AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
PO Box 93374, 2509 AJ The Hague,
The Netherlands
Hoge Nieuwstraat 8, 2514 EL The Hague,
The Netherlands
T +31 70 8888 500 - F +31 88-0712140
autoriteitpersoonsgegevens.nl

Clearview AI Inc.
99 Wall Street
#5730, New York, NY, 10005
United States

Date
16 May 2024

Our reference

Contact person

Subject
Decision to impose fines and orders subject to a penalty for non-compliance

Dear members of the board,

The Autoriteit Persoonsgegevens (hereinafter: AP) has decided to fine Clearview AI Inc. (hereinafter: Clearview) a total amount of **€ 30,500,000**. Clearview violated the General Data Protection Regulation by infringing the standards mentioned below.

First of all, the AP finds that for the purpose of their 'Clearview for law-enforcement and public defenders' service, Clearview processes, without a legal basis to do so, personal data of data subjects who are within the territory of the Netherlands. In doing so, Clearview violates Article 5(1), opening words and subsection (a) of the General Data Protection Regulation (hereinafter: GDPR), read in conjunction with Article 6(1) GDPR.

Second of all, for the purpose of said service, Clearview violates Article 9(1) GDPR, by processing a special category of personal data (biometric data) of data subjects who are within the territory of the Netherlands.

Third of all, the AP finds that Clearview does not adequately inform data subjects. Consequently, Clearview acts contrary to Article 12(1) GDPR, read in conjunction with Article 14(1) and (2) GDPR, and contrary to Article 5(1), opening words and subsection (a) GDPR.

Fourth of all, Clearview violated Article 12(3) GDPR, read in conjunction with Article 15 GDPR by not responding to two access requests by data subjects. And fifth of all, since Clearview does not facilitate data subjects within the territory of the Netherlands in exercising their right of access, they violate Article 12(2) GDPR, read in conjunction with Article 15 GDPR.

The circumstance that Clearview has not designated a representative in the European Union within the meaning of Article 4, opening words and paragraph 17 GDPR, although they are obliged to do so pursuant to Article 27(1) GDPR, also constitutes a violation of the GDPR. The AP refrains from imposing a fine for this violation, as Clearview has already been fined for this violation by the Italian and the Greek Data Protection Authorities.

The AP also decided to impose **four orders subject to a penalty for non-compliance** on Clearview, which orders relate to ending the still ongoing violations.

The AP takes the view that imposing administrative fines and orders subject to a penalty for non-compliance on Clearview is not only appropriate but also necessary, as it regards serious violations. After all, Clearview violated the rights and freedoms of citizens by unlawfully processing their personal data (including biometric data), by not fully informing citizens about such processing, by not responding to access requests by citizens and by not designating a representative in the European Union.

The administrative fines and the orders subject to a penalty for non-compliance will be elucidated in this decision. To that end, (1) the reason and course of the proceedings, (2) the established facts, (3) the violations, (4) the amount of the fines and (5) the orders subject to a penalty for non-compliance will successively be addressed. In conclusion (under 6), the decision follows and you will also be informed about what you can do if you do not agree with the decision.

The Dutch-language decision is authentic, however this English-language version contains a complete and accurate translation of it.

Date
16 May 2024

Our reference

Contents

Date
16 May 2024

Our reference

1. Reason and course of the proceedings

1 On 3 January 2023, the AP received a complaint from a data subject. The data subject in question complained about Clearview AI Inc. not having complied with an access request he submitted. On 24 January 2023, the AP received a similar complaint from another data subject. To conclude with, the AP received a tip-off by a third data subject on 11 April 2023. In said tip-off, the data subject stated that from Clearview's reply to an access request it followed that several photos of (the face of) the data subject had been included in the Clearview database.

2 By letter of 6 March 2023, the AP informed Clearview about the fact that the AP had launched an ex officio investigation into the processing of personal data by Clearview for the purpose of the facial recognition tool that Clearview offers.

3 This investigation resulted in the Directorate of Policy, International, Strategy and Communication of the AP drawing up a report of findings (hereinafter: investigative report) on 1 May 2023. On 1 June 2023, this investigative report was handed over to the enforcement unit of the Directorate of Legal Affairs and Legislation Advice of the AP.

4 By letter of 20 June 2023, the AP sent Clearview a notification of intent to enforce, as well as the underlying investigative report and supporting documents. Clearview was given the opportunity to express their opinion on the investigative report and the supporting documents. By email of 21 June 2023, the AP sent a copy of the letter of 20 June 2023 to Clearview. Clearview did not use the opportunity offered by the AP to give their opinion on the notification of intent to enforce.

2. Facts

2.1 Clearview's business activities and processing operations

5 Clearview has their registered office in New York, United States.[1] Clearview does not have a branch in Europe, nor does the company have a representative in the European Union (hereinafter also: the Union).

6 Clearview provides services that utilize facial recognition technology. That means, an algorithm capable of accurately analysing faces in an image to such an extent that it will subsequently be able to recognize that same face (and consequently the same person) in other images.

7 To be able to recognize a face in various images, Clearview utilizes a sophisticated algorithm. The core of said algorithm consists of a 'model' built up using so-called machine learning. The model converts a depicted face into a unique code. This is also known as 'embedding' or 'vector'. The vector is compiled such

[1] Clearview AI Inc., 99 Wall Street #5730, New York, N.Y. 10005, USA.

that when several images of the face of the same individual are subjected to the algorithm, the related vectors differ very little from each other. By comparing the vector of the data subject's face to other vectors, it is possible to find other images in which the face of the data subject in question is depicted.

8 Clearview built a database consisting of over 30 billion photos (hereinafter: the database). The photos in the database originate from publicly accessible internet sources, including social media platforms, personal and professional websites, news articles, mug shots and American public databases containing information about convicted persons. The photos are collected by so-called 'crawlers'. Crawlers are software programmes that automatically record information on the internet. Usually, this is started with on the basis of a list of websites (URLs)[2] to be visited, but in addition, the settings of the crawler can be adjusted such that hyperlinks to other websites are automatically followed. In that way, depending on the settings, a large part of the internet can be recorded, even when the original list of URLs to be visited is short. This way of operating is known as 'scraping'. Clearview stated the following about this in their 'Company Overview': "Clearview AI has a propriety open-web crawling algorithm which has collected data from millions of domain names (…)". In this case it regards a kind of 'untargeted scraping'. In untargeted scraping, the information is collected in an untargeted and systematic way. That means collecting takes place on the scraper's own initiative, irrespective of whether a Clearview client made a search inquiry.

9 In their crawler, Clearview did not set any limitations in terms of geographical location or nationality. Clearview compares the scope of the collection to the data Google stores, for which no a priori limitations apply either: "Clearview AI's image repository consists of public data that can be obtained by a typical Google search".[3]

10 Furthermore, Clearview's crawler has the same access rights as any other visitor of the same web page. This means for instance that a social media profile that is accessible to friends only cannot be visited and recorded by Clearview. In this context, the AP notes it is not unusual for the data subject's profile photo and corresponding name to be visible even in case of a private social media profile.

11 Of each image showing one or several faces that the Clearview crawler finds, Clearview records the following information:
- URL of the web page of the original photo;
- the photo itself;
- any information describing the characteristics of the photo, such as date and time when the photo was taken, subject to that information being part of the photo (hereinafter: metadata);
- the vector related to the face (or faces) in the photo.
When reference is made to "the photos" in this decision, this is understood to include any related metadata, vector and the URL of the photo as well.

[2] An URL (Uniform Resource Locator) – in short – is the address of a web page.
[3] https://www.clearview.ai/post/what-clearview-ai-has-implemented-to-ensure-that-facial-recognition-technology-is-used-responsibly

12 The machine learning algorithm Clearview uses, is trained and tested using photos Clearview retrieves from the above-mentioned database. In training and testing, multiple images of faces are used of which it is known that they belong to the same person (for instance because they are part of the same social media profile). Based on the examples, the model "learns" how to compare faces and consequently how to search as well.

2.2 How the algorithm operates and a description of the 'Clearview for law-enforcement and public defenders' service

13 The 'Clearview for law-enforcement and public defenders' service, provided by Clearview and focal point of this decision (hereinafter also: the service), consists of making the database mentioned in marginal number 8, storing over 30 billion of photos, searchable. By calculating the vectors for each photo in advance, users are enabled to search 'by face' (in essence: by vector) and in that way find other images of the same face in the Clearview database.

14 The 'Clearview for law-enforcement and public defenders' service is meant for government and investigative authorities. This service enables those authorities to search the above-mentioned database (Clearview Platform). The user of this service follows the steps described below.

15 Before the search process can start, the user must have a digital photo of a data subject, also called a 'probe image'. This image may have come from a telephone, security camera, body cam or from another source. The user's objective is finding out which other photo in the Clearview database shows the data subject. If the Clearview database for instance contains a photo from a blog post or social media profile, this will enable the user to identify the data subject.

16 The first step consists of uploading the probe image to the Clearview servers. When doing so, certain information about the case is sent along as well.[4] After uploading, Clearview calculates the vector of the probe image by means of the trained model.

17 By comparing the vector of the data subject's face to all other vectors in their database, Clearview retrieves the photos that also show the data subject, provided such photos are in their database. These images were collected by Clearview at an earlier stage using the crawler mentioned in marginal numbers 8 ff.

18 The photos that were found, including the related URLs, are then fed back to the user.

19 By following the links to the URLs on which the original photos were found by the crawler, the user is enabled to retrieve more personal data of the data subject, and in doing so maybe identify them. When it

[4] For instance case number and type of criminal offence.

regards a profile photo on a social media platform, the identification often is easy as it usually regards personalized profiles.

3. Assessment

20 In sections 3.1 and 3.2 the material and territorial scope of the GDPR will be gone into. In sections 3.3-3.8 the assessment of the responsibility of the controller, lawfulness of the processing, the processing of special categories of personal data, transparency obligations, rights of data subjects and representation within the Union will successively be addressed.

3.1 Material scope of the GDPR

3.1.1 Legal framework

21 Pursuant to Article 2(1) GDPR, the regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

22 Article 2(2) GDPR stipulates that the GDPR does not apply to the processing of personal data:
a. in the course of an activity which falls outside the scope of Union law;
b. by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
c. by a natural person in the course of a purely personal or household activity;
d. by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

23 The exceptions to the applicability of the GDPR as listed in Article 2(2) GDPR, according to the Court of Justice of the European Union (hereinafter: CJEU) should be interpreted strictly.[5]

24 In that connection the CJEU considered that Article 2(2), opening words and subsection (a) GDPR, read in the light of recital 16 of the GDPR, must be regarded as being designed solely to exclude from the scope of that regulation the processing of personal data carried out by state authorities in the course of an activity which is intended to safeguard national security or of an activity which can be classified in the same category. It particularly regards activities having the aim of safeguarding the essential functions of the state and the fundamental interests of society.[6]

[5] CJEU 22 June 2021, C-439/19, ECLI:EU:C:2021:504, para 62.
[6] CJEU 22 June 2021, C-439/19, ECLI:EU:C:2021:504, paras 66 and 67.

25 Pursuant to Article 4, opening words and paragraph 1 GDPR, personal data are understood to mean any information relating to an identified or identifiable natural person (data subject).

26 Article 4, opening words and paragraph 2 GDPR stipulates that processing is understood to mean any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

27 Article 4, opening words and paragraph 14 GDPR stipulates that 'biometric data' are understood to mean personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

28 From recital 51 of the GDPR follows that the processing of photographs should not systematically be considered to be processing of special categories of personal data as "they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person."

3.1.2 Factual findings

29 From the Clearview business model it follows that in the operation of their business, Clearview collects photos from public sources through scraping and stores them. Clearview also endorses this in their various privacy statements. In addition to visual material, these photos may also contain metadata[7]. As described above in marginal number 8, the Clearview database contains over 30 billion different photos.

30 As explained in section 2.2, a vector of the face of the person or persons shown in the photo is made on the basis of the photo in the database. These facial features can be used later on in identifying individuals and retrieving which photos within the Clearview database also show that individual.

3.1.3 Legal assessment

31 The AP finds that the processing operations of Clearview fall under the material scope of the GDPR. The AP substantiates this as follows.

3.1.3.1 (Special) personal data

32 First of all, the photos as well as the metadata relating to it and the source of the photos are personal data within the meaning of Article 4, opening words and paragraph 1 GDPR. After all, in the photos Clearview collects individuals are recognizably shown. In addition, the photo's metadata, if available, may result in

[7] See marginal number 11.

identifying the data subject. The source of the photo as well, in the form of an URL, may comprise a unique identifier of a data subject, for instance in the form of a user name or user-id.

33 In addition, the vectors of the collected photos, which vectors were created using the Clearview algorithm, are biometric data within the meaning of Article 4, opening words and paragraph 14 GDPR, and special personal data within the meaning of Article 9(1) GDPR. The AP substantiates this as follows.

