the city of Stockholm and their function can
generally described as follows. The separation of front end and back end system simplifies
the data process when it comes to multilayer development and maintenance of computer systems. One
front-end systems are mainly used to send questions and requests and receive data from
the backend system. It allows users to interact and use one
information system. Usually, 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
user interface (GUI) and / or a front-end 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 obtained from databases and
data processing components.

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

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

All registered guardians in the School Platform have because of it
current shortage had the opportunity to unauthorized access to information. According to
the Board of Education, a person has taken advantage of this opportunity and done
paging of 101 unique people. The shortcoming has existed since the subsystem

was launched. The module where the shortage existed has been in operation since 26 October 2018. This deficiency had not been captured in previous function and safety tests before the function was put into production.

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

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 components (graphical user interface), as well as for a program to request and provide services from another program.

9 Individual development plan.

The Data Inspectorate's assessment

Security requirements

The Data Inspectorate initially states that in the subsystem Student documentation in the School Platform is extensive personal data processing involving thousands of students, guardians and teacher.

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

As mentioned above, sensitive personal data is further processed

health when examining admission to the special primary school, special school,

upper secondary special school, and special education for adults according to 7, 18 and 21

Cape. the Education Act. Even an indication that a student is attending such a school is one

sensitive task.

The Data Inspectorate further states that in the subsystem Student documentation

data relating to students' health are treated as data contained in

various inquiries about students, special adaptations, etc. Also information on

that some students go to a special school involves the treatment of sensitive

personal data.

In addition, extensive personal data processing is added in

The student documentation that does not constitute sensitive personal data according to

the Data Protection Regulation but is to be regarded as extra privacy sensitive such as

information relating to assessments and data from development interviews.

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

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

the risks to the data subjects' freedoms and rights, the Data Inspectorate considers

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

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

the Data Protection Regulation.

Assessment of technical measures

The technical shortcoming in the Student Documentation that is now being examined 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 not
would be available became available. According to the Board of Education
information could be accessed by unauthorized persons, e.g. a. other people's first name,
last name, social security number, type of school (eg special primary school), year, school ID,
class and students' assessments from the module development talks. This technical
shortage has meant that all registered guardians in the School Platform
has had the opportunity to unauthorized access to information about all registered
students, including sensitive and privacy-sensitive information concerning
students.

The Data Inspectorate notes that the technical security measures that have
taken in the subsystem The student documentation in the School Platform has been
deficient as unauthorized persons have been able to easily access
comprehensive sensitive and privacy-sensitive personal data concerning
thousands of students. The Board of Education has thus breached its obligation
pursuant to Article 32 (1) of the Data Protection Regulation, taking into account the latest
development, implementation costs and the nature, scope of treatment,
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 which is now being examined in the subsystem
According to the Swedish Data Inspectorate's assessment, the student documentation should have
detected at an early stage, before the processing of personal data
was started. The Data Inspectorate considers that an appropriate security in this case
includes an ability to continuously ensure the confidentiality of
treatment systems and services.

The requirement of adequate security also includes having a procedure for

regularly test, examine and evaluate the effectiveness of the technical

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

current technical deficiency was discovered by a guardian long after

subsystem The student documentation was launched, shows that the Board of Education

neither has ensured to continuously ensure confidentiality in this

subsystem or had a procedure for regularly testing, examining and

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

meets the requirements of the Data Protection Regulation. The Data Inspectorate finds that

this too is a shortcoming in the requirements of appropriate security under Article 32 (1) (i)

the Data Protection Regulation.

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

personal information in the Student Documentation which is part of the School Platform in

in breach of Article 32 of the Data Protection Regulation.

The Data Inspectorate also assesses that the Board of Education has processed

personal data in the subsystem in question in breach of Article 5 (1) (f)

the Data Protection Regulation. This is because the board has not secured one

appropriate security for personal data, including protection against unauthorized or

illicit treatment through the use of appropriate technical measures.

2.5 Home page

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

General about the Home page

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

in the subsystem The start page is called "contacts" where personal information from School 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 guardians and children / pupils and children / pupils connection to classes / groups. This is controlled based on information in Children and student register.

