HELLENIC DATA
PROTECTION AUTHORITY

Athens, 13-07-2022

Ref. No: 1809

DECISION 35/2022

The Hellenic Data Protection Authority convened remotely on 19-04-2022, following the meeting of 29-03-2022, following an invitation of its President, to examine the case mentioned in the present case history. The President of the Authority, Konstantinos Menoudakos and the regular members of the Authority, Grigorios Tsolias and Christos Kalloniatis as rapporteurs, Spyridon Vlachopoulos, Konstantinos Lambrinoudakis, Charalambos Anthopoulos and Aikaterini Iliadou attended. Present, without voting rights, were Fotini Karvela, Maria Alikakou, Anastasia Kaniklidou, Kyriaki Karakasi, legal auditors — lawyers, as well as Georgios Roussopoulos and Pantelis Kammas, IT auditors, as assistant rapporteurs and Eirini Papageorgopoulou, employee of the Administration Department, as secretary.

The Authority took into account the following:

Ref. No. G/IN/3458/26-05-2021 complaint submitted to the Authority by the non-profit civil organization named 'Homo Digitalis' on behalf of the complainant, A, is in principle a complaint of a breach of A's right of access vis-à-vis the United States-based company Clearview AI (St.214 W 29th St,2nd Floor, New York City, NY, 10001). That complaint, which also seeks an examination, on the whole, of the practices of the defendant company from the point of view of the protection of personal data, was submitted simultaneously with four other relevant complaints before the supervisory authorities of Austria, France, Italy and the United Kingdom, aiming to a coordinated response to the practices of that company by the competent supervisory bodies.

In the context of the present case, the complainant sent an e-mail to the company concerned on 24 March 2021, exercising her right of access under Article 15 of the General Data Protection Regulation (Regulation (EU) 2016/679 — GDPR) to her personal data processed by

that company, while on the same date she received confirmation of the successful receipt of that request by the recipient. Afterwards, on 26 April 2021, the complainant reintroduced the above request with a reminder message to the defendant. On 30 April 2021, the complainant was informed by a representative of Clearview AI that the request submitted by email had not been detected and was asked to attach a photograph of her, so that her request is forwarded as urgent, if she had used an e-mail address other than the one through which she made the request for the first time. On 5-5-2021 and in response to the above, the complainant sent an electronic confirmation of receipt of her request from the defendant dated 24 March 2021, while on 26 May 2021 she submitted the complaint in question to the Authority.

The Authority, in its examination of the above complaint, by Ref. no. G/IN/4752/16-07-2021 document addressed the defendant company and, after recalling the provisions of Articles 3(2) and 27 of the GDPR on the territorial scope of the GDPR and on representatives of controllers or processors not established in the European Union (hereinafter: EU), asked the company for information on the details of its representative in the EU, if it is based in a country outside the EU. In the event that the company has an establishment within the EU, a series of questions were submitted concerning the identity of the controller or processor for the processing in question, the possibility of more than one establishment of the controller or processor on the territory of the EU and the indication of the main establishment in the event of more than one such establishment. In addition, and further to the above questions, clarification of the nature of the processing as cross-border was requested either in the sense that it is carried out in the context of the activities of any several establishments of the defendant in several Member States, or in the sense that it affects or is likely to substantially affect data subjects in several Member States. Finally, the above questions also included information as to whether the complainant exercised a right as a data subject and, if so, what was the defendant's response to it and within which deadline.

Then, by Ref. No. G/IN/5303/16-08-2021, the defendant company, after claiming that it is not subject to the GDPR, stated that it is based in the U.S. and does not have an establishment in the EU. It then challenged the application of Article 3(2) of the GDPR, since it allegedly does not provide products or services to data subjects within the EU, nor does it monitor the behavior of data subjects within the EU. The defendant stressed that its services are provided