34 Article 4, opening words and paragraph 14 GDPR stipulates that biometric data are understood to mean personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

35 From Article 4, opening words and paragraph 14 GDPR, and from recital 51 of the GDPR it follows that the mere fact that individuals are shown recognizably in photos is not enough to consider these photos biometric data. This is only so when they are processed through a specific technical means allowing the unique identification or authentication of a natural person. The AP finds that this requirement has also been met and the AP substantiates this as follows.

36 From section 2.2 it follows that Clearview uses an algorithm to convert the collected photos and the uploaded photos into vectors. From section 2.2.2 it follows that Clearview manages a database containing collected photos and the vectors corresponding to those photos. So, by using this facial recognition technology, Clearview utilizes a technical means.

37 In addition, the purpose of the technical means must be allowing the unique identification of natural persons. From section 2.2 it follows that it is inherent to the nature of the service that the service is being used for by means of a photo of a data subject - the probe image - that is to be uploaded, finding other photos of said same data subject in the Clearview database. Using the algorithm, the vectors of the probe image are compared to the vectors of the collected photos that are in the database. This is how the user can retrieve in which photos the data subject is being shown and access is obtained to the URLs and metadata related to said image. So, by using the Clearview search function a data subject can unambiguously be identified.

3.1.3.2 Processing (special) personal data

38 It was established above that the service of Clearview consists of (i.a. by means of scraping) collecting, storing and updating personal data and providing them to third parties. The AP therefore comes to the conclusion that personal data are being processed within the meaning of Article 4, opening words and paragraph 2 GDPR. The requirements for applying the GDPR, as laid down in Article 2(1) GDPR, have thus been met.

3.1.3.3 Exceptions as regards the material scope

39 The exceptional situations laid down in Article 2(2) GDPR are not applicable. Clearview is a private party and not a member state, government body or authorized authority. For that reason, the exceptional situations laid down in Article 2(2) opening words and subsections (a), (b) and (d) GDPR cannot apply. Nor is Clearview a natural person, so that the exceptional situation under (c) does not apply either.

3.1.3.4 Conclusion as regards the material scope of the GDPR

40 Taking the above into account, the AP comes to the conclusion that Clearview processes (special) personal data for providing their services via the Clearview Platform. The requirements for applying the GDPR, as laid down in Article 2(1) GDPR, have thus been met. The exceptional situations laid down in Article 2(2) GDPR are not applicable. Taking this into consideration, the processing operations of personal data by Clearview fall under the material scope of the GDPR.

3.2 Territorial scope of the GDPR

3.2.1 Legal framework

41 Article 3 GDPR defines the territorial scope of the regulation. From the second paragraph of said provision it follows that the scope of the GDPR is not limited to the territory of the European Union (hereinafter: the Union). The GDPR may also be applicable to processing operations by controllers that are outside of the Union. This is first of all the case when the controller offers goods or services to data subjects who are in the Union. In addition, the GDPR applies to monitoring the behaviour of data subjects in the Union. So, considering the latter situation, the GDPR is in any case applicable if:

a. the controller is not established in the Union;
b. personal data are processed of data subjects who indeed are in the Union;
c. the processing operation is related to monitoring the behaviour of data subjects, to the extent that such behaviour takes place in the Union.

42 About the monitoring of behaviour referred to under (c), recital 24 of the GDPR says that in order to determine whether a processing operation can be considered monitoring (in Dutch: 'controle van het gedrag') data subjects, it should be ascertained whether natural persons are being tracked on the internet, including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

43 In the Guidelines 3/2018 on the territorial scope of the GDPR of 12 November 2019, the European Data Protection Board (hereinafter: EDPB) noted that the use of the word "monitoring" or "checking" implies that the controller has a specific purpose in mind for the collection and subsequent reuse of the relevant

data about an individual's behaviour within the EU. The EDPB takes the view that any online collection or analysis of personal data of individuals in the EU would not automatically count as 'monitoring'. It will be necessary to consider the controller's purpose for processing the data and, in particular, any subsequent behavioural analysis or profiling techniques involving that data. The EDPB takes the wording of recital 24 of the GDPR into account, in which it is indicated that to determine whether processing involves monitoring a data subject's behaviour, the tracking of natural persons on the internet, including the potential subsequent use of profiling techniques, is a key consideration.[8]

3.2.2 Factual findings

44 By letter of 17 March 2023, Clearview informed the AP they are established in the United States and do not have a branch in the EU. The stationery states that Clearview's address is 99 Wall Street #5730, New York, N.Y. 10005 (United States). Clearview's website states the same address.

45 In their letter, Clearview among other things stated:

> "Clearview AO does not respond to Art. 15 GDPR access requests, because it is not subject to the GDPR as we have mentioned. In the past, Clearview voluntarily provided European residents with information about their appearance or non-appearance in Clearview AI search results upon request. However, we have terminated that practice, both to reduce potential security risks and to better reflect the fact that Clearview AI's activities are not within the territorial scope of the GDPR. As such, Article 15 is not applicable to Clearview AI."

46 In Clearview's privacy statement of 29 January 2020, as published on their website, it says that citizens of the European Economic Area (the EU member states, Liechtenstein, Norway and Iceland) or Switzerland who wish to lodge a complaint or seek a solution for a dispute with Clearview regarding the processing of their personal data, may apply to the competent data protection authority of their country free of charge.

47 In 2020, according to Statistics Netherlands [CBS], 97% of the Dutch aged 12 or older had access to the internet at home.[9] 87.6% of the interviewed people indicated they had used the internet almost every day the previous three months. In 2019, 63% of the Dutch aged 12 or older were active on one or more social networks such as Facebook, Twitter, Instagram, or Snapchat.[10]

[8] Guidelines 3/2018 on the territorial scope of the GDPR, 12 November 2019, page 20.
[9] https://www.cbs.nl/nl-nl/cijfers/detail/83429NED?dl=2F8AA
[10] https://longreads.cbs.nl/nederland-in-cijfers-2020/wie-gebruikt-het-vaakst-sociale-media/#:~:text=Vrijwel%20iedereen%20in%20de%20leeftijdsgroep,laatste%20jaren%20vaker%20sociale%20media.

3.2.3 Legal assessment

3.2.3.1 Controller is not established in the Union

48 It is a fact that Clearview is not established in the Union. This follows from what is stated on the Clearview website, the Clearview stationery and the letter dated 17 March 2023 that Clearview sent to the AP.

3.2.3.2 Processing personal data of data subjects in the Netherlands

49 In section 3.1.3.2 it has already been concluded that Clearview processes (special) personal data. The question that now needs to be answered is whether the processing operation also includes personal data of Dutch data subjects.

50 In response to the first request for information by the AP, Clearview only replied that they take the view that the GDPR does not apply to them, for which reason they did not answer the questions asked by the AP. The same goes for the questions regarding the processing of personal data of Dutch data subjects. In addition, Clearview made it known that they no longer handle access requests by data subjects from the European Union.

51 However, the AP ascertained that Clearview also processes data of Dutch data subjects - as well as the personal data of other citizens in other member states of the Union. This becomes clear from the following.

Response to an access request by a Dutch data subject

52 On 11 April 2023, as stated in marginal number 1, the AP received a tip-off from a Dutch data subject who had submitted an access request to Clearview in time. 'In time' meaning that Clearview responded to said request before they decided that they would no longer handle new requests from EU citizens. Based on the probe image the data subject furnished, three images were found that originated from different websites having .nl for TLD. The response to the access request included the images found and the exact URLs on which they could be found. This proves for a fact that said Dutch data subject appeared in the Clearview database and that Clearview scraped Dutch websites.

Absence of a filter for Dutch data subjects

53 In addition to this, the AP takes into account that according to Clearview, the database contains 30 billion images, and that by now this number has in all likelihood grown. No measures have been taken to filter and bar images of Dutch data subjects (or their behaviour in the Netherlands) from the database. On the contrary, from the previous marginal number it follows that Clearview's crawler scrapes Dutch websites as well. In this context, the AP furthermore takes into account that the internet and social media are widely used in the Netherlands. By way of illustration, the AP refers to marginal number 47.

54 Considering the above, the AP ascertains that Clearview's database also contains personal data of Dutch data subjects.

Clearview's privacy statement of 29 January 2020

55 As indicated in marginal number 46, the privacy statement on Clearview's own website stated, in any case as from 29 January 2020, that data subjects from the European Economic Area should apply to their national supervisory authority in the event of complaints about Clearview. From this, the AP deduces that Clearview processes personal data of those data subjects - including Dutch data subjects -. After all, if this was not so, referring to national supervisory authorities in the event of complaints would be pointless. Taking this into consideration, the position Clearview takes in their letter of 17 March 2023 that the GDPR would not be applicable to them, is contrary to the aforementioned findings of the AP.

Decisions by other European supervisory authorities

56 In addition to this, the AP refers to the following enforcement decisions and measures on the basis of the GDPR that other European supervisory authorities took against Clearview. Those decisions are a confirmation that Clearview processes personal data of data subjects across Europe.

57 Applying the GDPR, the German supervisory authority in Hamburg (Hamburgische Beauftragte für Datenschutz und Informationsfreiheit) ordered Clearview by letter of 27 January 2021 to remove biometric data of a German citizen. This citizen made an access request and the German supervisory authority ascertained that from Clearview's response to the request it follows that the German citizen actually appeared in the database.

58 In an enforcement decision based on the GDPR dated 10 February 2022, the Italian supervisory authority (Garante per la protezione dei Dati Personali) i.a. ascertained that four complainants had submitted an access request to Clearview and that three of them received a substantive response from Clearview. The Italian supervisory authority further ascertained that said three complainants appeared in three, thirteen and nine images, respectively, in the database.

59 In an enforcement decision partly based on the GDPR dated 18 May 2022, the British supervisory authority (Information Commissioner's Office) ascertained that personal data of British citizens had been processed by Clearview. The British supervisory authority i.a. based this conclusion on establishing for a fact that British clients had had trial periods to try out the Clearview service, in the course of which five enforcement bodies made a total of 721 search inquiries. Clearview returned search results to those bodies. Currently, Clearview no longer provides the service in Great Britain. The British supervisory authority for that matter has no indications that the number of images of British citizens in the Clearview database has decreased.

60 In an enforcement decision based on the GDPR dated 17 October 2022, the French supervisory authority (Commission nationale de l'informatique et des libertés) concluded that Clearview had processed personal data of

French citizens. In that connection, the French supervisory authority considered that the images Clearview processes, are not limited to the territory of the United States, but are indeed collected from i.a. social networks that are used all over the world.

61 In an enforcement decision based on the GDPR dated 9 May 2023, the Austrian supervisory authority (Datenschutz Behörde) concluded that Clearview had processed personal data of an Austrian complainant who had made an access request.

3.2.3.3 Processing is related to monitoring the behaviour of data subjects in the Netherlands

62 In the EDPB Guidelines 3/2018 on the Territorial Scope of the GDPR it is stated that the application of Article 3(2), opening words and subsection (b) GDPR, does not require that the controller intends to monitor the behaviour of a data subject in a targeted manner, but that it is of importance to consider the controller's purpose for processing the data and, in particular, any subsequent behavioural analysis or profiling techniques involving that data. The subsequent use is also relevant.

63 From the description of Clearview's processing of personal data it follows that the personal data in the Clearview database are enriched over time with new information. The decision by the Italian supervisory authority moreover states that changes in the looks of data subjects do not prevent new data from being linked to old data. By enriching old data with new images, metadata and associated URLs, an archive is created of continuously updated information on data subjects over the course of time.

64 As elucidated in chapter 2, the objective of the Clearview service is to enable clients to match probe images with images of the same data subject that are already in the Clearview database. By being able to search and match images in this way, Clearview's clients are enabled to go through the above-mentioned archive of information about a data subject and follow the behaviour of the individuals shown in the images over the course of time. It may for example regard the individual's relation status, parental status, location or place of residence, use of social media, habits (for instance whether the individual in question smokes or drinks), profession or pastime, ability to drive a car, which (paid) activities this individual performs (and whether those activities are legal).

65 In this way, Clearview's clients learn more about the individuals shown in the photos, including their identities. Establishing identity is not the only reason, however. Considering the envisaged clients of the service (government and investigative authorities), it is more than likely that what all these authorities are really interested in individuals, who because of their (suspected) behaviour, are interesting for law enforcement officers.

66 Taking the envisaged clients of the service into account (government and investigative authorities), they also use the service to take decisions that (may) affect the data subjects, to predict or analyse their behaviour, to apprehend them, to gather evidence about what they have done or to prevent illegal activities. Monitoring an individual's behaviour by a Clearview client may comprise the following:

ascertaining where an individual is or was at a certain point in time, keeping tabs on an individual over the course of time by repeatedly submitting the same probe image of said individual, combining the search results with information obtained from other types of monitoring or surveillance.

67 Considering the sources from which Clearview obtains the images in their database (including social media), the above-mentioned behaviour unavoidably also includes the behaviour of Dutch data subjects within the Union. In that connection it is also relevant that, as a rule, those data subjects will spend most of their time in the Netherlands, so that obviously the photos Clearview collects, will for the best part cover the behaviour in the Netherlands - which by no means precludes that it will also cover the behaviour of Dutch citizens across the Union.

