The police authority

Sent only by e-mail

registrator.kansli@polisen.se

Record number:

DI-2020-2719

Your record number:

A126,614 / 2020

Date:

2021-02-10

Decision after supervision according to

Criminal Data Act - The Police Authority

use of Clearview AI

The decision of the Integrity Protection Authority

The Integrity Protection Authority states that the Police Authority has processed

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

the Criminal Data Act by using the application Clearview AI during the period autumn

2019 through March 3, 2020.

The Integrity Protection Authority decides on the basis of ch. § 1 of the Criminal Data Act that

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

thousand crowns.

The Integrity Protection Authority submits to the Police Authority in accordance with ch. § 7 first

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

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

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

ensure that all processing of personal data is in accordance with the constitution. The measures must have

taken no later than 15 September 2021.

The Privacy Protection Authority submits with the support of ch. Section 7, first paragraph 2

Criminal Data Act The Police Authority that according to ch. Section 2 of the Criminal Data Act informs them

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

to the extent that the obligation to provide information is not limited according to ch. § 5

the Criminal Data Act. The information must have been submitted no later than 15 September 2021.

The Privacy Protection Authority submits with the support of ch. Section 7, first paragraph 2

Criminal Data Act Police authority to take possible and relevant measures to they

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

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

Postal address:

Box 8114

104 20 Stockholm

Website:

www.imy.se

E-mail:

imy@imy.se

Phone:

08-657 61 00

Report on the supervisory matter

The Integrity Protection Authority (IMY), formerly the Data Inspectorate, received attention in

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

could have used the application Clearview AI. IMY initiated against the background of
the information immediately a review where the Police Authority was asked to answer about
the authority used the application as well as with what legal aid processing in so
fall occurred. Opinions 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 has provided the application to the employees. IMY therefore initiated one
in-depth review of the Police Authority's use of Clearview AI.

Clearview AI is an application provided by a US company that offers
a face recognition service where the user, after downloading the application on
a digital device, uploads an image that is biometrically matched to a very large one
number of images scraped from the open internet.1 The user then gets a result in
form of a number of URLs where any matches exist.2

The police authority's use of the Clearview AI application

The police authority has stated that the application Clearview AI has been used in a number
opportunities during the period autumn 2019 to 3 March 2020.
They are employees at the National Operations Department (NOA) and the South region
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, e.g. in order to
identify plaintiffs in suspected sexual offenses against children and in the reconnaissance 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 offenses against children and tested by employees against images in the Police Authority
s.k. NOTE portal.3 When the Police Authority's use of Clearview AI became known
through information in the media, the authority's data protection officer went out with one
recommendation that the National Forensic Center and NOA clarify and
disseminate that such use was not permitted.

Justification of the decision

The police authority's responsibility for employees' treatment of

personal data in the law enforcement activities

The police authority is a large organization with a special task of enforcing the law

and order. In addition, the police authority is governed by clear legislation on how

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

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

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

a special responsibility for the personal processing of personal data.

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

websites. IMY Report 2021: 1; Integrity protection report 2020 - report on developments in the IT area when it

applies to integrity and new technology, p. 70.

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

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

The police authority is, as the person responsible for personal data, responsible for everything

personal data processing that takes place under the authority's guidance or on

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

personal data processing carried out at the authority falls under the Police Authority's

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

persons on an equal footing with employees (eg temporary staff) or

contractor performs.4 Also of ch. Section 1 of the Police Treatment Act (2018: 1693)

within the area of the Criminal Data Act (PBDL) it appears that the Police Authority is responsible for the personal data processing carried out at 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 adequate safeguards are in place in place through appropriate technical and organizational measures. The police authority shall ensure that there are clear guidelines and routines regarding the IT tools provided 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 Police Authority, there are a few employees who used Clearview AI without the authority provided the application to the employees. However, the treatment has taken place in the performance of the employees' duties at the authority. The treatment has in addition, performed with personal data obtained from current investigations and at the majority of cases during ongoing criminal investigations, ie. 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 deprive it responsibility that the authority has as personal data controller.