Among the personal data processed in the Home Page are students and teachers name, e-mail address, school connection, connection to groups, connection to departments, mentor groups and courses. Data on is also processed guardian's name, social security number, address, e-mail address, telephone number and connection to children.

In the subsystem Start page, there are a total of 440,695 registered, of which 31,847 are employees, 233,062 guardians and 122,699 students in municipal primary and lower secondary school and high school.

Technical shortage

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

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

The technical deficiency was remedied on the day it was discovered, on 24 August 2019, through a code change that was produced.

The Data Inspectorate's assessment

Security requirements

The Data Inspectorate initially states that in the subsystem Start page in The school platform provides extensive personal data processing that concerns 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 view of the scope of the personal data processing that takes place in the home system subsystem, the nature and nature of the treatments and the risks to them The data inspectorate's freedoms and rights are considered by the Data Inspectorate to be of high demands the technical measures to be taken to ensure an appropriate security level in accordance with Article 32 of the Data Protection Regulation.

The assessment of technical measures

The technical shortcoming in Startsidan, which is now being examined, has meant that guardians by changing calls in the developer tool in their browser with the help of social security numbers could search for other guardians who are registered on the Home page. This means that guardians have on one easily accessed by other guardians without authorization personal data. The Board of Education has thus breached its obligation

pursuant to Article 32 (1) of the Data Protection Regulation, taking into account the latest development, implementation costs and the nature, scope of treatment, 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 subsystem in question.

The Data Inspectorate assesses that an appropriate security in this case includes one ability to continuously ensure the confidentiality of treatment systems and services. The current technical shortage should according to The Data Inspectorate's assessment has been discovered at an early stage before the processing of personal data began. That the current shortage was discovered by a guardian after the startup subsystem was launched, shows that the Board of Education did not have a satisfactory procedure either the requirements of the Data Protection Regulation to regularly test, examine and evaluate the effectiveness of the technical measures taken. This too is lack of appropriate security requirements under Article 32 (1) of the Data Protection Regulation.

The Board of Education in the City of Stockholm has thus considered personal data in the subsystem in question in breach of Article 32 i the Data Protection Regulation.

The Data Inspectorate further assesses that the Board of Education in the city of Stockholm has processed the personal data in the current subsystem in violation of the article 5.1 f in the Data Protection Ordinance because the board has not secured one appropriate security for personal data, including protection against unauthorized or illicit treatment.

2.6 The administration interface

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

General information about the Administration Interface

The administration interface was common to the two subsystems

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

subsystems are executed. The system read data from the Children and Pupil Register which is

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

this interface and was then shown to users in various interfaces

based on the role of the system and depending on the settings made.

The administration interface was not intended for guardians. People with

a combination of roles such as teacher or chancellor who is also

guardians had no access to the information linked to the role

guardian when logging in to 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 connection

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

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

valid / invalid) and the application for leave.

Technical deficiencies

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

found links to log in 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 "Contact information teachers"

where name, e-mail address and work telephone number are displayed. Further has

the interface has not been found to be adapted for handling confidential information

tasks. Individuals with protected identities have not had a marking as

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

covered by the current deficiency, but that these can not be distinguished from the others

registered.

The shortcoming has existed since the function was launched, probably since August 2017.

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

the Board of Education be trivial because the inquiry then claimed that

no data that guardians could not see in another interface

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

was then said to only show the student's current teacher and what subjects they have with them

eleven. It was also said that no contact details were shown. The shortage would be solved

with a code merger which was then planned in 2019. The release as

the correction would be covered by early 2019, however, is postponed to the future.

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

contact information for teachers, such as name, class, school, subject / course, email address (both work and private address)

and telephone number (both work and private numbers).

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

interface and incorrectly accessed data. It is also not possible to get it

how many of the teachers covered by the reports also had their private e-mail address entered in the Children and Pupils'

Register and which could thus be shown to

unauthorized. The Board of Education can not state the number of registered as

was affected by this technical deficiency. At present, there are between 50 and 60 teachers

which have a protected identity in this subsystem. The Board of Education can not

nor appreciate what the current shortage has meant for the data subjects

as the board has not received any indications of consequences.

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

city on 26 August 2019 that the supplier would close the access for

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

The Data Inspectorate's assessment

Security requirements

The Data Inspectorate initially states that in the Administration Interface

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

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

data on teachers with protected identities were also processed.

