The police authority

Sent by email only

registrar.kansli@polisen.se

Diary number:

DI-2020-2719

Your diary number:

A126.614/2020

Date:

2021-02-10

Decision after supervision according to

the crime data act – the police authority

use of Clearview AI

The Privacy Protection Authority's decision

The Privacy Protection Authority states that the Police Authority has processed

personal data in violation of ch. 2 § 12 and ch. 3 Section 2 and Section 7, first paragraph

the crime data act by using the Clearview AI application during the autumn period

2019 through March 3, 2020.

The Privacy Protection Authority decides with the support of ch. 6. Section 1 of the Criminal Data Act that

The police authority must pay a sanction fee of 2,500,000 (two million five hundred

thousand crowns.

The Privacy Protection Authority instructs the Police Authority according to ch. 5 Section 7 first

paragraph 2 of the Criminal Data Act to take educational and other organizational measures

measures required according to ch. 3 Section 2 of the Criminal Data Act to ensure that the routines

which exists reaches the entire organization and that the authority can thus show and

ensure that all processing of personal data is constitutional. The actions must have

taken no later than September 15, 2021.

The Privacy Protection Authority orders with the support of ch. 5. Section 7 first paragraph 2

the crime data act, the police authority that according to ch. 4 Section 2 of the Criminal Data Act inform them

registered, whose personal data the Police Authority entered into Clearview AI, in it

extent the obligation to provide information is not limited according to ch. 4 Section 5

the crime data act. The information must have been submitted no later than September 15, 2021.

The Privacy Protection Authority orders with the support of ch. 5. Section 7 first paragraph 2

the crime data act The police authority to take possible and relevant measures so that they

personal data entered by the Police Authority into Clearview AI is deleted from it

the application. Such measures must have been taken by September 15, 2021.

Mailing address:

Box 8114

104 20 Stockholm

Website:

www.imy.se

E-mail:

imy@imy.se

Phone:

08-657 61 00

Account of the supervisory matter

The Norwegian Data Protection Authority (IMY), formerly the Data Protection Authority, was noticed in

February 2020 through information in the media that law enforcement authorities in Sweden

could have used the Clearview AI application. IMY launched against the background of
the data immediately an examination where the Police Authority was asked to answer about
the authority used the application and with what legal support processing in so
case happened. Statements from the Police Authority in the spring of 2020 showed that
the application has been used by some employees within the authority on a number of occasions without
that the authority provided the application to the employees. IMY therefore initiated a
in-depth review of the Police Authority's use of Clearview AI.

Clearview AI is an application provided by an American company that offers
a facial recognition service where the user, after downloading the application on
a digital device, uploads an image which is matched by biometrics against a very large one
number of images scraped from the open internet.1 The user then gets a result i
form of a number of web addresses where possible matches are found.2

The police authority's use of the Clearview AI application

The police authority has stated that the application Clearview AI was used in a number of cases
occasions during the period autumn 2019 up to and including 3 March 2020.
They are employees at the National Operative Department (NOA) and region South
who have used Clearview AI. At NOA, the application has been used by a total of six
employees, five of whom used the application in operational activities, i.a. in order to
identify plaintiffs in suspected sexual crimes against children as well as in intelligence activities to try to identify unknown
persons when investigating serious
organized crime. At police region South, the application has been used in investigations
of sexual crimes against children and tested by employees against images in the Police Authority
so-called OBS portal.3 When the Police Authority's use of Clearview AI became known
through information in the media, the authority's data protection officer came out with a
recommendation that the National Forensic Center and NOA should clarify and
spread that such use was not permitted.

Justification of the decision

The police authority's responsibility for employees' treatment of

personal data within law enforcement activities

The police agency is a large organization with a special mission to enforce the law

and order. The police authority is also governed by clear legislation regarding how

personal data must be processed, especially within law enforcement activities.

The large amount of personal data, including sensitive data, that the authority processes

as well as the far-reaching powers the Police Authority has means that the authority has

a special responsibility for personal data being processed correctly.