3.2.3.4 Conclusion

68 Now that Clearview is not established in the Union, Clearview processes personal data of data subjects who are in the Netherlands and the processing is related to monitoring behaviour of data subjects in the Netherlands, the AP comes to the conclusion that the processing of personal data by Clearview for the purpose of their service falls under the territorial scope of the GDPR.

3.3 Controller

3.3.1 Legal framework

69 Article 4, opening words and paragraph 7 GDPR stipulates that controller is understood to mean the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.

3.3.2 Factual findings

70 Considering the services Clearview provides, two situations as regards the responsibility of the controller can be distinguished.

71 First of all, personal data are being processed in the context of setting up, maintaining and enriching the Clearview database and for training the Clearview facial recognition algorithm. Clearview performs said processing operations at their own initiative in order to be able to provide their (potential) users with a service. The users of the Clearview services are not involved in Clearview's (untargeted) scraping of personal data from the internet, setting up and maintaining the database of collected photos nor in training the algorithm. After all, at the moment Clearview processes these data, those users are generally not even in the picture yet. For instance, the users do not give instructions or indicate preferences regarding the types of photos that are included in the Clearview database or the sources from which they are collected.

72 Second of all, personal data are being processed within the context of a search inquiry of a Clearview user, the user wanting to find photos in the Clearview database that show the same person as in the probe image. When a Clearview user wants to identify an individual in a photo on the basis of the Clearview database, the user has to upload this photo to Clearview themselves. On the basis of this photo, Clearview will by means of their algorithm verify whether there is a 'match', and feeds such photo(s) back to the user.

3.3.3 Legal assessment

73 The AP ascertains that Clearview processes personal data when scraping the internet. The purpose for which they do so is determined by Clearview themselves, namely providing and developing their services to (potential) clients and creating a database consisting of billions of photos that can be gone through on the basis of a search inquiry from a client (user) of Clearview.

74 In section 2.2 the actual operation of the Clearview Platform was set out in short. From this it follows i.a. that Clearview determines the process relating to the collection of personal data, the build-up of the database, its maintenance, and the training of the Clearview facial recognition algorithm. Clearview independently determines which personal data they collect, the way in which they do so and therefore also by which means they process the personal data. Clearview also determines which technology they will then use to compare the photos uploaded by clients to all photos that are already in the database set up and maintained by Clearview.

75 The AP therefore considers Clearview a controller within the meaning of Article 4, opening words and paragraph 7 GDPR.

3.4 Lawfulness: Articles 5 and 6 GDPR

3.4.1 General

76 Pursuant to Article 5(1), opening words and subsection (a) GDPR, personal data must be processed lawfully in relation to the data subject.

77 Article 6(1) GDPR stipulates that processing will be lawful only if and to the extent that at least one of the conditions stated under (a)-(f) applies (legal bases of the processing).

78 In this case only the legal basis mentioned in Article 6(1), opening words and subsection (f) GDPR is relevant (namely: legitimate interest), as Clearview relied on this legal basis in one of the privacy statements the AP examined and because the other legal bases in Article 6(1) GDPR evidently do not apply to this case.[11]

[11] Clearview has no relation whatsoever with the data subject, so that the legal bases listed in Article 6(1), opening words and subsections (a), (b) and (d) GDPR (consent, agreement and vital interest) cannot apply. Nor does Clearview have a legal obligation or

79 For successfully relying on the legal basis of legitimate interest (Article 6(1) opening words and subsection (f) GDPR) three cumulative conditions have to be complied with:
1. the controller or a third party must have a legitimate interest;
2. the processing of personal data must be necessary for attending to said legitimate interest;
3. when balancing the interests of the controller (or third party) and the data subject, the interests or fundamental rights and freedoms of the data subject(s) do not prevail.

3.4.2 Legitimate interest (condition 1)

3.4.2.1 Legal framework of legitimate interest

80 For successfully relying on Article 6(1), opening words and subsection (f) GDPR, first of all the condition must be complied with that Clearview as a controller pursues an interest of their own or of a third party, that may be qualified as legitimate. This means that those interests have been designated a legal interest in (general) legislation or elsewhere in law. It must regard an interest that is also protected at law, that is considered worthy of protection and that in principle must be respected and is enforceable.

81 From CJEU case law it follows that the interests must furthermore be real and present.[12] That means they should not be speculative, prospective or derived. A legitimate interest must be lawful (i.e. in accordance with applicable law), sufficiently clearly articulated (i.e. sufficiently specific) and represent a real and present interest (i.e. not be speculative). [13]

3.4.2.2 Factual findings legitimate interest (condition 1)

82 By means of a request for information, the AP requested Clearview to further elucidate said legitimate interest.[14] Not considering themselves bound by the GDPR, Clearview failed to do so.

83 In Clearview's privacy statement of 29 January 2020 it is stated that Clearview only processes personal data if:

- the processing is necessary to perform our contractual obligations towards users or to take pre-contractual steps at user request, such as authenticating your log on to our services;
- the processing is necessary to comply with our legal or regulatory obligations, such as tax reporting or regulatory requirements;
- the processing is necessary for the legitimate interests of Clearview, and does not unduly affect your interests or fundamental rights and freedoms;

public task requiring processing, so that the legal bases of Article 6(1), opening words and subsections (c) and (e) are not applicable either.
[12] CJEU 11 December 2019, C-708/18, ECLI:EU:C:2019:1064, para. 44.
[13] Opinion 06/2014 on the concept of 'legitimate interest of the controller' in Article 7 of Directive 95/46/EC, 9 April 2014, Group data protection Article 29, p. 25.
[14] See case document 6.

- in some cases, and as may be requested from you from time to time, we have obtained prior consent.

84 In the AP's view, the first item mentioned above relates to the legal basis for processing personal data of users of the service. The second item relates to the legal basis for processing personal data to comply with (administrative) statutory requirements that are imposed on Clearview. So, these items do not relate to processing personal data for setting up the database and the services built up around it that Clearview provides. Consent cannot be considered a basis for these processing operations either, as Clearview does not ask consent and therefore does not obtain consent from data subjects.

85 In their privacy statement of 29 January 2020, Clearview does not further elucidate Clearview's legitimate interest mentioned under the third item. In the other privacy statements of Clearview's that were consulted for the AP investigation, no mention is made of any legal basis for the processing of personal data.

86 The current privacy statement of Clearview describes the purpose of collecting publicly available photos and information derived from them as follows:

> "As part of Clearview's normal business operations, it collects photos that are publicly available on the internet. The photos may contain metadata which may be collected by Clearview due to it being contained in the photos, and information derived from the facial appearance of individuals in the photos."[15]

87 From the current privacy statement it also follows that Clearview processes publicly available photos and information derived from them with the purpose of offering their products and services, improving their products and services and training their algorithms.

88 On the subject of the interest of third parties (in this case the users), the AP ascertains that on their website, Clearview refers to the interest that (potential) users of the Clearview services might have in the processing operations by Clearview. On the website[16] Clearview i.a. argues that:

> "Law enforcement are overwhelmed with the amount of digital evidence they have access to. This should not come as a surprise given the proliferation of smartphones, tablets, computers, and other connected devices. Some estimates show that there will be 7.5. billion smartphones in the world by 2024. […] As digital evidence grows, we find that the common thread is often faces – a person of interest's face found online from internet crimes, found after CCTV footage captures a crime, found in agency collected evidence like body cam footage, or from footage captured by citizen public safety apps like "Ring""

and:

[15] https://www.clearview.ai/privacy-policy
[16] https://app.hubspot.com/documents/6595819/view/640216868?accessId=a02cbe

> "Clearview AI is committed to offering cutting-edge identity tools for responsible organizations charged with protecting society. Every day, our products are used to deter crime, rescue victims, and make real contributions to public safety. […] We believe that when used by responsible organizations, our technology has the power to help build a safer, more secure society"

3.4.2.3 Legal assessment legitimate interest

89 Below, the AP will answer the question whether Clearview's own interest or any third party's interests, respectively, qualify as a legitimate interest within the meaning of Article 6(1), opening words and subsection (f) GDPR.

Clearview's own interest, offering access to the Clearview Platform against payment

90 From section 2.2.2 it follows that Clearview's business model consists of providing access to the Clearview Platform against payment.

91 Consequently, Clearview's own interest lies in the fact that the processing of personal data is a necessity for them to be able to engage in regular business operations. The CJEU stipulated that any processing of personal data will at all times constitute an interference with the fundamental right to the protection of personal data.[17] Although the freedom to conduct a business comprises the freedom to perform economic or commercial activities, such freedom does not extend so far as to cover activities that almost fully coincide with infringing the fundamental rights of others. In the case of the investigated service provided by Clearview, the processing of personal data is not an incidental circumstance of the service, said processing actually is what the service is all about. Clearview's own interest therefore does not qualify as a legitimate interest within the meaning of Article 6(1), opening words and subsection (f) GDPR.

The interest third parties have in combating crime, tracing victims and other public duties

92 In respect of the interest Clearview's users (government authorities and investigative services) have, the AP notes that if Clearview takes the position that the user's interest can be found in combating crime, in tracing victims and in other public duties, such interests do not qualify as a legitimate interest of a third party within the meaning of Article 6(1), subsection (f) GDPR. Said interests are society-wide interests that the Dutch and European legislators have placed with public authorities (government authorities) in dedicated and specific legislation. Based on Article 6(1) GDPR, government authorities (therefore) cannot rely on the principle of legitimate interest within the context of exercising their duties. The interests of Clearview's users therefore do not qualify as a legitimate interest.

[17] CJEU 8 April 2014, C-293/12 and C-594/12, ECLI:EU:C:2014:238.

3.4.2.4 Conclusion as regards legitimate interest

93 To the extent that Clearview relies on the legal basis of legitimate interest, such reliance already falls through on the basis of the first condition. For the sake of completeness and due care, the AP will nonetheless go into the second and third condition (necessity and balancing of interest, respectively).

3.4.3 Necessity (condition 2)

3.4.3.1 Legal framework of necessity

94 For successfully relying on the legal basis of legitimate interest, the processing operation must also be necessary for attending to the legitimate interest. In respect of this second condition, the CJEU stipulated that exceptions to the protection of personal data and the restriction thereof must remain within the boundaries of what is strictly necessary.[18] The concrete test is whether less invasive means are available to serve the same end.[19] This condition must furthermore be examined in conjunction with the principle of 'data minimisation', as laid down in Article 5(1), opening words and subsection (c) GDPR. According to this principle, the personal data must be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'.[20]

3.4.3.2 Factual findings as regards necessity

95 In reply to the AP's request for information, Clearview did not provide any elucidation on the necessity of the processing operations.

96 Clearview continuously collects photos and other personal data of data subjects that can be associated thereto - such as the source of the image and metadata, if any – from public sources on the internet (see marginal number 8). It regards a type of 'untargeted scraping'. On the Clearview website, the service is promoted by offering an 'unparalleled volume of data'.[21] In marginal number 9 it has been established that in collecting these photos and other personal data, no measures are being taken to bar data of Dutch data subjects from the database.

97 In their current privacy statement, Clearview argues the following about the retention period: "We store personal information for as long as necessary to carry out the purposes for which we originally collected it and for other legitimate business purposes, including to meet our legal, regulatory, or other compliance obligations."[22]

3.4.3.3 Legal assessment of necessity

[18] CJEU 11 December 2019, C-708/18, ECLI:EU:C:2019:1064, para. 46 and CJEU 4 May 2017, C-13/16, ECLI:EU:C:2017:336, para. 30.
[19] Opinion 06/2014 on the concept of 'legitimate interest of the controller' in Article 7 of Directive 95/46/EC, 9 April 2014, Group data protection Article 29, p. 29.
[20] CJEU 11 December 2019, C-708/18, ECLI:EU:C:2019:1064, para. 48 and CJEU 4 July 2023, C-252/21, ECLI:EU:C:2023:537, para. 109.
[21] https://app.hubspot.com/documents/6595819/view/454213073?accessId=c85a92
[22] https://www.clearview.ai/privacy-policy

98 The AP finds that the processing of personal data by Clearview is not limited to what is strictly necessary. The AP substantiates this as follows.

99 As regards Clearview's processing activities that are related to collecting and recording personal data from public sources on the internet, it is relevant that Clearview collects those data on their own initiative, irrespective of the search inquiries by the users. The personal data that Clearview continuously collects in enormous quantities are then recorded by Clearview in a database, whereas at the moment of collection and recording it is not at all certain yet that the personal data in question are relevant for search inquiries by Clearview's clients. On the contrary, it is highly likely indeed that a considerable part of the personal data in Clearview's database will not at all be relevant for the search inquiries of specific users. Taking into account the enormous quantity of personal data and the diversity of public digital sources Clearview uses to collect these data, the AP does not consider it likely that the majority of the personal data in the Clearview database will ever become relevant for future search inquiries. The processing of the personal data therefore does not fall within the boundaries of what is strictly necessary in order to be able to pursue the interests.

100 In addition thereto, the AP notes that the broad phrasing of the retention period in Clearview's privacy statement, offers them leeway to retain photos and other personal data on their database into infinity. Also considering the fact that changes in the looks of data subjects do not prevent new data from being linked to old data, Clearview's storage of the enormous quantity of personal data – of which the AP already concluded above that a considerable part will not be relevant for the search inquiries of Clearview users – without a concrete retention period, constitutes a serious infringement of the data subjects' privacy that is not proportionate to the purposes served by the processing operations.