The Data Inspectorate considers, as previously mentioned, that information concerning persons

with protected identities are very worthy of protection / privacy then the risks

for the freedoms and rights of the data subjects are great in the treatment of these

personal data. Given the nature and nature of the

personal data processing that has taken place in the Administration Interface and

the risks to the data subjects' freedoms and rights, the Data Inspectorate considers

that high demands be placed on the technical measures to be taken to

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

the Data Protection Regulation.

The assessment of technical measures

In the Administration interface, guardians have via Google search

been able to find links for logging in to the Administration Interface there
guardians should not be able to log in. In this interface have guardians
been able to produce information on e.g. a. teachers' private contact details such as
email address and private phone numbers. This interface has also been proven
not be adapted for handling data on individuals with protected

identity. This means that unauthorized persons have been able to access
information on persons with a protected identity.
Because the current shortage has meant that unauthorized persons have had
possibility to access information about persons with a protected identity
the Board of Education has breached its obligation under Article 32 (1) (i)
the Data Protection Regulation that, taking into account recent developments,
implementation costs and the nature, scope, context of the treatment
and purposes and the risks to the rights and freedoms of natural persons
appropriate technical measures to ensure an appropriate level of safety in
relation to the risk.
The Data Inspectorate assesses that an appropriate security in this case includes one
ability to continuously ensure the confidentiality of treatment systems
and services. The current technical shortage should according to
The Data Inspectorate's assessment has been discovered at an early stage before
the processing of personal data began. The mentioned shortcoming has
has been around for a long time since the system was launched.
The Board of Education was made aware of the shortcoming in November 2018,
but chose not to remedy it until the deficiency was rediscovered in August

2019. The Board of Education has thus breached the necessity of

continuously ensure confidentiality in the current interface. The requirement of

Appropriate security also includes having a procedure to regularly

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

measures to ensure the safety of treatment which neither has

in this case in the light of the foregoing.

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

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

the Data Protection Regulation.

The Data Inspectorate also assesses in this part that the Board of Education has

processed personal data in the relevant interface in violation of Article 5 (1) (f)

the Data Protection Ordinance because the board has not ensured an appropriate

security of personal data.

2.7 Impact assessment

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

The Board of Education states that since the Children and Pupil Register

put on production before 25 May 2018 has no comprehensive

impact assessment under Article 35 of the Data Protection Regulation yet

implemented. However, impact assessments have been carried out continuously

as new functionalities have been added.

The committee believes that an impact assessment needs to be made and work on

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

detected during penetration tests has been promptly remedied.

The Board of Education has further stated that it is working with one
risk management plan, where what is discovered in risk and impact assessments
be addressed systematically in accordance with the city's risk matrix and that objective
is that there will soon be active risk management for the whole
The school platform. The Board of Education has a developed process for that
ensure adequate information security that involves risk and
impact assessments shall be carried out
Regarding the Administration Interface, there will be no impact assessment
to be done for this part because the interface has been discontinued and is no longer in
use.

The Data Inspectorate's assessment

In the subsystems and modules that have been the subject of the Data Inspectorate
review treats students, school staff and guardians
personal data of varying degrees of sensitivity. The current subsystems covered
of the supervision in question involves the treatment of a large number
personal data of a large number of data subjects, who are largely children, who in
the Data Protection Regulation is highlighted as vulnerable natural persons10.
The Data Inspectorate notes that the subsystems in question are extensive
personal data processing with different types of personal data such as grades,
inquiries about students, development talks, special adaptations, children and
adults with protected identities. Furthermore, sensitive people are also treated
personal data to a certain extent, ie. specific categories of data such as
referred to in Article 9 (1) as health information. It is thus a question of one

10
See recital 75 of the Data Protection Regulation.

extensive personal data processing if a large number of registered in

the system.

The Data Inspectorate states that it is a question of a treatment as with

consideration of its nature, scope, context and purpose is likely to lead

to a high risk to natural persons rights and freedoms in such a way

which requires that the Board of Education should have implemented one

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

35.3 (b) further states that an impact assessment under paragraph 1 in particular

shall be required in the case of large-scale treatment of special

categories of data referred to in Article 9 (1). The Data Inspectorate states

that the processing of personal data in the relevant subsystems is of it

the nature referred to in Article 35 (3) (b) of the Data Protection Regulation, which is a

circumstance which in particular requires an impact assessment.