The web service states that they collected three billion facial images from Facebook, YouTube and millions of others

websites. IMY report 2021:1; Privacy protection report 2020 - reporting of developments in the IT area when it

applies to privacy and new technology, p. 70.

2 https://clearview.ai, 2020-11-25.

3 IT support within the Police Authority where intelligence information is relayed to law enforcement.

The police authority, as the personal data controller, is responsible for all

personal data processing that takes place under the authority's management or at

on behalf of the authority according to ch. 3 Section 1 of the Criminal Data Act. This means that all

personal data processing carried out at the authority falls under that of the Police Authority

personal data responsibility, including the processing of personal data assistants, employees,

persons who are to be equated with employees (eg hired personnel) or

contractor performs.4 Also of ch. 2. Section 1 of the Act (2018:1693) on police treatment

within the area of the Criminal Data Act (PBDL) it appears that the Police Authority is responsible for the personal data processing carried out by the authority. That means it is

The police authority's obligation to ensure that all processing that takes place within the authority has i.a. a legal basis, a legitimate purpose and that sufficient protective measures are in place through appropriate technical and organizational measures. The police authority shall ensure that there are clear guidelines and routines regarding the IT tools used by the employees may use and that the employees are sufficiently trained and informed about how personal data may be processed.5

According to the Swedish Police Agency, there are a few employees who used Clearview AI without the authority provided the application to the employees. However, the treatment has taken place when performing the employees' tasks at the authority. The treatment has also carried out with personal data taken from current investigations and at the majority of occasions during ongoing criminal investigations, i.e. during exercise of authority. That it happened without the authority providing Clearview AI or approved the use of the IT tool, the Police Authority does not thereby deprive it responsibilities that the authority has as a personal data controller.

IMY states against this background that the Police Authority is responsible for them employees' processing of personal data when using Clearview AI.

The police authority's obligation to through technical and organizational measures ensure and show that the authority's personal data processing is constitutional

As the person in charge of personal data, the Police Authority has according to ch. 3 Section 2 of the Criminal Data Act an obligation to, through technical and organizational measures, ensure and be able to demonstrate that the authority's processing of personal data is constitutional and that it data subject's rights are protected. It must be assessed in each individual case which ones measures that are needed taking into account e.g. which personal data is processed.6

Organizational measures can e.g. be adopting internal strategies for data protection,
inform and train employees and ensure a clear distribution of responsibilities.7 Actions
that can be taken to show that the processing is constitutional can e.g. be
documentation of IT systems, treatments and measures taken, etc.8
In the matter, the police authority has submitted an internal routine for processing personal data
within the authority. Any additional guidance document for the employees' treatment of
personal data has not been submitted. Nor any basis regarding how education of
employees or how the internal routine should reach the entire organization has been submitted or
accounted for. There is also no information that any education or equivalent
activity has actually been carried out within the authority. That employees at two different

Prop. 2017/18:232 pp. 171 f., 319 and 452.

See further below under the heading The Police Authority's obligation to through technical and organizational measures
ensure and demonstrate that the authority's personal data processing is constitutional.

6 Prop. 2017/18:232 p. 172 f.

7 Sandén, H-O, 2019, SFS 2018:1177 Legal commentary, Norstedt's law.

8 Prop 2017/18:232, p. 453.

organizational units used Clearview AI in violation of current regulations shows
that the routine did not have sufficient impact within the authority. The police authority has courage
this background has not been able to demonstrate that there are sufficient organizational measures, i
form of e.g. internal strategies or training, in place to ensure that

the treatment is constitutional.

IMY states that the Police Authority has not taken appropriate organizational measures

measures to ensure and be able to demonstrate that the authority's treatment of

personal data has been constitutional. The police authority has thus transgressed

3 ch. Section 2 of the Criminal Data Act.

The police authority's processing of biometric data i

in connection with the use of Clearview AI

According to the Police Authority's information, images of people, which were then converted into

biometric data, in ongoing operational matters read into Clearview AI at one

several occasions.