to government law enforcement authorities outside the EU, while denying that the creation by its own search engine of links to photos available online constitutes monitoring of the behavior of data subjects, as these are instant image projections without any systematic/continuing observation of each person. According to the defendant, there is no GDPR implementation scope, as it has a search engine that automatically displays results on the basis of the most relevant algorithm in relation to the question introduced by a third party. In fact, the defendant concluded that there was a breach of public international law in the event that a company providing online services is obliged to comply with all laws worldwide. Then, and in the context of bona fide and voluntary assistance, as noted by the complainant, in relation to the present case, it confirmed that the request for access was made on 24 March 2021 by the complainant, who also submitted a reminder message on 26-4-2021. It then referred to the existence of a technical problem which prevented its representative from reading the file submitted by the complainant with her photograph in order to respond to her request, and although the company's standard practice in such cases is to request a photograph from the subject again, in the present case, it inadvertently replied to the complainant by sending the standard e-mail for cases where the request itself is not detected. Finally, the defendant stated that it had complied with the request for access by allegedly sending its reply to the complainant. However, it should be noted that by a supplementary letter from the complainant with ref. no. G/IN/4976/22-03-2022 it appears that she had received no reply from the defendant.

All the information in the file shows the following for the company in question:

Clearview AI, Inc. is based in the United States and was founded in 2017. Its unique product is a facial recognition platform, which allows users to associate photos of faces present in the company's database with photos of them on the internet. Its platform, according to what is stated on its website[1] *"is supported by facial recognition technology and includes the largest known database containing more than ten (10) billion facial images from public online sources, including news, websites, signage photos, public social media and other public sources".*

[1] https://www.clearview.ai/overview (retrieved 26/5/2022 — translation from English)

This complaint states that according to publicly available sources[2] and the conclusions reached by other EU supervisory authorities, which have examined similar complaints against Clearview AI, Inc.,[3] the facial recognition tool provided by the defendant operates as follows:

1. The company collects, through the use of 'web scraping' techniques, images containing human faces from social networks (particularly Facebook and Twitter), blogs and generally websites on which publicly accessible photos are available, as well as videos available online (e.g. YouTube). Together with these images, the company also collects information it extracts from these photos, including geolocation metadata that the photo may contain and information derived from the appearance of the person's face in the photos[4]. This information is stored in Clearview's database.

2. The company processes the images using special techniques, so that every person shown in a photograph is converted into a certain numerical sequence, which is called "vector" and is recognizable by machines.

3. The above numerical sequences are stored in the company's database and are fragmented for the listing of the database and for future identification of persons. Thus, each person in the database has a separate vector and a fragmented value associated with it.

4. When a user of Clearview services wants to identify a person, they post an image and perform a search. Clearview analyses this image and extracts a vector for the face on the image, which then fragments and compares against all fragmented vectors stored in its database. Finally, the company extracts each identified image from its database and provides a list of results, containing all the corresponding images and metadata. If a user clicks on any of these results, he/she is directed to the source page of the image.

---

[2] See Joint Investigation of Clearview by the Data Protection Supervisory Authorities of Canada, Quebec, British Columbia and Alberta, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/#toc7. See also the U.S. Patent and Trade Marks Register: https://tmsearch.uspto.gov/bin/showfield?f=doc&state=4803:tnmzul.2.1

[3] See decision of the Supervisory Authority for the Protection of Personal Data of Hamburg https://noyb.eu/sites/default/files/2021-01/545_2020_Anh%C3%B6rung_CVAI_ENG_Redacted.PDF. Decision of the Garante https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en. Decision of CNIL https://www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet.

[4] See (at the date of the meeting) Clearview AI Privacy Policy, Inc. https://www.clearview.ai/privacy-policy

Finally, the Authority, by Ref. no. G/OUT/887/11-4-2022 document, called the defendant company, sending at the same time a translation into English of the complaint at issue, so that it can be heard in the videoconference of 19-4-2022 of the Plenary of the Authority. However, the defendant did not appear and subsequently the Authority proceeded to the examination of the file and, after hearing the rapporteurs and the clarifications from the assistant rapporteurs, and after a thorough discussion,

DELIBERATED ACCORDING TO THE LAW

1. In accordance with Article 3(2)(b)GDPR, "*this Regulation applies to the processing of personal data of data subjects located in the Union by a controller or processor not established in the Union, if the processing activities relate to: b) monitoring their behavior to the extent that such behavior takes place within the Union.*"