3.4.3.4 Conclusion as regards necessity

101 The AP arrives at the conclusion that the processing of personal data is not limited to what is strictly necessary. Now that relying on the legal basis of legitimate interest also falls through on the basis of the second condition, the processing of personal data by Clearview for the purpose of providing their services cannot be based on that either. Below, for the sake of completeness, the AP will also go into the third and last cumulative condition.

3.4.4 The balancing of interests (condition 3)

3.4.4.1 Legal framework of the balancing of interests

102 The third cumulative condition for successfully relying on a legitimate interest is that the interests or fundamental rights and freedoms of the data subject(s) do not override the legitimate interest the

controller relies on. From CJEU legal precedents it follows that the weighing of the opposing rights and interests at issue in principle depends on the particular circumstances of a specific case.[23]

103 First of all the CJEU stipulated that the **seriousness of the infringement** of the data subject's rights and freedoms is an essential component of the required weighing or balancing exercise on a case-by-case basis.[24] In this respect, account must be taken i.a., of the nature of the personal data at issue, in particular of the potentially sensitive nature of those data, and of the nature and specific methods of processing the data at issue, in particular of the number of persons having access to those data and the methods of accessing them.

104 When assessing the seriousness of the infringement of the data subjects' fundamental rights and freedoms, the scale of the processing at issue and its impact on the data subjects must also be taken into account.[25] Also relevant in all this is whether the data have been disclosed by the controller or have otherwise been made accessible to a large number of individuals, or that large quantities of personal data are being processed in combination with other data. This is for instance the case when profiling for commercial purposes. Seemingly innocuous data, when processed on a large scale and combined with other data may lead to inferences about more sensitive data.[26]

105 In addition thereto, the **reasonable expectations** of the data subject based on their relationship with the controller must be taken into account. From recital 47 of the GDPR it follows that relevance must be given to the question whether there is a 'relevant and appropriate' relationship between the data subject and the controller, in situations such as where the data subject is a client or in the service of the controller. From recital 47 it furthermore follows that it is about expectations that the data subject may reasonably have at the time and in the context of the collection of the personal data. Likewise, the CJEU in this context also considered that the data subject's reasonable expectations that his or her personal data will not be processed when, in the circumstance of the case, that person cannot reasonably expect further processing of those data, are also relevant.[27] From established CJEU legal precedents it furthermore follows that in this balancing exercise it is possible to take into consideration the fact that the seriousness of the infringement of the data subject's fundamental rights resulting from that processing can vary depending on the possibility of accessing the data at issue in public sources.[28]

106 When balancing the interests, the **safeguards** the controller may have put in place must furthermore be taken into account. Safeguards may reduce the impact on data subjects and consequently influence the

[23] CJEU 4 May 2017, C-13/16, ECLI:EU:C:2017:336, para. 31.
[24] CJEU 11 December 2019, C-708/18, ECLI:EU:C:2019:1064, paras. 56 and 57.
[25] CJEU 4 July 2023, C-252/21, ECLI:EU:C:2023:537, para. 116.
[26] Compare opinion 06/2014 on the concept of 'legitimate interest of the controller' in Article 7 of Directive 95/46/EC, 9 April 2014, Group data protection Article 29, p. 39.
[27] Compare recital 47 of the GDPR and CJEU, 11 December 2019, C-708/18, ECLI:EU:C:2019:1064, para. 58
[28] CJEU 24 November 2011, C-468/10 and C-469/10, ECLI:EU:C:2011:777, paras. 44 and 45; CJEU 4 May 2017, C-13/16, ECLI:EU:C:2017:336, para. 32;
CJEU 11 December 2019, C-708/18, ECLI:EU:C:2019:1064, paras. 54 and 55.

balancing of interests. For instance, compliance with the statutory requirements under the GDPR, including in terms of proportionality and transparency, may contribute to the view that the controller meets the requirements of Article 6(1), opening words and subsection (f) GDPR.[29]

3.4.4.2 Factual findings as regards balancing of interests

107 In response to the AP's request for information, Clearview did not elucidate the balancing of interests that has to be made in the context of the third condition in order to successfully rely on the legal basis of legitimate interest.

108 In section 3.1.3.1 it has been established that Clearview's application of facial recognition technology qualifies as processing biometric data in view of unique identification of an individual within the meaning of Article 4, opening words and paragraph 14 GDPR, read in conjunction with Article 9(1) GDPR.

109 In addition, there is question of large-scale processing of personal data, which moreover also relates to minors. From information on the Clearview website it follows that they also offer the application of facial recognition software for identifying children. On their website, Clearview for instance state: "a federal agency's child exploitation unit tripled the number of victims identified with Clearview AI".[30]

110 The AP furthermore ascertained that the photos collected by Clearview are also being used to train the algorithm underlying the facial recognition technology.

111 In addition thereto, the AP ascertained in what way the processing operations by Clearview enable the users of the service to monitor data subjects and for which purposes the users of Clearview deploy the search functionality. By continuously collecting personal data from public sources and enriching the old data from the database with these new data, an archive of information is created about data subjects over the course of time. Users can go through this archive of information by conducting a search inquiry using a photo of a data subject.

112 In conclusion, the AP ascertained that Clearview does not actively take measures to remove photos and the data associated thereto from their database, once these photos are no longer published on the public internet (for instance because the data subject changed their privacy settings in their social media account, or a photo was taken offline from a publicly accessible website). In those cases, the data subject themselves has to submit a request for erasing the photo from the Clearview database the moment the photo in question is no longer publicly accessible on the internet.

[29] Compare opinion 06/2014 on the concept of 'legitimate interest of the controller' in Article 7 of Directive 95/46/EC, 9 April 2014, Group data protection Article 29, p. 41.
[30] https://www.clearview.ai/child-exploitation

3.4.4.3 Assessment of the balancing of interests

Seriousness of the infringement

113 In respect of the nature of the data involved, the AP ascertained that Clearview processes biometric personal data on a large scale, which data also relate to data subjects who are minors. Recital 38 of the GDPR states that this vulnerable group of data subjects merits specific protection under the GDPR, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of creating personality or user profiles.

114 As regards the nature and actual manner of processing the personal data by Clearview, the AP found that there is question of a grave infringement of the data subjects' privacy. Clearview systematically and on a large scale processes various types of personal data from a large number of sources that are combined and analysed in a database, without Clearview being fully transparent about it. The processing of personal data is not only complex and extensive, it moreover offers Clearview's clients the opportunity to go through data about individual persons and obtain a detailed picture of the lives of these individual persons. These processing operations therefore are highly invasive for data subjects.

115 In addition to this, the processing operations may have negative consequences for the data subjects. After all, as Clearview's database is continuously enriched with new personal data, users - by means of search inquiries into individuals shown in the image - can follow the behaviour of data subjects over the course of time.

116 Taking the above into account, the interests and fundamental rights of data subjects are most seriously infringed.

Reasonable expectations

117 As stated in marginal number 105, the reasonable expectations of the data subject must be assessed on the basis of their relationship with the controller. To that end, a reasonable and appropriate relationship should exist between them at the moment of the processing. This is not the case for the services Clearview provides: there is no relationship whatsoever between Clearview and the data subjects whose personal data have been included in the Clearview database. For that reason alone, data subjects need not expect any processing of their personal data by Clearview.

118 The public nature of the data collected by Clearview for the purpose of their service, does not entail that the data subjects (had) had to be prepared for their personal data being used in the manner Clearview does in this specific case. In this context, it is particularly relevant that the collection of personal data takes place automatically, without the data subject being notified thereof beforehand or afterwards. In addition to this, Clearview's database and facial recognition software are not publicly accessible. The majority of data subjects therefore is not even aware of the processing operations by Clearview.

119 The AP therefore concludes that in all fairness the data subjects do not need to expect that their personal data are being processed by Clearview.

The safeguards put in place

120 As regards the safeguards Clearview can put in place to limit the infringement, the AP ascertained that Clearview does not actively take measures to delete photos and data associated with them from the database once those photos are no longer published on the public internet.

121 As regards the information Clearview publishes on their website, it is noted that in doing so Clearview does not comply with the statutory obligations under the GDPR. Considering what is stated in marginal number 156 below, it is not clear to Dutch citizens that their photos (including metadata) are being processed by Clearview for facial recognition purposes. Data subjects can only become aware of this when they accidentally come across the name of Clearview, for instance in media reports. For data subjects this does not constitute any safeguard against unwanted consequences.

122 The AP did not find any evidence either of other safeguards that have been put in place.

Balancing of interests

123 On the basis of all the above-mentioned circumstances, the AP comes to the conclusion that 1) the interests and fundamental rights of data subjects are most seriously infringed, 2) data subjects do not have or do not need to have reasonable expectations about their personal data being processed by Clearview and 3) Clearview has put insufficient safeguards in place to reduce the consequences for data subjects.

124 In contrast to all this is the interest that Clearview relies on in their privacy statement of 29 January 2020, consisting of performing commercial activities through the processing of personal data. Even if it were assumed that this interest could be a legitimate interest, it cannot be given the same importance as the interests and fundamental rights of data subjects requiring the protection of their personal data. The interests of the data subjects override Clearview's own interest to perform commercial activities, as the interests of the data subjects go (much) further beyond merely capitalizing on the processing of personal data. Taking this into consideration, but also the seriousness of the infringement set out above, not having a reasonable expectation of the processing operation and the circumstance that Clearview has put insufficient safeguards in place to reduce the consequences for data subjects, the AP can only draw the conclusion that the interests of data subjects have to prevail over Clearview's alleged - and unsubstantiated - legitimate interests.

3.4.4.4 Conclusion as regards the balancing of interests

125 The AP therefore concludes that the interests, fundamental rights and freedoms of the data subjects requiring the protection of personal data, override the interests on which Clearview rely. Relying on the

legal basis of legitimate interest would - if it were to be assessed - fall through on the basis of the third condition.

126 Considering the consequences the processing operation has for the data subjects, the seriousness of the infringement and Clearview not having put safeguards in place that would sufficiently limit the consequences for data subjects, the AP comes to the conclusion that in this case the interests of data subjects prevail over Clearview's interest.

3.4.5 Conclusion as regards the lawfulness (Articles 5 and 6 GDPR)

127 Clearview does not comply with any of the three cumulative conditions so as to be able to rely successfully on the legal basis of legitimate interest. Consequently, Clearview do not have a lawful legal basis for the processing operations of personal data. As from 13 January 2019[31], Clearview has therefore in any case acted unlawfully as they acted contrary to Article 5(1), opening words and subsection (a) GDPR, read in conjunction with Article 6(1) GDPR.[32] To date, Clearview has not ceased this violation.

3.5 Lawfulness: Article 9 GDPR

3.5.1 Legal framework

128 To the extent relevant here, Article 9(1) GDPR stipulates that: "Processing of [...] biometric data for the purpose of uniquely identifying a natural person [...] shall be prohibited."

129 From recital 51 of the GDPR it follows that personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms, merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. According to this recital, such personal data should not be processed, unless processing is allowed in specific cases set out in the GDPR.

130 To the extent relevant here, Article 9(2) GDPR stipulates that: "Paragraph 1 shall not apply if one of the following applies:
a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
(...)
e) processing relates to personal data which are manifestly made public by the data subject".

[31] The AP uses this date as starting date of the violation because it follows from the oldest privacy statement of 13 January 2019 that the processing operations by Clearview already took place at that moment.
[32] This follows from Clearview's privacy statement of 1 January 2019, see marginal number 151.

131 There is question of 'data manifestly made public' within the meaning of Article 9(2) subsection (e) GDPR, when the data subject intended, explicitly and by clear affirmative action to make the personal data in question accessible to the general public.[33]

3.5.2 Factual findings

132 From section 2.1 it follows that Clearview converted collected and uploaded photos into vectors through facial recognition technology with the purpose of unambiguously identifying data subjects for the benefit of Clearview users.

133 Clearview's privacy statement says that Clearview, as part of their business activities, collects publicly accessible photos from the internet with the purpose of offering products and services, improving products and services and training algorithms.

134 The publicly accessible photos from the internet collected by Clearview, are converted into a vector and together with metadata, if any, are stored in the database. Users of the service can go through this database.

3.5.3 Legal assessment

135 It is an established fact that the processing operations by Clearview are connected to the application of facial recognition technology to the photos either collected by Clearview and/or uploaded by users. The personal data that are the result of these processing operations qualify as biometric data within the meaning of Article 4, opening words and paragraph 14 GDPR, and thus constitute 'a special category of personal data' as referred to in Article 9 GDPR.

136 The above means that the ban on this type of processing operations as laid down in Article 9(1) GDPR applies unless one of the grounds for exception listed in the second paragraph of that Article applies. In that connection the AP notes that according to the CJEU, Article 9(2) GDPR must be interpreted strictly.[34]

137 Neither in the privacy statements examined nor anywhere else, does Clearview rely on any of the grounds for exception listed in Article 9(2) GDPR.