Against this background, IMY states 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 demonstrate that the authority personal data processing is in accordance with the constitution

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

Organizational measures can include be to adopt internal data protection strategies,

inform and train employees and ensure a clear division of responsibilities.7 Measures

which can be taken to show that the treatment is constitutional can e.g. be

documentation of IT systems, treatments and measures taken, etc..8

In the case, the police authority has submitted an internal routine for processing personal data

within the authority. Some additional governing document for the employees' treatment of

personal data has not been submitted. Nor any data on 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 p. 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 processing of personal data is in accordance with the constitution.

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

7 Sandén, H-O, 2019, SFS 2018: 1177 Lagkommentar, Norstedts juridik.

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

5

organizational units used Clearview AI in violation of applicable regulatory shows

that the routine has not had sufficient impact within the authority. The police authority has the courage

this background has not been able to show that there are sufficient organizational measures, in

form of e.g. internal strategies or training, in place to ensure that

the treatment is in accordance with the constitution.

IMY notes 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 in accordance with the constitution. The police authority has thus violated

Chapter 3 Section 2 of the Criminal Data Act.

The police authority's processing of biometric data in

associated with the use of Clearview AI

According to the Police Authority's information, there are pictures of people, who were then transformed into

biometric data, in ongoing operational matters loaded into Clearview AI at a

several times.

The police authority has not reported on how the biometric data read into

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

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

third country or if the information is disclosed to others in connection with its use. The

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

made before using Clearview AI.

Biometric personal data is sensitive personal data and may, according to ch. 12 §

the Criminal Data Act is only dealt with if it is specifically prescribed and absolutely necessary

for the purpose of the treatment. Of ch. 2 Section 4 of the 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 like Clearview AI involves the biometric of individuals

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

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

processing of personal data when using such a service is unlikely

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

underlying the Criminal Data Directive.9 The European Data Protection Board has expressed

for a similar view.10

The processing of biometric data that took place during the Police Authority's use

of Clearview AI has been performed without any control or knowledge from the Police Authority

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

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

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

processing of biometric data in the service Clearview AI 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 the physical and physical

persons with regard to the processing of personal data by the competent authorities in order to prevent, deter, investigate, detect or prosecute offenses or carry out criminal penalties, and the free flow of such information and if

repeal of Council Framework Decision 2008/977 / JHA.

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

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

Obligation to carry out an impact assessment

According to ch. Section 7, first paragraph, of the Criminal Data Act, a person responsible for personal data is obliged to

carry out an impact assessment before starting a new treatment that can

assumed to entail a special risk of invasion of the data subject's privacy.

The preparatory work for the Criminal Data Act and the underlying Criminal Data Directive appear

that in assessing whether an impact assessment is needed, the treatment must

scope, nature, context and nature are taken into account. Special consideration must be given to the treatment

includes any new technology.11

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

these may, as reported above, only be treated if specifically prescribed and

absolutely necessary in view of the purpose of the treatment. Since

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

includes face recognition, with new technology provided by an external actor in

third countries, the treatment can be assumed to have entailed a special risk of intrusion into

registered privacy. An impact assessment would therefore have

carried out before starting treatment. The use of the Clearview application

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

invasion 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 employees performed during use

by Clearview AI. The lack of organizational measures has led to employees using

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

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

IMY states that the Police Authority in violation of ch. Section 7, first paragraph

the Criminal Data Act has 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 of the IMY

violations of the said law. These consist of i.a. injunctions, prohibition of

processing and issuing a penalty fee.

Of ch. 6 Sections 1 and 2 of the Criminal Data Act follow that the IMY can issue a penalty fee at

violation of i.a. the provisions of ch. Section 12 and Chapter 3 §§ 2 and 7

the Criminal Data Act. The penalty fee must meet the requirements set out in the Criminal Data Directive

that sanctions should be proportionate, dissuasive and effective.12

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

special consideration shall be given to the circumstances specified in ch. 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 pp. 309 f.

infringement of the infringement, the nature, severity of the infringement and

duration, what the personal data controller or personal data assistant has done to

limit the effects of the infringement, and whether the controller or

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

IMY notes that the Police Authority has failed in several respects in its

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

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

the processing of personal data in the case in question 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 has processed

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

the Criminal Data Act.