The police authority has not explained how the biometric data that was read into the

Clearview AI is processed in the application, e.g. if and if so how long the data

is saved, how the matching of biometric data is done, if the data is transferred to

third countries or if the data is disclosed to others in connection with use. The

is due, according to information from the Police Authority, to the fact that there are no legal assessments

done prior to the use of Clearview AI.

Biometric personal data is sensitive personal data and according to ch. 2 Section 12

The Criminal Data Act is only processed if it is specifically prescribed and absolutely necessary

for the purpose of the treatment. Of ch. 2 § 4 PBDL states that the Police Authority

may process biometric data if the use is absolutely necessary for

the purpose of the treatment.

The use of a service such as Clearview AI means that individuals' biometric

personal data is matched against large amounts of personal data that have been collected unfiltered

from the open internet. According to IMY's assessment, a law enforcement agency's

processing of personal data when using such a service probably not

meet the strict requirement of necessity that follows from the Criminal Data Act and that

the underlying crime data directive.9 The European Data Protection Board has expressed

for a similar view.10

The processing of biometric data that took place when used by the Police Authority

by Clearview AI has been carried out without any control or knowledge from the Police Authority

about how the data is handled by Clearview AI. Any assessment of the treatment

been absolutely necessary according to ch. 2 Section 12 of the Criminal Data Act has not happened. Through it

information submitted in the case, the Police Authority has not shown that the authority's

processing of biometric data in the Clearview AI service has been absolutely necessary for

the purpose of the treatment.

Article 10 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of physical

persons with regard to the processing of personal data by competent authorities in order to prevent, prevent, investigate, disclose or prosecute crimes or enforce criminal penalties, and the free flow of such information and about

repeal of the Council's framework decision 2008/977/RIF.

10 EDPB response to MEPs Sophie in 't Veld, Moritz Körner, Michal Šimečka, Fabiene Keller, Jan-Christoph Oetjen, Anna Donáth, Maite Pagazaurtundúa, Olivier Chastel, concerning the facial recognition app developed by Clearview AI.

IMY states that the Police Authority's processing of biometric data has taken place in

conflict with ch. 2 Section 12 of the Criminal Data Act.

Obligation to carry out an impact assessment

According to ch. 3 Section 7, first paragraph of the Criminal Data Act, a personal data controller is obliged to

carry out a consequence assessment before starting a new treatment that can

is assumed to entail a particular risk of infringement of the data subject's personal integrity.

It is clear from the preparatory work for the crime data act and the underlying crime data directive

that when assessing whether an impact assessment is needed, the treatment

scope, nature, context and species are taken into account. Particular attention must be paid to the treatment

includes any new technology.11

The personal data that has been processed in the application is biometric data and

these may, as reported above, only be processed if it is specifically prescribed and

absolutely necessary with regard to the purpose of the treatment. Since

the use of Clearview AI has involved the processing of biometric data, which

includes facial recognition, with new technology provided by an external player i

third country, the processing may be assumed to have entailed a particular risk of infringement

data subject's personal privacy. An impact assessment would therefore have

completed before the treatment was started. The use of the Clearview application

However, AI was started without any legal considerations or consideration of risks

breach of the data subjects' personal privacy took place.

The police authority has not used the application systematically in its operations and

the application has not been recommended by the authority. As IMY stated above is

however, the Police Authority is responsible for the treatment carried out by employees during use

by Clearview AI. The lack of organizational measures has resulted in employees using

the application without first carrying out an impact assessment, despite the fact that

required according to ch. 3 Section 7 of the Criminal Data Act.

IMY states that the Police Authority, contrary to ch. 3 Section 7 first paragraph

the Criminal Data Act failed to carry out an impact assessment before use

by Clearview AI.

Choice of intervention

Of ch. 5 Section 7 of the Criminal Data Act follows the corrective powers IMY has at its disposal

violations of said law. These consist of i.a. injunctions, prohibitions against

processing and issuance of a penalty fee.