The Data Inspectorate has, on the basis of guidelines from the Article 29 Working Group and the criteria developed by the

group11, adopted a

list of when an impact assessment is to be made.12

In addition to the situations referred to in Article 35 (3) of the Data Protection Regulation, and

taking into account the derogation in Article 35 (10), an impact assessment shall

regarding data protection is made if the planned processing meets at least

two of the nine criteria mentioned in the list.

In this case, sensitive data or data is processed by a lot

personal character, large-scale data and vulnerable data

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 regulatory authority or a data protection officer in accordance

11

Guidelines on data protection impact assessment and determination of whether

the treatment "is likely to lead to a high risk" within the meaning of 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, no. DI-2018-13200

2 4 (31)

The Data Inspectorate

DI-2019-7024

with Article 20 of Directive 95/46 / EC and the implementation of which has not changed

since previous control. As a good practice, however, one should

Impact assessment is reviewed continuously and evaluated regularly.

The Data Inspectorate finds that there is no circumstance that

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

specify that even if an impact assessment is not required on 25 May

In 2018, it is necessary for the person responsible for personal data to perform one

impact assessment, at an appropriate time and as part of its

general liability.13

The Data Inspectorate states that the processing of personal data takes place

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

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

impact assessment under Article 35 of the Data Protection Regulation

implemented in the respective subsystems covered by this supervision, in order to:

assess the consequences of the planned treatment for the protection of

personal data in accordance with Article 35.

The fact that the system was launched before 25 May 2018 does not affect

the assessment of the inspectorate. 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 performed.

In the current review, the Data Inspectorate has assessed that it has existed

technical deficiencies in several subsystems covered by the supervision. The inspection has

also assessed that the eligibility allocations have been more extensive in it

the module where the issue has been examined (Compulsory school monitoring). Against the background of

the Board of Education's own information that has emerged in the case in question

impact assessment, the Data Inspectorate considers that the Board of Education,

during the period 25 May 2018 until 27 August 2020, has not implemented one

impact assessment covering the compulsory schooling subsystems,

Student documentation, Home page and the Administration interface in its

whole. If the board had made a complete impact assessment, so

the deficiencies found could probably have been avoided. The Board of Education

has thus not carried out an impact assessment that meets the requirements of

Guidelines on data protection impact assessment and determination of whether

the treatment "is likely to lead to a high risk" within the meaning of the Regulation

2016/679, last revised and adopted on 4 October 2017, WP 248 rev. 01. 2 (6) pp. 1516

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Article 35 of the subsystems concerned and has thus dealt with

personal data in violation of the current provision.

Choice of intervention

3.1 Possible intervention measures

The Data Inspectorate has a number of corrective powers available according to

Article 58 (2) (a) to (j) of the Data Protection Regulation, inter alia, to impose it

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

Regulation and if required in a specific way and within a specific period.

Of point (i) of Article 58 (2) and Article 83 (2) of the Data Protection Regulation

it appears that the Data Inspectorate has the authority to impose administrative

penalty fees in accordance with Article 83. Depending on the circumstances of

in 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) sets out the factors to be taken into account in deciding that:

administrative penalty fees shall be imposed and in determining

the size of the fee.

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

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

issue a reprimand in accordance with Article 58 (2) (b) (i)

the Data Protection Regulation. Account must be taken of aggravating and mitigating

circumstances of the case, such as the nature of the infringement, the degree of difficulty and

duration and previous infringements of relevance.

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.

3.2 Order

The Data Inspectorate has found that the Board of Education in the city of Stockholm,

by having a more extensive allocation of competencies than necessary in

the subsystem / module Compulsory school monitoring, has processed personal data in

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 continuously as new functionalities have

has not met the requirements for carrying out an impact assessment in

in accordance with Article 35 of the Data Protection Regulation.

The Board of Education 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 Data Inspectorate submits to the Board of Education, on the basis of Article 58 (2) (d)

in the Data Protection Regulation, to limit authorization allocations in the module

Compulsory school supervision for those people who have a need for treatment

the personal data to perform their tasks in the current module.