138 In the case in hand, only the ground for exception listed in Article 9(2), opening words and subsection (e) GDPR might be relevant. This exception only applies to data that are manifestly made public by the data subject. This is the case, as considered above, if the data subject intended, explicitly and by clear affirmative action, to make the personal data in question accessible to the general public.

[33] CJEU 4 July 2023, C-252/21, ECLI:EU:C:2023:537, para. 77.
[34] See e.g. CJEU 4 July 2023, C-252/21, ECLI:EU:C:2023:537, para. 76.

139 The other grounds for exception listed in Article 9(2) GDPR evidently do not apply in this case. As already ascertained in marginal number 77, the data subjects' consent is not obtained, so that the ground for exception stated in Article 9(2), opening words and subsection (a) GDPR is not applicable either.

140 The AP takes the view that the ground for exception listed in Article 9(2), opening words and subsection (e) does not apply either. The mere circumstance that the personal data referred to above are found online, does not mean that data subjects had the intention of making all those data accessible to the general public, explicitly and by clear affirmative action. For instance, this is not even the case when a photo (of the face) of a data subject is placed on the internet by a third party. Also, the situation in which a user has put their social media profile in private mode and this user does not have the possibility to protect their profile photo (or is not aware of such possibilities), does not constitute manifestly making public as referred to above. After all, there is no question of that user explicitly and by clear affirmative action having intended to make their personal data accessible to the general public.

3.5.4 Conclusion as regards lawfulness (Article 9 GDPR)

141 Now that Clearview cannot rely on any of the grounds for exception listed in Article 9(2) GDPR, Clearview has in any case been acting contrary to Article 9(1) GDPR since 13 January 2019[35], on account of processing a special category of personal data (biometric data) of data subjects who are within the territory of the Netherlands. To date, Clearview has not ceased this violation.

3.6 Transparency obligations: Articles 5, 12 and 14 GDPR

3.6.1 Legal framework

142 Article 5(1), opening words and subsection (a) GDPR stipulates that personal data have to be processed in a transparent manner in relation to the data subject. Transparency, along with lawfulness and fairness, is one of the basic principles of the processing of personal data.

143 In recital 60 of the GDPR it says that the principles of transparent processing require that the data subject be informed of the existence of the processing operation and its purposes.

144 In addition thereto, recital 39 of the GDPR says that data subjects should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.

145 In the Guidelines on transparency under Regulation (EU) 2016/679 (hereinafter: Transparency Guidelines) it is emphasized that one of the central considerations of the transparency and fairness principles is that data subjects should be able to determine in advance what the scope and consequences of

[35] See footnote 31

the processing entails and they should not be taken by surprise at a later point about the ways in which their personal data have been used.[36]

146 Article 12(1) GDPR stipulates that the controller takes appropriate measures in order for the data subjects to receive the information relating to the processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information will be provided in writing or by other means.

147 In Article 14(1) and (2) GDPR, the concrete substantive requirements have been laid down with which controllers have to comply in terms of informing data subjects where the information has not been obtained directly from the data subject. The Transparency Guidelines elucidate the nature, scope and content of these requirements.[37] As Clearview does not receive the personal data from the data subjects directly, but through other (public) sources, such as social media platforms, Article 14 GDPR is leading in the assessment whether Clearview complies with the GDPR transparency obligations.

148 In the Transparency Guidelines it says that data controllers should present the information efficiently and succinctly in order to avoid information fatigue, and that this information should be clearly differentiated from other non-privacy related information. In addition thereto, the information should be provided in as simple a manner as possible, avoiding complex sentences and language structures. The information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations. In particular the purposes of, and legal basis for processing the personal data should be clear.[38]

3.6.2 Factual findings

149 The AP examined four different versions of the privacy statement of Clearview:
- the privacy statement including the latest amendments on 29 December 2022 (the most recent privacy statement);
- the privacy statement including the latest amendments on 20 March 2021;
- the privacy statement including the latest amendments on 29 January 2020; and
- the privacy statement including the latest amendments on 13 January 2019.

150 The AP compared these four documents with the requirements laid down in Article 14 GDPR. The result of this comparison is included in the table below:

[36] Transparency Guidelines, marginal number 10.
[37] Transparency Guidelines, marginal number 23 ff.
[38] Transparency Guidelines, marginal numbers 8-13.

Date
16 May 2024

Our reference

Type of information	Privacy statement 29-12-2022	Privacy statement 20-3-2021	Privacy statement 29-1-2020	Privacy statement 13-1-2019
The identity and contact details of the controller Art. 14(1) subsection (a)	+	+	+	+
Contact details Data Protection Officer Art. 14(1) subsection (b)	-	-	+	+
The purposes of and legal basis for the processing operation Art. 14(1) subsection (c)	-	-	+/- (the possible grounds are indeed mentioned, but no reference is made to Arts. 6 and 9 GDPR)	+/- (the possible grounds are indeed mentioned, but no reference is made to Arts. 6 and 9 GDPR)
The categories of personal data Art. 14(1) subsection (d)	+	+	+	+
The recipients of the data Art. 14(1) subsection (e)	-	-	-	-
Details of transfers to third countries Art. 14(1) subsection (f)	-	-	- (the possibility of international transfer is indeed mentioned, but not to which countries)	- (the possibility of international transfer is indeed mentioned, but not to which countries)
Retention periods Art. 14(2) subsection (a)	+	+	-	-
The legitimate interests of Clearview Art. 14(2) subsection (b)	-	-	-	-
Rights of data subjects Art. 14(2) subsection (c)	-	- (access only)	+	+
The right to withdraw consent at all times Art. 14(2) subsection (d)	N/A	N/A	N/A	N/A

The right to lodge a complaint with a supervisory authority Art. 14(2) subsection (e)	-	-	+	-
The source from which the personal data originate Art. 14(2) subsection (f)	-	-	-	-
The existence of automated decision-making Art. 14(2) subsection (g)	N/A	N/A	N/A	N/A

151 The four different Clearview privacy statements describe how Clearview uses the information and which information Clearview collects from (1) the users of Clearview products, (2) Clearview's business contacts (for instance Clearview's service providers and processors) and of (3) 'others online'. This is how the four privacy statements make it clear that Clearview processes photos that are publicly available on the internet (as well as the metadata, such as geographical location, that come with it), personal data of users (such as name and contact details) and data of individuals who provided Clearview with their data themselves (for instance in the context of an access request). Clearview gives a limited description of the reason as to why they process this information (see marginal number 152 below) and in any case without referring to the specific grounds (and legitimate interests, if any) listed in Articles 6 and 9 GDPR. In the two most recent privacy statements, Clearview answers the question of how long the data are subsequently retained as follows: "as long as possible to carry out the purposes".

152 The 'general' reason Clearview gives for these processing operations is that they collect these data for providing their products and services. In the most recent privacy statement (dated 29 December 2022), the following is stated about the specific processing of the template (vectors) and the photos themselves:

Face vectors and photos, and such metadata as image files may contain (sensitive personal information).	From the Internet	**SOLD** We may have sold this category of personal information to law enforcement, governmental agencies, authorized contractors of law enforcement or government agencies, security and national security professionals. Please note: Clearview does not provide any third party with access to face vectors Clearview produces. **SHARE** We have not shared this category of personal information for cross-context behavioral advertising. **SERVICE PROVIDERS, CONTRACTORS OR PROCESSORS** We may have disclosed this category of personal information with service providers, contractors or processors who provide us with certain services, such as cloud storage and other technology services. **PURPOSE OF PROCESSING** We process this personal information to provide our services to customers and to cooperate with our customers' investigation, research, or fulfillment of their government duties concerning conduct or activity that the Customer or Clearview reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations . For more details regarding our use and disclosure of this category of personal information, please see **Why Do We Collect Data?** and **Who Do We Disclose Data To?** sections above.

153 According to the privacy statement, the reason for this specific processing operation is providing services to Clearview clients, such as government authorities, investigative services or other public/private security services. In that way, Clearview collaborates in investigations of their clients into the possible violations of federal or local laws and regulations, or so Clearview says. Apart from the photos originating from public sources ('From the internet'), the privacy statements do not clarify which specific sources Clearview uses for that purpose. The first two privacy statements the AP found on the web (dated 13 January 2019 and 29 January 2020) state the following about the use of photos: "Clearview does not compile, analyze, combine with other data, or otherwise process the images we collect in order to link them to real persons on behalf of users."

154 The extract above (under marginal number 152) also illustrates that Clearview does not share personal data ensuing from the (templates) of the collected photos with third parties for online purposes, but they do share them with service providers, suppliers and processors. All four Clearview privacy statements the AP studied, include a short elucidation regarding the question when Clearview provides personal data to said third parties. In none of the cases are the specific categories of recipients or the recipients themselves mentioned. It is also unclear to which countries outside the United States the data are transferred, and which safeguards apply in such instances.

155 In relation to mentioning the rights of data subjects, the privacy statements show a turnaround over time. The privacy statements of 20 March 2021 and 29 December 2022 (the two most recent privacy statements) do not state what constitute the rights of data subjects and the manner in which data subjects can take steps to exercise such rights. However, there are separate web pages for the citizens of California, Virginia and Illinois with specific forms for submitting for instance access, rectification and/or deletion requests.

Nor do the privacy statements mention that the data subject has the right to lodge a complaint with a supervisory authority. The privacy statements of 29 January 2020 and 13 January 2019 do mention all the rights data subjects have, and the privacy statement of 29 January 2020 also mentions the right to lodge a complaint with a supervisory authority.

3.6.3 Legal assessment

156 None of the privacy statements the AP assessed, comply with the transparency obligations that ensue from Article 12(1) GDPR, read in conjunction with Article 14 GDPR. The most important objection is that it is unclear to data subjects that Clearview (might) be processing their photos (including metadata) for facial recognition purposes. Data subjects may only be aware of this when they accidentally come across the name of Clearview, for instance in media reports.[39]

157 More in particular, Clearview violates these stipulations by failing to take appropriate measures in order for the data subjects to receive the following information: (1) the legal bases for processing the personal data (including a reference to the applicable provision of Article 9 GDPR), (2) the retention periods, (3) the (categories of) recipients of the data, (4) the details of transfers to third countries, (5) the rights of data subjects[40], (6) the possibility of lodging a complaint with a supervisory authority (with the exception of the privacy statement of 29 January 2020), and (7) the source from which the personal data originate (if the specific source is not mentioned: the nature of the sources and the type of organisation/industry/sector).

158 Moreover, merely placing a privacy statement on the Clearview website is not enough to comply with 'shall provide' as referred to in Article 14 GDPR. In that connection, the AP notes that Clearview, for the purpose of their services, collects personal data from public sources through untargeted scraping and stores those data, which data include photos, the URL of those photos, metadata of those photos and vectors belonging to the face (or faces) in those photos, whereas data subjects usually have not been notified thereof (beforehand or afterwards) by Clearview. Clearview should also take active steps to provide the data subject with the information in question. Article 12(1) GDPR after all prescribes that the controller provides the information referred to and that the controller takes appropriate measures to ensure that the data subject receives the information. Merely stating information on their website therefore does not suffice.

[39] Moreover, data subjects are unable to ascertain this beyond any doubt, as Clearview does not respond (any longer) to access requests, see below in section 3.7.
[40] This only applies to the privacy statements of 20 March 2021 and 29 December 2022, the version of 20 March 2021 did mention the right of access, however.

3.6.4 Conclusion as regards the transparency obligations (atricles 5, 12 and 14 GDPR)

159 The AP comes to the conclusion that since 13 January 2019, Clearview has in any case been acting contrary to Article 12(1) GDPR, read in conjunction with Article 14(1) and (2) GDPR. The AP also comes to the conclusion that by not complying with this obligation, Clearview has also violated the principles of transparency and fair data processing, as laid down in Article 5(1), opening words and subsection (a) GDPR. To date, Clearview has not ceased these violations.

3.7 (Facilitating) right of access of data subjects: Articles 12 and 15 GDPR

3.7.1 Legal framework

160 Article 12(2) GDPR stipulates that the controller shall facilitate the exercise of data subject rights under Articles 15-22 GDPR. In that context, recital 59 of the GDPR states that modalities should be provided for facilitating the exercise of the data subject's rights under the GDPR.

161 Pursuant to Article 12(3) GDPR, the controller shall provide information on action taken on a request under Articles 15-22 GDPR to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

162 Pursuant to Article 15(1) GDPR, the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data.

3.7.2 Factual findings

163 Above, the AP ascertained that Clearview's most recent privacy statement of 29 December 2022 does not mention the possibility EU citizens have to exercise their data subject rights as referred to in Articles 15-22 GDPR.[41]

164 In addition, in their reply dated 17 March 2023, Clearview informed the AP they had stopped responding to access requests: "Clearview AI does not respond to Art. 15 GDPR access requests, because it is not subject to the GDPR as we have mentioned. In the past, Clearview AI voluntarily provided European residents with information about their appearance or non-appearance in Clearview AI search results upon request. However, we have terminated that practice, both to reduce potential security risks and to better reflect the fact that Clearview AI's activities are not within the territorial scope of the GDPR. As such, Article 15 is not applicable to Clearview AI."