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

Police Department's use of Clearview AI. However, this is not crucial for if

penalty fee shall be charged, without the fact that the risk of injury existed is in accordance

preparatory work sufficient for this.13 Through the use of Clearview AI has employees

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

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

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

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

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

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

stated, the IMY considers the risk of injury for the data subjects to be high in the case in question.

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

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

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

account for what happened to the personal data the authority entered into

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

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

Section 1 of the Public Access to Information and Secrecy Act (2009: 400), and the Police Authority has not

presented any breach of confidentiality that could justify disclosure of

the data. These circumstances mean that there are reasons to look seriously

the infringements.

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

determining the amount of the penalty fee. An attenuating circumstance is that

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

However, the use of Clearview AI has taken place in a total of a few months,

and ceased only after the Privacy Protection Authority's investigation began.

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

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

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

It may further be considered aggravating that the data of the data subjects were 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 provided

13

14

Prop. 2017/18: 232 pp. 483.

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

matats in. The fact that it has been biometric, ie. sensitive personal data, such as

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

there are reasons to take the infringement seriously.15

In summary, the reported circumstances entail a penalty fee

shall be levied and that a relatively substantial penalty fee is justified.

The size of the penalty fee

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

the infringement was excusable or that it would be unreasonable to issue a penalty fee. The

the fact that the data controller did not know the rules or had

Inadequate procedures are not a reason to reduce the penalty fee.16 IMY

notes that there have also been no other reasons for reducing

the sanction 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 penalty fee for

violation of ch. 3 Section 7 of the same law may not exceed SEK 5 million. Of

the second paragraph follows that for a violation of e.g. Chapter 2 Section 12 and Chapter 3 § 2

According to the Criminal Data Act, a penalty fee may amount to a maximum of SEK 10 million. The highest

the amount that can be determined is thus ten million kronor.

IMY decides on the basis of an overall assessment that the Police Authority shall pay one

penalty fee of SEK 2,500,000.

Instructions

The police authority shall be instructed to take training measures and others

organizational measures required according to ch. Section 2 of the Criminal Data Act to ensure

that the existing routines reach the entire organization and that the authority can thus show

and ensure that all processing of personal data is in accordance with the constitution. The measures

must have been taken by 15 September 2021.

According to ch. 4 Section 2 of the Criminal Data Act shall be the person responsible for personal data 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 include include the legal basis

for the processing, categories of recipients of the personal data and for how long

personal data may be processed. The preparatory work shows that the provision is

applicable e.g. in cases where the data subject risks losing his or her rights if

does not receive the information or if it is important to him or her for any other reason

to know the treatment in order to be able to exercise their rights. Another example

that is included 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 information obligation 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 statute or otherwise stated in the decision

which has been announced on the basis of the constitution that information may not be disclosed, e.g. of

taking into account the interest in preventing, deterring or detecting criminal activity;

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

Prop 2017/18: 232 pp. 485.

Prop 2017/18: 232 p.465

17 Prop. 2017/18: 232 pp. 465

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

criminal law).

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

personal data entered by the Police Authority in Clearview AI. It is therefore important that

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

in particular as regards sensitive personal data processed in breach of

Chapter 2 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 has not

stated something that the data subjects 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

Chapter 4 Section 2 of the Criminal Data Act with the restrictions that follow from Chapter 4 § 5 of the same law.

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

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

Clearview AI. Then there is a lack of information about what happened to the personal data

shared with Clearview AI and if these are still stored with the application should

Finally, the police authority is instructed to take possible and relevant measures to

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

Such measures must have been taken by 15 September 2021.

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

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

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

The case is handled by Chief Justice 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 information to:

The Data Protection Ombudsman: dataskyddsombud@polisen.se

How to appeal

If you want to appeal the decision, you must write to the Privacy Protection Authority. Enter i

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 Integrity 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 data that may be covered by

secrecy. The authority's contact information can be found on the first page of the decision.