The Data Inspectorate also submits to the Board of Education, with the support of an article

58.2 d of the Data Protection Regulation, to implement one as soon as possible

impact assessment in the compulsory schooling subsystems,

The student documentation and the start page for guardians who meet

the requirements of Article 35 of the Data Protection Regulation.

3.3 A penalty fee shall be imposed

The Data Inspectorate has above assessed that the Board of Education in the relevant

subsystems have infringed 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 an infringement

of these, the supervisory authority shall consider imposing administrative

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

In view of the fact that they identified infringements in the subsystems

Compulsory school monitoring, student documentation, the administration interface and

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

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

personal data including data on persons with a protected identity,

health information, grades, etc. it is not a matter of a minor infringement.

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

The Board of Education shall thus be subject to administrative sanction fees.

3.4 Determining the size of the penalty fee

General provisions

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.

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 a maximum of 10

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

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

Article 83 (5), while infringements of Articles 32 and 35 are covered by the lower

the maximum amount in accordance with Article 83 (4).

Article 83 (2) of the Data Protection Regulation sets out the factors to be taken into account in

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

sanction fee shall, among other things. a. account is taken of Article 83 (2) (a) (nature of the infringement,

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

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

knowledge) and k (another 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 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 Article 5 is to be judged as more serious and covered by

the higher penalty fee. In order for penalty fees to be effective and

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

A person responsible for personal data must ensure before launching a new system

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

taken to ensure adequate security must be set high when it comes to the issue

about a large number of data subjects and especially when it comes to data on

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

privacy-sensitive personal data processing takes place.

In the present case, special consideration has been given to the Board of Education in the City of Stockholm has processed an extensive amount of personal data in the digital platform used in the city of Stockholm, Skolplattformen, and that the violations have concerned data on a very large number of data subjects, at least above one hundred thousand registered. The current violations have included both sensitive and sensitive personal data concerning children who are extra worthy of protection. The violations have also meant that unauthorized persons have been able to obtain access to data on persons with a 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 sheep part of the data.

Furthermore, the following aggravating and mitigating circumstances have been weighed into the various subsystems that have been examined.

Compulsory school surveillance

Adverse circumstances in the module Compulsory schooling are the risks for individuals' lives caused by unauthorized access to privacy-sensitive personal data concerning approximately 60 students with protected identity. Another aggravating circumstance that the inspectorate has taken into account is that the Board of Education has still not addressed the qualifications in module so that each user only has access to the data provided he needs to perform his duties.

The student documentation

What have been aggravating circumstances regarding the shortcomings that have found in the Student Documentation is that the technical shortcomings of this supervision

covers have enabled unauthorized access to sensitive and much

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

All registered guardians have, by on a relatively simple

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

social security numbers, information about students attending special school and students' grades and

reviews. The technical shortcomings in the Student Documentation have outside

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

was discovered by a guardian.

As an attenuating circumstance, the Education Board's actions have to

remedy the shortcomings after the discovery has been weighed in the assessment of

the size of the penalty fee.

Home page

The technical deficiency in the subsystem The start page has arisen in connection with

launch of a new functionality. That which has been aggravating

circumstances is that the defect was discovered by a guardian and not by

the Board of Education. This indicates that the Board of Education does not have

sufficient test seduction when launching new functionalities. As

mitigating circumstance, the inspectorate has taken into account the current

the shortage has existed for a short period and that the Board of Education

remedied the deficiency promptly after the discovery.

The administration interface

What has been aggravating regarding the shortcomings that have existed in the subsystem

The administration interface is that the shortcomings could have led to unauthorized persons

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

which can have very serious consequences for the individual.

Other aggravating circumstances that have been taken into account in the assessment of

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

which exceeds one year and that the Board of Education as in November 2018

was made aware of the shortcomings of the Administration Interface,

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

Overall assessment of the size of the penalty fee

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

The Board of Education in the city of Stockholm must pay an administrative fee

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

the violations in the subsystems Compulsory school monitoring, Student documentation,

The administration interface and the Home page for guardians.

This decision was made by the Director General Lena Lindgren Schelin after

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

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

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 information to:

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

4. 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.