[41] As stated in the previous footnote, this only applies to the privacy statements of 20 March 2021 and 29 December 2022, the version of 20 March 2021 did mention the right of access, however.

165 The AP received two complaints about two access requests that were submitted to Clearview on 6 October 2022 and 20 December 2022, respectively. The complainants informed the AP that Clearview had not responded to those requests.

3.7.3 Legal assessment and conclusion as regards the rights of data subjects (Articles 12 and 15 GDPR)

166 It is an established fact that as regards the two access requests dated 6 October 2022 and 20 December 2022, Clearview did not respond to them. Consequently, Clearview violated Article 12(3) GDPR, read in conjunction with Article 15 GDPR.

167 The AP includes the violation of Article 12(3) GDPR, read in conjunction with Article 15 GDPR in the question whether Clearview also violates Article 12(2) GDPR. To that end, the AP considers the following.

168 Pursuant to Article 12(2) GDPR, the controller must facilitate the exercise of data subject rights under Articles 15. However, Clearview fails to facilitate data subjects in exercising their right of access. First of all, it has been established that as regards the two above-mentioned access requests, Clearview has not responded to them. In addition thereto, Clearview declared in reply to a question put to them by the AP, that they would not be responding to access requests any more at all. This policy was reflected in Clearview's privacy statement as amended on 29 December 2022.

169 Considering the above, the AP concludes that since 6 October 2022[42], Clearview has in any case violated Article 12(3) GDPR, read in conjunction with Article 15 GDPR, by not facilitating data subjects who are within the territory of the Netherlands in exercising their right of access. To date, Clearview has not ceased this violation.

3.8 Representative of a controller who is not established in the Union: Article 27 GDPR

3.8.1 Legal framework

170 Article 4, opening words and paragraph 17 GDPR stipulates that 'representative' means a natural or legal person established in the European Union who, designated by the controller or processor in writing pursuant to Article 27 GDPR, represents the controller or processor with regard to their respective obligations under the GDPR.

171 Article 27(1) GDPR stipulates that where Article 3(2) GDPR applies, the controller or processor designate in writing a representative in the Union. Article 27(2) GDPR stipulates that this obligation does not apply to:

[42] The AP considers October 2022 the starting date of the violations, as this is the date of the first access request on the basis of which a data subject lodged a complaint with the AP, see marginal numbers 1 and 165.

(a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) GDPR or processing of personal data relating to criminal convictions and offences referred to in Article 10 GDPR, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or
(b) a public authority or body.

172 Pursuant to Article 27(3) GDPR, the representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

3.8.2 Factual findings

173 In section 3.1.3.2, the AP already came to the conclusion that Clearview processes personal data. In addition thereto, it was found that Article 3(2) GDPR applies to Clearview and that Clearview's processing operations are related to monitoring the behaviour of data subjects in the Union.

174 The AP ascertained that Clearview has not designated a representative within the Union in connection with the processing of personal data.

175 The AP consulted the Commercial Register of the Chamber of Commerce, but did not find any companies associated to Clearview. A similar consultation of the European Justice portal (e-Justice Portal) did not result in finding a branch or representative of Clearview in the European Union either.

176 The AP asked Clearview, among other things, whether they had a branch or representative within the Union. Clearview did not respond to that question. Clearview did declare that they do not have a branch within the Union. Clearview argues that they do not have clients in the Netherlands and the Union and that they are not involved in monitoring behaviour within the Union. Also see marginal number 50 of this decision, in which Clearview informed the AP that they would no longer take access requests (by EU citizens) into consideration.

177 Clearview's website, and a search of the internet itself, do not result in finding a representative or business address of Clearview in the Union.

3.8.3 Legal assessment and conclusion as regards a representative of a controller who is not established in the Union (Article 27 GDPR)

178 As already concluded in marginal number 68 above, the processing of personal data by Clearview for the purpose of their service falls under the territorial scope of the GDPR.

179 In addition thereto, the AP ascertains that Clearview has not designated a representative in the EU as referred to in Article 4, opening words and paragraph 17 GDPR, although they are obliged to do so pursuant to Article 27(1) GDPR. The exceptions to this obligation listed in Article 27(2) GDPR do not apply as Clearview is a private party processing special categories of personal data on a large scale.

180 The AP therefore arrives at the conclusion that Clearview acts contrary to Article 27(1) GDPR. To date, Clearview has not ceased this violation.

4. Fines

181 Clearview committed the following violations:

1. Unlawful processing of personal data
   Since 13 January 2019, for the purpose of their 'Clearview for law-enforcement and public defenders' service, Clearview has in any case processed personal data of data subjects who are within the territory of the Netherlands. They have done so without a lawful legal basis, and therefore violate Article 5(1), opening words and subsection (a) GDPR, read in conjunction with Article 6(1) GDPR (hereinafter also: violation 1). To date, Clearview has not ceased this violation.

2. Unlawful processing of special personal data
   Since 13 January 2019, for the purpose of their 'Clearview for law-enforcement and public defenders' service, Clearview has in any case violated Article 9(1) GDPR by processing a special category of personal data (biometric data) of data subjects who are within the territory of the Netherlands (hereinafter also: violation 2). To date, Clearview has not ceased this violation.

3. Violation of the transparency obligation
   Since 13 January 2019, Clearview has in any case violated Article 12(1) GDPR, read in conjunction with Article 14(1) and (2) GDPR, as well as Article 5(1), opening words and subsection (a) GDPR, by failing to take appropriate measures in order for data subjects who are within the territory of the Netherlands to receive all information as referred to in Article 14 GDPR (hereinafter also: violation 3). To date, Clearview has not ceased this violation.

4. Brushing aside two access requests
   Clearview violated Article 12(3) GDPR, read in conjunction with Article 15 GDPR, by erroneously not responding to two access requests by data subjects (hereinafter also: violation 4).

5. Not facilitating data subjects in exercising their right of access
   Since 6 October 2022, Clearview has in any case violated Article 12(2) GDPR, read in conjunction with Article 15 GDPR, by not facilitating data subjects who are within the territory of the Netherlands

in exercising their right of access (hereinafter also: violation 5). To date, Clearview has not ceased this violation.

6. Not designating a representative in the Union
Clearview violates Article 27(1) GDPR by not designating a representative in the Union as referred to in Article 4, opening words and paragraph 17 GDPR (hereinafter also: violation 6). To date, Clearview has not ceased this violation.

182 Pursuant to Article 58(2), opening words and paragraph (i) GDPR, in conjunction with Article 83 GDPR, and read in conjunction with Article 14(3) GDPR Implementation Act (hereinafter: GDPRIA), the AP has the authority to impose an administrative fine. CJEU case law shows that from the wording of Article 83(2) GDPR it follows that infringements of the GDPR provisions that have been culpably committed by the controller - meaning infringements that were committed intentionally or negligently - may result in an administrative fine being imposed on the controller pursuant to said Article.[43] In this case, there are culpable forms of conduct on the part of Clearview for which the AP will impose fines.

183 The AP takes the view that imposing fines is not only appropriate but also necessary, as Clearview has violated the rights and freedoms of citizens in various ways. The AP considers this a serious matter and therefore proceeds to imposing fines for violations 1-5.

184 Because violation 5 (not facilitating data subjects in exercising their right of access) necessarily leads to violation 4 (not responding to two access requests), the AP imposes one fine for these two violations.

185 Considering Article 50 of the Charter of Fundamental Rights of the European Union (hereinafter: the Charter) and Article 5:43 of the Dutch General Administrative Law Act (hereinafter: DGALA), the AP refrains from imposing a fine for violating Article 27(1) GDPR (violation 6, not designating a representative in the Union), as Clearview has already been fined for that violation by the Italian and the Greek Data Protection Authorities, respectively. These decisions have already become final.[44]

Guidelines on the calculation of administrative fines

186 In the plenary meeting of 24 May 2023, the EDPB agreed to the adoption of the final text of the Guidelines 04/2022 on the calculation of administrative fines under the GDPR (hereinafter: the Guidelines on the calculation of administrative fines).[45] The AP will apply these Guidelines to this case.[46] The AP's (national)

[43] CJEU 5 December 2023, C-683/21, ECLI:EU:C:2023:949 (*NVSC*), paras. 73 and 83; CJEU 5 December 2023, C-807/21, ECLI:EU:C:2023:950 (*Deutsche Wohnen*), paras. 68 and 76.
[44] Compare the decision of the Dutch Central Appeals Tribunal of 3 July 2018 (ECLI:NL:CRVB:2018:2059), legal grounds 4.1-4.5. Also see CJEU 14 September 2023, C-27/22, ECLI:EU:C:2023:265.
[45] Also see Guidelines 04/2022 on the calculation of administrative fines under the GDPR.
[46] Also see https://www.autoriteitpersoonsgegevens.nl/actueel/nieuw-boetebeleid-voor-overtredingen-avg

policy rules on determining the amount of administrative fines are not applicable to violations of the GDPR committed by undertakings.[47]

4.1 Methodology for determining the amount of the fine

187 The Guidelines on the calculation of administrative fines describe the following method for calculating administrative fines for infringements of the GDPR:

1. Identifying which and how many processing operations and infringements are to be decided on.
2. Defining the starting amount for the further calculation of the fine;
3. Evaluating aggravating and mitigating circumstances that require the fine to be increased or decreased;
4. Identifying which maximum amounts apply to the infringements and whether those maximum amounts are not exceeded due to increases applied in previous or next steps;
5. Analysing whether the final amount of the calculated fine meets the requirements of effectiveness, dissuasiveness and proportionality, and adjusting the fine accordingly.

188 These steps will consecutively be gone through. In section 4.2, the AP will go into the starting amounts for the violations. In section 4.3, the AP will assess the mitigating or aggravating circumstances for the violation. In conclusion, the AP will assess in section 4.4 whether the statutory fine maximum is exceeded and whether the fines are effective, dissuasive and proportionate.

4.2 Starting amounts for the violations

4.2.1 Step 1: Identifying the processing operations and defining infringements

189 As described in the Guidelines on the calculation of administrative fines, in order to determine the starting amount for calculating the fine, it must first be determined whether one or more sanctionable forms of conduct are at issue.

190 First of all, the AP found that for the benefit of their 'Clearview for law-enforcement and public defenders' service, Clearview processes personal data of data subjects who are within the territory of the Netherlands, and that Clearview does so without a lawful basis. In doing so, Clearview violated Article 5(1), opening words and subsection (a) GDPR, in conjunction with Article 6(1) GDPR (violation 1, unlawful processing of personal data). In addition thereto, the AP came to the conclusion that for the purpose of said service, Clearview violated Article 9(1) GDPR by processing a special category of personal data (biometric data) of data subjects who are within the territory of the Netherlands (violation 2, unlawful processing of special personal data).

[47] See https://www.autoriteitpersoonsgegevens.nl/documenten/boetebeleidsregels-autoriteit-persoonsgegevens-2023

191 The AP further concluded that Clearview violates Article 12(1) GDPR, read in conjunction with Article 14(1) and (2) GDPR, as well as Article 5(1), opening words and subsection (a) GDPR by failing to take appropriate measures in order for data subjects who are within the territory of the Netherlands to receive all information as referred to in Article 14 GDPR (violation 3, violation of the transparency obligation). In addition thereto, the AP came to the conclusion that Clearview violates Article 12(2) GDPR, read in conjunction with Article 15 GDPR, and Article 12(3) GDPR, read in conjunction with Article 15 GDPR by not facilitating data subjects who are within the territory of the Netherlands in exercising their right of access by not responding to access requests (violations 4 and 5).

192 Although individually subject to a fine, the violations as regards the lawfulness of the processing operation (violations 1 and 2, unlawful processing of - special - personal data) as well as the violation relating to failing to take appropriate measures in order for data subjects to receive all information as referred to in Article 14 GDPR (violation 3, violation of the transparency obligation), should be considered as infringements regarding the same or linked processing operations as referred to in Article 83(3) GDPR. After all, this article stipulates that where a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of the GDPR, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement. The AP will take this into account when setting the final amount of the fine (see section 4.3).

193 However, violations 4 and 5 (not responding to two access requests, and not facilitating data subjects in exercising their right of access, respectively), each constitute a separate sanctionable form of conduct. First of all, the AP takes in consideration the fact that at a later point in time (namely in 2022) Clearview decided not to respond to access requests any longer. Second of all, this form of conduct does not necessarily relate to the same group of data subjects. After all, not every data subject whose personal data are being processed or to whom the privacy statement applies, will make an access request.

4.2.2 Step 2: Starting amounts

194 The starting amount is the basis for the further calculation of the amount of the fine in the subsequent steps, taking all relevant facts and circumstances into account. The Guidelines on the calculation of administrative fines state that the starting amount is determined on the basis of three elements: i) the categorisation of infringements by nature under Article 83(4)-(6) GDPR; ii) the seriousness of the infringement; and iii) the turnover of the undertaking. All three elements will be discussed below.