Of ch. 6 §§ 1 and 2 of the Criminal Data Act follows that IMY can issue a sanction fee at

violation of i.a. the provisions in ch. 2 § 12 and ch. 3 Sections 2 and 7

the crime data act. The penalty fee must meet the requirements set out in the crime data directive

that sanctions must be proportionate, dissuasive and effective. 12

When assessing whether a penalty fee should be levied and the size of the penalty fee

special consideration must be given to the circumstances specified in ch. 6. Section 4 of the Criminal Data Act,

i.e. if the violation was intentional or due to negligence, the damage, danger or

11

12

Prop. 2017/18:232 p.181 f.

Prop. 2017/18:232 p. 309 f.

violation that the violation entailed, the nature of the violation, degree of severity and

duration, what the personal data controller or personal data assistant did to

limit the effects of the breach, and if the personal data controller or

the personal data assistant was previously required to pay a penalty fee.

IMY states that the Police Authority failed in several respects in its

personal data responsibility when using Clearview AI. The police authority has not

taken sufficient organizational measures to ensure and be able to demonstrate that

the processing of personal data in the current case has been constitutional, processed

biometric data in violation of the Criminal Data Act and failed to implement a

impact assessment.

As IMY stated above, this means that the Police Authority processed

personal data in violation of ch. 2 § 12 and ch. 3 Section 2 and Section 7, first paragraph

the crime data act.

It has not been possible to investigate whether the data subjects suffered any actual damage

Police use of Clearview AI. However, this is not decisive for whether

penalty fee must be charged, without the fact that there is a risk of damage is according to

the preparatory work enough for this.13 Through the use of Clearview AI, employees have

at the Police Authority gained access to privacy-sensitive information about a large number

registered. The European Court of Justice has stated that access to large amounts of personal data

by an authority must be seen as a special infringement, regardless of whether the individual suffered any

damage from the processing or not.14 Also the information entered by the Police Authority

the application has been of a privacy-sensitive type and it has not been possible to clarify what

what happened to this personal data after the input. Due to what now

stated, IMY assesses the risk of harm to the data subjects as high in the current case.

The police authority has processed personal data without legal considerations and without

any control over or assessment of the processing's intrusion into individuals' personal

integrity. Regarding the use of Clearview AI, the Police Authority has not been able to

give an account of what happened to the personal data entered by the authority

the application and with the result obtained. It can be assumed that the data

which is entered into the application is often covered by some form of confidentiality, e.g. 35 ch.

Section 1 of the Publicity and Confidentiality Act (2009:400), and the Police Authority has not

presented any confidentiality-breaking basis that could justify disclosure of

the data. These circumstances mean that there are reasons to take a serious look

the violations.

The extent and duration of the treatment must also be taken into account

the determination of the amount of the penalty fee. A mitigating circumstance is that it

only a few are registered whose personal data has been shared with Clearview AI.

However, the use of Clearview AI has taken place over a period of a few months,

and only ceased after the Swedish Privacy Agency's review began.

In addition, through the use of Clearview AI, the Police Authority has gained access to

a large number of personal data and it is unclear how long they entered

the personal data and the data obtained through the matching have been processed.

Furthermore, it may be considered aggravating that the data of the registrants has been matched against one

application with personal data from the entire open internet and that

The police authority has no knowledge of what happened to the information that

13

14

Prop. 2017/18:232 p. 483.

Judgments of the European Court of Justice in cases C-594/12 paragraph 35 and C-623/17 paragraph 70.

entered. The fact that it was biometric, i.e. sensitive personal data, such as

has been processed and the fact that the data has been used for facial recognition also means that it

there are reasons to take the violation seriously. 15

In summary, the reported circumstances result in a penalty fee

must be levied and that a relatively significant penalty fee is justified.

The size of the penalty fee

According to ch. 6 § 5 of the Criminal Data Act, a penalty fee may be reduced in whole or in part

the violation was excusable or that it would be unreasonable to issue a penalty fee. The the circumstance that the personal data controller did not know the rules or had defective procedures are not a reason to lower the penalty fee.16 IMY states that no reason has otherwise emerged for setting it down the penalty fee according to ch. 6 Section 5 of the Criminal Data Act.