Re i) the categorisation of infringements by nature under Article 83(4)-(6) GDPR

195 As stated in the Guidelines on the calculation of administrative fines, nearly all obligations of the controller are categorized in the provisions of Article 83(4)-(6) GDPR. The GDPR distinguishes between two types of infringements. On the one hand, the infringements that are sanctionable under Article 83(4) GDPR, and for which a maximum fine of € 10 million applies (or in the case of an undertaking, 2% of the

undertaking's annual turnover, whichever is higher), and on the other hand, the infringements that are sanctionable on the basis of Article 83(5) and (6) GDPR, and for which a maximum fine of € 20 million applies (or in the case of an undertaking, 4% of the undertaking's annual turnover, whichever is higher). By making this distinction, the legislator provided a first indication, in the abstract, of the seriousness of the infringement: the more serious the infringement, the higher the fine.

196 In this case, considering Article 83(5) GDPR and to the extent this is relevant here, an administrative fine of up to € 20 million can be imposed for the violations 1-5. From this categorization it follows that the legislator considers those infringements to be serious.

Re ii) Seriousness of the infringements

197 When determining the seriousness of the infringement, the nature, gravity and duration of the violation, as well as the intentional or negligent character of the infringement and the categories of personal data involved must be taken into account.

Nature of the infringements

198 As regards the nature of violations 1 and 2 (unlawful processing of - special - personal data) the AP notes the following. Article 6 GDPR is an elaboration on the principle of lawfulness as laid down in Article 5 GDPR. This is one of the six basic principles of the GDPR and consequently a fundamental requirement for the protection of personal data. The principle of lawfulness ensures the data subjects' control over their personal data. By violating this principle, said control is harmed. In addition thereto, Article 9 GDPR affords an extra high level of protection to data of which the processing may involve situations in which a serious risk may arise due to the consequences such processing may have for the data subjects. This risk is deemed so harmful that the processing of these data is prohibited unless an exception applies.

199 The nature of violations 1 and 2 in this case relates to the unlawful processing of (biometric) personal data of data subjects. These articles represent the conditions for lawfulness and therefore the fundamental requirements for processing under the GDPR. In relation to the nature of these violations, it should furthermore be taken into account that the processing operations relate to special categories of personal data, namely biometric data, regarding which a higher level of protection applies.

200 As regards the nature of violations 3, 4 and 5 (violation of the transparency obligation and violations of - the duty to facilitate - the right of access, respectively), the AP notes that the controller has to provide the data subject with the information required to guarantee a fair and transparent processing vis-à-vis the data subject, with due observance of the specific circumstances and the context within which the personal data are being processed. Data subjects have the right to receive all information referred to in Article 14(1)

and (2) GDPR so as to enable them to exercise their other rights under the GDPR. Right of access is necessary to enable data subjects to exercise their other rights under the GDPR. A controller has to facilitate a data subject in exercising their right of access. In this case, there is no question of the latter as currently it is Clearview's policy not to respond to access requests. When a controller does not comply with these obligations, it impacts the right data subjects have to their private life being respected and their personal data being protected.

Gravity of the violations

201 As regards the gravity of violations 1 and 2 (unlawful processing of - special - personal data), the AP first of all notes that the unlawful processing operations are at the core of Clearview's business activity. Clearview does not occasionally process different kinds of personal data for facial recognition purposes, they do so systematically and on a large scale. In this process, Clearview makes use of personal data from a large number of sources which data are being combined and analysed in a database. In addition thereto, said database is constantly being enriched with new personal data. It offers users the opportunity to go through data about individuals, obtain a detailed picture of the lives of these individuals and follow their behaviour. For data subjects, these processing operations are far-reaching and may even have adverse consequences for them. Clearview carries out these processing operations without the consent of data subjects and without Clearview having a legitimate interest. The unlawful processing operations moreover relate to a very large number of data subjects in the Netherlands, including minors, who deserve special protection vis-à-vis a controller. The AP also takes the invisible nature of the processing into account. After all, data subjects usually are not aware of the processing operation and in all fairness they do not need to expect their personal data to be processed in this way. Data subjects might only become aware of it when they accidentally come across the name of Clearview, for instance in media reports or on Clearview's website (on which the processing operations are described in general terms only).

202 In substantiation of the gravity of violations 3, 4 and 5 (violation of the transparency obligation and violations of - the duty to facilitate - the right of access, respectively), the AP notes - in addition to what has been considered in the previous marginal number - that because in the context of their business activity Clearview processes (biometric) personal data in a way that is deeply far-reaching for data subjects, it is of great importance that Clearview is also transparent about the processing of those personal data, that data subjects have the right to access the personal data Clearview has collected about them and that it is easy for them to exercise that right. The AP considers it a grave matter that Clearview has actually made it impossible for data subjects to exercise their right of access and does not provide data subjects with all information listed in Article 14 GDPR. The AP takes note of the fact that Clearview included some information in their privacy statement/policies.

Duration of the violations

203 As regards the duration of violations 1 and 2 (unlawful processing of - special - personal data), the AP ascertained that the unlawful processing (that is contrary to Articles 6 and 9 GDPR) has in any case been taking place since 13 January 2019 and continues to this day. The same goes for violation 3 (violation of the transparency obligation). It regards a considerable period. The AP considers it a grave matter that Clearview still have not ceased violations 1, 2 and 3.

204 The AP also had to conclude that Clearview has in any case not facilitated data subjects in exercising their right of access (violation 5) since 6 October 2022, and that said violation continues to this day. The latter violation may have started at a later date than violation 3 (violation of the transparency obligation), but it resulted in a further reduction of the control data subjects have over the processing of their personal data. The fact that Clearview has not ceased violation 5 (not facilitating data subjects in exercising their right of access), is also something the AP considers a grave matter.

Degree of culpability of the violations

205 As regards the intentional or negligent character of the infringements, the AP takes notice of the circumstance that Clearview purposefully tried to place themselves beyond the legal system of the GDPR, whereas Clearview is aware of the fact that they knowingly collect photos of Dutch citizens from public sources by means of scraping and store those photos, on the basis of which they subsequently make a vector of the individual(s) shown in the photos. That way, individuals can be identified and monitored. This, in addition to the fact that several supervisory authorities in the Union have ascertained various instances of Clearview infringing the GDPR, does not only prove that Clearview was aware of the fact that their conduct was contrary to the GDPR, they moreover knowingly continued said conduct even after those other supervisory authorities in the Union had imposed sanctions on them. The majority of those sanctions had been imposed even before the AP started their investigation into Clearview. Under those circumstances, it is the opinion of the AP that this is not a matter of negligence, but a matter of deliberate intent.

Categories of personal data to which the infringements relate

206 To conclude with, the AP considers that Clearview processes special (biometric) personal data within the meaning of Article 9 GDPR, which is an aggravating circumstance.

Conclusion as regards the seriousness of the infringements

207 Considering the above-mentioned circumstances, the AP comes to the conclusion that violations 1-5 regard grave violations - in the category 'infringements of a high level of seriousness', as referred to in the Guidelines on the calculation of administrative fines.

Re iii) The turnover of the undertaking

208 From Article 83(5) GDPR it follows that for violations 1-5 an administrative fine of up to € 20 million can be imposed on Clearview.

209 As noted in marginal number 64 of the Guidelines on the calculation of administrative fines, it is fair that the starting amounts to be determined reflect a distinction of the size of the undertaking and also factor in the undertaking's turnover.

210 However, the AP also points out that despite repeated requests by the AP, Clearview absolutely did not provide any information about their turnover. In doing so, Clearview knowingly deprives the AP of the possibility to consider Clearview's turnover in the sanctions and factor it in. For that reason, the AP feels compelled to start from the maximum fine of € 20 million.

Conclusion as regards starting amounts for the violations

211 As explained above, this is a case of serious violations in the category of 'infringements of a high level of seriousness'. According to the Guidelines on the calculation of administrative fines, in the calculation of the administrative fine for such infringements, it holds good that the supervisory authority sets the starting amount for further calculation at a point between 20% and 100% of the maximum fine of in this case € 20 million. This corresponds to an amount of between
€ 4 million and € 20 million. According to the Guidelines on the calculation of administrative fines, the general rule that applies is that the more serious the infringement within its own category, the higher the starting amount will be.

212 Taking the above into account, the AP finds that as regards violations 1 and 2 (unlawful processing of - special - personal data), the starting amount for the calculation of the fine has to be considerably high.

213 As regards the violations 3, 4 and 5 (violation of the transparency obligation and violation of - the duty to facilitate - the right of access) it was concluded that these are also serious violations. The AP finds that the starting amounts for those violations should therefore be high as well. The fact that Clearview included some information in their privacy statements will be taken into account by the AP as regards violation 3 (violation of the transparency obligation).

4.3 Assessment of mitigating or aggravating circumstances for the violations

214 According to the Guidelines on the calculation of administrative fines, it should then be analysed whether the circumstances of the case give reason to set the fine higher or lower than the starting amount

determined for this purpose. The circumstances to be taken into account are stated in Article 83(2), opening words and subsections (a)-(k) GDPR. The circumstances set out in that provision should only be taken into account once. In the previous step - to the extent that it applies - the nature, gravity and duration of the violations (subsection a), the intentional or negligent character of the infringement (subsection b) and the categories of personal data (subsection g) have already been taken into account. This leaves subsections (c)-(f) and (h)-(k).

215 One of the applicable circumstances is to what extent the supervisory authority was cooperated with to remedy the infringement and limit its possibly adverse effects (subsection f).

216 In that connection, the AP considers it an aggravating circumstance that, despite the above-mentioned interventions of various supervisory authorities (within and outside of the EU), Clearview has not taken any measure to make their activities GDPR-compliant, Clearview has taken the view that they are not subject to the GDPR and refused to answer questions by the AP. The AP apportions this aggravating circumstance for the fine equally to (i) violation 1, (ii) violation 2, (iii) violation 3 and (iv) violations 4 and 5.

217 There is no evidence of the other circumstances stated in Article 83(2), opening words and subsections (c) and (e) and (g)-(k) GDPR, nor do they give reason to increase or lower the fine.

4.4 Assessment of the fine maximum (Article 83(3) GDPR) and whether the fines are effective, proportionate and dissuasive

218 In section 4.2.1 above, the AP found that violations 1, 2 and 3 (unlawful processing of - special - personal data and violation of the transparency obligation, respectively) should be considered as infringements that relate to the same or linked processing operations as referred to in Article 83(3) GDPR.

219 Considering Article 83(3) GDPR[48] and the fact that infringements are subject to monetary fines pursuant to Article 83(5) GDPR, the AP sets the fine for those violations at € 20,000,000.

220 As set out above in marginal number 193, violations 4 and 5 (not responding to two access requests and not facilitating data subjects in exercising their right of access, respectively) do not constitute a separate infringing form of conduct, for which reason these violations are not subject to Article 83(3) GDPR. Taking this into consideration, the AP sets the fine for those infringements at € 10,500,000.

[48] Article 83(3) GDPR stipulates that: 'where a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement'.

Fines are effective, proportionate and dissuasive

221 To conclude with, the AP will assess whether the fines are effective, proportionate and dissuasive and whether the legal maximum of the fine is exceeded. Also pursuant to Articles 3:4 and 5:46(2) of the DGALA, the administrative fine should not lead to a disproportionate outcome considering the circumstances of the specific case. This has also been laid down in Article 49 of the Charter.

222 Pursuant to Article 83(5), opening words and subsections (a) and (b) GDPR, the AP can impose an administrative fine for the above-mentioned violations. As described in the Guidelines on the calculation of administrative fines, imposing a fine can be considered effective if it achieves the objectives for which it was imposed. This purpose could on the one hand be to punish unlawful forms of conduct, and on the other hand be to foster compliance with the applicable rules. Considering the nature, gravity and duration of the infringements, as well as the other factors stated in Article 83(2) GDPR as assessed above, the AP finds that imposing administrative fines under these circumstances achieves both objectives and therefore is effective and dissuasive. The AP considers the amount of the administrative fines effective and dissuasive as well, also taking the circumstance into consideration that Clearview absolutely refused to provide information about the turnover achieved by them.

5. Orders subject to a penalty for non-compliance

223 The AP establishes for a fact that Clearview still has not ceased the unlawful processing operations. In addition thereto, Clearview still does not comply with the requirements of transparency ensuing from Article 12(1) GDPR, read in conjunction with Article 14 (1) and (2) GDPR. Clearview still fails to facilitate data subjects in exercising their right of access and Clearview still has not designated a representative in the Union.

224 Clearview has to end these violations as soon as possible. For this reason, the AP imposes four orders subject to a penalty for non-compliance. The AP does so pursuant to Article 58(2), opening words and subsection (d) GDPR and Article 16(1) GDPRIA read in conjunction with Article 5:32(1) DGALA.

225 For processing personal data in the context of the 'Clearview for law-enforcement and public defenders' service, the AP orders Clearview:

I. to end and not resume the violation of Article 5(1), opening words and subsection (a) GDPR, read in conjunction with Article 6(1) GDPR (violation 1, unlawful processing of personal data), as well as the violation of Article 9(1) GDPR (violation 2, unlawful processing of special personal data). Clearview can do so by demonstrably ending the processing of personal data of data subjects who are within the territory of the Netherlands and by removing the personal data that Clearview unlawfully obtained.

II. to end and not resume the violation of Article 12(1) GDPR, read in conjunction with Article 14(1) and (2) GDPR, as well as Article 5(1), opening words and subsection (a) GDPR (violation 3, violation of the transparency obligation). Clearview can do so by as yet demonstrably actively and fully provide data subjects, who are within the territory of the Netherlands, with the information as referred to in Article 14 GDPR in a concise, transparent, intelligible and easily accessible form.

III. to end and not resume the violation of Article 12(2) GDPR, read in conjunction with Article 15 GDPR (violation 5, not facilitating data subjects in exercising their right of access). Clearview can do so by demonstrable cessation of their policy of not responding to access requests by data subjects who are within the territory of the Netherlands.

IV. to end and not resume the violation of Article 27(1) GDPR (violation 6, not designating a representative in the Union). Clearview can do so by demonstrably in writing designating a representative in the Union as referred to in Article 4, opening words and paragraph 17 GDPR.

226 For order II, the AP refers to the Transparency Guidelines. These Guidelines provide examples of how a controller can provide information in a concise, transparent, intelligible and easily accessible form.

227 The AP attaches the following compliance periods and penalties for non-compliance to the above-mentioned orders. When determining the compliance periods, the AP took the estimated time that Clearview will need to comply with the orders into consideration. As regards the amount of the penalty for non-compliance, Article 5:32(2) DGALA stipulates that the amounts of a penalty for non-compliance should be reasonably proportionate to the gravity of the interest violated and to the intended effect of the penalty for non-compliance. In terms of the latter, it is important that a penalty for non-compliance must give such an incentive as to comply with the order.[49] Any benefit an offender gains from a violation, may be relevant and taken into account when determining the amount of the penalty for non-compliance.[50]

Order I: compliance period and amount of the penalty for non-compliance

228 The AP attaches a compliance period of three months to order I (ending the violations relating to the lawfulness of the processing operation and violating the ban on processing special personal data). If Clearview decides to end the processing of personal data of data subjects who are within the territory of the Netherlands in the context of the 'Clearview for law-enforcement and public defenders' service, this can be effected on short notice. The AP considers a compliance period of three months sufficient to do so.

[49] For instance see the decision by the Administrative Jurisdiction Division of the Dutch Council of State of 17 July 2013, ECLI:NL:RVS:2013:343, legal ground 9.1. and the decision by the Administrative Jurisdiction Division of the Dutch Council of State of 19 April 2017, ECLI:NL:RVS:2017:1100, legal ground 4.2.
[50] For instance see the decision by the Administrative Jurisdiction Division of the Dutch Council of State of 6 February 2019 (ECLI:NL:RVS:2019:321), legal ground 4.2.

229 If Clearview does not end the violation found within three months, they will forfeit, upon expiry of said compliance period, a penalty for non-compliance for each month (or part of a month) that the order has not, or not fully, been complied with. The AP will set the amount of this penalty for non-compliance at a sum of € 250,000 (in words: two hundred and fifty thousand Euro) for each month upon expiry of the compliance period, to a total maximum sum of € 1,500,000 (in words: one million five hundred thousand Euro). When determining the amount of the penalty for non-compliance, the AP considered that it regards a large-scale and long-term violation of the GDPR's principle that personal data are only allowed to be processed if there is a legal basis to do so and that in addition thereto Clearview unlawfully processes a special category of personal data (biometric data).
The amount of the penalty for non-compliance is also based on the circumstance that Clearview obtains financial benefits from the processing operation in violation of the GDPR.

Order II: compliance period and amount of the penalty for non-compliance

230 The AP attaches a compliance period of three months to order II (ending the violation relating to the transparency obligation). Clearview will need time to provide data subjects who are within the territory of the Netherlands with the information in accordance with Article 12(1) GDPR, read in conjunction with Article 14(1) and (2) GDPR. Clearview can take online measures to provide data subjects with all information in a concise, transparent, intelligible and easily accessible form. It is within Clearview's power to take theses measures. Taking the above into account, the AP considers three months sufficient.

231 If Clearview does not end the violation found within three months, they will forfeit, upon expiry of said compliance period, a penalty for non-compliance for each month (or part of a month) that the order has not, or not fully, been complied with. The AP will set the amount of this penalty for non-compliance at a sum of € 250,000 (in words: two hundred and fifty thousand Euro) for each month upon expiry of the compliance period, to a total maximum sum of € 1,500,000 (in words: one million five hundred thousand Euro). When determining the amount of the penalty for non-compliance, the AP took the extent of the violation into account as well as the fact that a provision that is part of one of the GDPR's principles, namely the transparency principle, has been violated. It is important that data subjects will be fully and clearly informed as quickly as possible about the processing of their personal data.

Order III: compliance period and amount of the penalty for non-compliance

232 The AP attaches a compliance period of one month to order III (ending the violation relating to how access requests are dealt with). Should Clearview decide to cease their policy of not responding to access requests by data subjects, this can be effected on short notice. The AP considers a one-month compliance period sufficient to that end.

233 If Clearview does not end the violation found within one month, they will forfeit, upon expiry of said compliance period, a penalty for non-compliance for each month (or part of a month) that the order has not, or not fully, been complied with. The AP will set the amount of this penalty for non-compliance at a

sum of € 250,000 (in words: two hundred and fifty thousand Euro) for each month upon expiry of the compliance period, to a total maximum sum of € 1,500,000 (in words: one million five hundred thousand Euro). When determining the amount of the penalty for non-compliance, the AP took the extent of the violation into account as well as the interest data subjects have in being able to exercise their right of access as quickly and as easily as possible, as exercising that right of access is necessary for enabling data subjects to exercise their other rights under the GDPR.

Order IV: compliance period and amount of the penalty for non-compliance

234 The AP attaches a compliance period of three months to order IV (ending the violation of not having designated a representative in the Union). The AP takes the view that this period gives Clearview sufficient opportunity to end the violation.

235 If Clearview does not end the violation found within three months, they will forfeit, upon expiry of said compliance period, a penalty for non-compliance for each month (or part of a month) that the order has not, or not fully, been complied with. The AP will set the amount of this penalty for non-compliance at a sum of € 200,000 (in words: two hundred thousand Euro) for each month upon expiry of the compliance period, to a total maximum sum of € 600,000 (in words: six hundred thousand Euro). When determining the amount of the penalty for non-compliance, the AP took the large-scale processing of (a special category of) personal data into account as well as the interest placed in the fact that a representative acts on behalf of a controller and can be approached by any supervisory authority.

Preventing the forfeiture of the penalties for non-compliance

236 If Clearview wishes to prevent the forfeiture of the penalties for non-compliance, documentary evidence demonstrating that they have complied with the orders will have to be submitted by them to the AP in a timely fashion.

Final conclusions

On the basis of what is stated above in this decision, the AP first of all finds that for the purpose of the 'Clearview for law-enforcement and public defenders' service, Clearview AI Inc. has no legal basis for the processing of personal data of data subjects who are within the territory of the Netherlands. In doing so, Clearview AI Inc. violates Article 5(1), opening words and subsection (a) GDPR, read in conjunction with Article 6(1) GDPR.
The AP also finds that for the purpose of said service, Clearview AI Inc. unlawfully processes a special category of personal data, namely biometric data, of data subjects who are within the territory of the Netherlands. In doing so, Clearview AI Inc. violates Article 9(1) GDPR.
The AP also comes to the conclusion that Clearview AI Inc. fails to take appropriate measures in order for data subjects who are within the territory of the Netherlands to receive all information as referred to in Article 14 GDPR. In doing so Clearview AI Inc. acts contrary to Article 12(1) GDPR, read in conjunction with Article 14(1) and (2) GDPR, and contrary to Article 5(1), opening words and subsection (a) GDPR.

The AP also finds that Clearview AI Inc. erroneously did not respond to two access requests by data subjects and that Clearview AI Inc. erroneously fails to facilitate data subjects who are within the territory of the Netherlands in exercising their right of access by not responding to access requests. In doing so, Clearview AI Inc. violates Article 12(3) GDPR, read in conjunction with Article 15 GDPR, and Article 12(2) GDPR, read in conjunction with Article 15 GDPR.

The AP comes to the conclusion that the ascertained infringements of rights and freedoms of data subjects are serious and therefore proceeds to enforcement towards Clearview AI Inc. The AP imposes the following measures:

6. Decision

Fines

I. The AP imposes an administrative fine in the amount of € 20,000,000 (in words: twenty million Euro) on Clearview AI Inc. for violating
- Article 5(1), opening words and subsection (a) GDPR, read in conjunction with Article 6(1) GDPR,
- Article 9(1) GDPR, and
- Article 12(1) GDPR, read in conjunction with Article 14(1) and (2) GDPR, as well as Article 5(1), opening words and subsection (a) GDPR.

II. The AP imposes an administrative fine in the amount of € 10,500,000 (in words: ten million five hundred thousand Euro) on Clearview AI Inc. for violating Article 12(2) and (3) GDPR, read in conjunction with Article 15 GDPR.[51]

Orders subject to a penalty for non-compliance

For processing personal data in the context of the 'Clearview for law-enforcement and public defenders' service, the AP orders Clearview AI Inc.:

I. to end and not resume the violation of Article 5(1), opening words and subsection (a) GDPR, read in conjunction with Article 6(1) GDPR as well the violation of Article 9(1) GDPR. Clearview AI Inc. can do so by demonstrably ending the processing of personal data of data subjects who are within the territory of the Netherlands and by removing the personal data that Clearview AI Inc. unlawfully obtained.

[51] The AP will pass on the claims for collection to the Dutch Central Judicial Collection Agency (CJIB). The AP will not proceed to the collection of the fines until any legal (follow-up) proceedings about this decision have been concluded.

Upon the expiry of the three-month compliance period after publication of this decision, Clearview AI Inc. will forfeit a penalty for non-compliance of € 250,000 (in words: two hundred and fifty thousand Euro), for each month (or part of a month) that the order has not, or not fully, been complied with up to a maximum of € 1,500,000 (in words: one million five hundred thousand Euro).

II. to end and not resume the violation of Article 12(1) GDPR, read in conjunction with Article 14(1) and (2) GDPR, as well as Article 5(1), opening words and subsection (a) GDPR. Clearview AI Inc. can do so by as yet demonstrably actively and fully provide data subjects, who are within the territory of the Netherlands, with the information as referred to in Article 14 GDPR in a concise, transparent, intelligible and easily accessible form.

Upon the expiry of the three-month compliance period after publication of this decision, Clearview AI Inc. will forfeit a penalty for non-compliance of € 250,000 (in words: two hundred and fifty thousand Euro), for each month (or part of a month) that the order has not, or not fully, been complied with up to a maximum of € 1,500,000 (in words: one million five hundred thousand Euro).

III. to end and not resume the violation of Article 12(2) GDPR, read in conjunction with Article 15 GDPR. Clearview can do so by demonstrable cessation of their policy of not responding to access requests by data subjects who are within the territory of the Netherlands.

Upon the expiry of the one-month compliance period after publication of this decision, Clearview AI Inc. will forfeit a penalty for non-compliance of € 250,000 (in words: two hundred and fifty thousand Euro), for each month (or part of a month) that the order has not, or not fully, been complied with up to a maximum of € 1,500,000 (in words: one million five hundred thousand Euro).

IV. end and not resume the violation of Article 27(1) GDPR. Clearview can do so by demonstrably in writing designating a representative in the Union as referred to in Article 4, opening words and paragraph 17 GDPR.

Upon the expiry of the three-month compliance period after publication of this decision, Clearview AI Inc. will forfeit a penalty for non-compliance of € 200,000 (in words: two hundred thousand Euro), for each month (or part of a month) that the order has not, or not fully, been complied with up to a maximum of € 600,000.00 (in words: six hundred thousand Euro).

Date
16 May 2024

Our reference

Yours sincerely,
Autoriteit Persoonsgegevens,

Mr A. Wolfsen, LLM
chair

Remedy clause

If you do not agree with this decision, you can submit a notice of objection to the Autoriteit Persoonsgegevens, within six weeks of the date the decision was sent. You can do so by regular post or digitally. Pursuant to Article 38 Dutch General Data Protection Regulation (Implementation) Act, submitting a notice of objection defers the effect of the decision to impose the administrative fine. For submitting a digital notice of objection, go to www.autoriteitpersoonsgegevens.nl, under the caption Contact, item "Bezwaar of klacht over de AP".[52]

The postal address for submitting an objection by regular post is:

Autoriteit Persoonsgegevens
P.O. Box 93374
2509 AJ The Hague, The Netherlands.

Please state 'AWB objection' on the envelope and mention 'Notice of objection' in the title of your letter.

In your notice of objection you should at least state:
- your name and address;
- the date of your notice of objection;
- the reference (case number) stated in this letter, or enclose a copy of this decision;
- the reason(s) why you do not agree with this decision;
- your signature.

[52] The direct URL is <https://www.autoriteitpersoonsgegevens.nl/over-de-autoriteit-persoonsgegevens/bezwaar-maken>.