Of ch. 6 Section 3 first paragraph of the Criminal Data Act follows that a sanction fee for violation of ch. 3 Section 7 of the same law may not exceed five million kroner. Of the second paragraph follows that for a violation of i.a. 2 ch. § 12 and ch. 3 Section 2 the Criminal Data Act allows a sanction fee to amount to a maximum of ten million kroner. The highest the amount that can be determined is thus ten million kroner.

IMY decides based on an overall assessment that the Police Authority must pay a penalty fee of SEK 2,500,000.

Orders

The police authority must be ordered to take educational measures and others organizational measures required according to ch. 3 Section 2 of the Criminal Data Act to ensure that the routines that exist reach the entire organization and that the authority can thereby demonstrate and ensure that all processing of personal data is constitutional. The measures must have been taken no later than September 15, 2021.

According to ch. 4 § 2 of the Criminal Data Act, the personal data controller must in an individual case provide certain information to the data subject, if necessary for him or her to be able to exercise their rights. The information must, among other things, include the legal basis for the processing, categories of recipients of the personal data and for how long the personal data may be processed. It appears from the preparatory work that the provision is applicable e.g. in cases where the data subject risks suffering loss of rights if he or she does not receive the information or if it is important to him or her for other reasons to know the processing in order to exercise their rights. Another example

which is addressed in the preparatory work is that sensitive personal data has been processed in violation of 2

Cape. Section 11 on sensitive personal data. 17

The obligation to provide information according to ch. 4 Section 2 of the Criminal Data Act does not apply to that extent

it is specifically prescribed by law or other constitution or otherwise appears from a decision

which has been notified with the support of the constitution that information may not be disclosed i.a. of

consideration of the interest in preventing, preventing or detecting criminal activity,

investigate or prosecute crimes, that other legal investigations or investigations do not

Prop 2017/18:232 p. 485.

Prop 2017/18:232 p.465

17 Prop. 2017/18:232 p. 465

15

16

prevented, or that someone else's rights and freedoms are protected (Chapter 4, Section 5

Criminal Code).

As IMY stated, it has not been possible to clarify what happened to them

personal data entered by the Police Authority into Clearview AI. It is therefore important to

the data subjects become aware of the processing in order to be able to exercise their rights,

especially as it concerns sensitive personal data that has been processed in violation of

2 ch. § 11 BDL. IMY therefore assesses that the Police Authority has an obligation to leave

information according to ch. 4 § 2 BDL. During the investigation, the Police Authority did not

stated something that the registered should have been informed about the use.

Against this background, the police authority must be ordered to provide information to them

registered, whose personal data the Police Authority entered into Clearview AI, according to

4 ch. Section 2 of the Criminal Data Act with the limitations that follow from ch. 4. Section 5 of the same law.

The information must have been submitted no later than September 15, 2021.

As IMY stated, the Police Authority has entered sensitive personal data into

Clearview AI. As there is no information about what happened to the personal data

that has been shared with Clearview AI and whether these are still stored with the application shall

The police authority is finally ordered to take possible and relevant measures to

ensure that the personal data entered into Clearview AI is deleted from the application.

Such measures must have been taken no later than September 15, 2021.

This decision has been taken by the general manager Lena Lindgren Schelin after a presentation

by lawyer Elena Mazzotti Pallard. The lawyer Frida Orring is also involved in the proceedings

and the process owner for the supervision process Katarina Tullstedt participated. At the final

the proceedings are handled by head of law David Törngren and head of unit Charlotte Waller

Dahlberg participated.

Lena Lindgren Schelin, 2021-02-10 (This is an electronic signature)

Appendix:

How to pay penalty fee.

Copy for the attention of:

The data protection officer: dataskyddsombud@polisen.se

How to appeal

If you want to appeal the decision, you must write to the Swedish Privacy Agency. Enter in

the letter which decision you are appealing and the change you are requesting. The appeal shall

have been received by the Privacy Protection Authority no later than three weeks from the date of the decision

was announced. If the appeal has been received in time, send

The Privacy Protection Authority forwards it to the Administrative Court in Stockholm

examination.

You can e-mail the appeal to the Privacy 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.