In that regard, recital 24 of the GDPR provides, in relation to the inclusion of a processing within the territorial scope of the GDPR on the basis of Article 3(2)(b), that *"... in order to determine whether a processing activity can be considered to monitor the conduct of a data subject, it should be ascertained whether individuals are tracked online, including the potential subsequent use of personal data processing techniques consisting of shaping a natural person's 'profile', in particular with a view to making decisions concerning him or her or analyzing or predicting his or her personal preferences, behaviors and attitudes."*

The EDPB Guidelines 3/2018 on the territorial scope of the GDPR clarify in this regard that *"contrary to the provision of Article 3(2)(a), neither Article 3(2)(b) nor recital 24 explicitly establishes a required degree of "targeting intention" on the part of the controller or processor in order to determine whether the monitoring activity could trigger the application of the GDPR to the processing activities. However, using the word "monitoring" implies that the controller has a specific intention in mind to collect and subsequently re-use the relevant data on a person's behavior within the EU. The EDPB does not consider that any online collection or analysis of personal data in the EU is automatically regarded as 'monitoring'. It is necessary to examine the purpose of the controller for the processing of the data and, in particular, for*

any subsequent use of behavioral analysis or profiling techniques that include such data. The EDPB takes into account the wording of recital 24, which states that in determining whether the processing can be considered to monitor the behavior of a data subject, a key parameter is to monitor individuals online, including the potential subsequent use of profiling techniques."

2. Article 4 par. 1 GDPR defines personal data as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3. Furthermore, in accordance with Article 4 par. 4 profiling means "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects of a natural person, in particular to analyses or predict aspects relating to the performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements of that natural person*".

In this regard, the Guidelines on automated decision-making and profiling for the purposes of Article 29 Working Party Regulation 2016/679 specify that profiling must: (a) be an automated form of processing, (b) relate to personal data, and (c) assess personal aspects of a natural person, while stressing *that "the widespread availability of personal data on the internet and from Internet of Things (IoT) devices, as well as the ability to find associations and establish links, may enable the identification, analysis and prediction of aspects of a natural person's personality or behavior and interests and habits*"[5].

4. According to Article 4(14) GDPR, biometric data means "*personal data resulting from specific technical processing linked to the physical, physiological or behavioral characteristics of a natural person and which allow or confirm the unequivocal identification of that natural person, such as facial images or dactyloscopic data".*

[5] Guidelines on automated decision-making and profiling for the purposes of Article 29 Working Party Regulation 2016/679, WP251Rev.01, 3 October 2017 as finally revised and adopted on 6 February 2018, p. 5, 7, https://ec.europa.eu/newsroom/article29/items/612053

In addition, according to Article 9(1) GDPR, the special categories of personal data requiring special protection include biometric data for the purpose of the unambiguous identification of a person.

In that regard, recital 51 of the GDPR states that photographs of persons are covered by the definition of biometric data only in the case of processing by means of specific technical means allowing unambiguous identification or verification of a natural person's identity.

5. According to Article 55(1) GDPR, "*each supervisory authority shall be competent to carry out the tasks and exercise the powers conferred on it in accordance with this Regulation in the territory of its Member State*".

Article 56(1) GDPR stipulates that "*without prejudice to Article 55, the supervisory authority of the main or single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing operations of that controller or processor in accordance with the procedure laid down in Article 60*".

The GDPR cooperation mechanism (art. 60 et seq. GDPR) applies only in the case of a controller or processor with one or more establishments in the EU[6]. Similarly, recital 122 of the GDPR states that "*Each supervisory authority should be competent, in the territory of its Member State, to exercise the powers and perform the tasks conferred on it in accordance with this Regulation. This should cover in particular processing (...) carried out by a controller or processor not established in the Union, when targeting data subjects residing in its territory*".

Therefore, in the case of a controller without an establishment in the EU, which falls within the scope of the GDPR on the basis of the targeting criterion set out in Article 3(2) GDPR, each national supervisory authority is competent to verify its compliance with the GDPR on the territory of its Member State.

6. Where Article 3(2) GDPR applies, Article 27 provides that the controller is obliged to designate in writing a representative in the EU, who must be established in one of the Member States where the data subjects are located, whose data are processed in connection

[6] See Guidelines of Art. 29 WP for the identification of the lead authority of a controller or processor, WP 244, https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=44102

with an offer of goods or services to them or whose conduct is monitored, unless one of the exceptions provided for in paragraph 2 of that Article 27 applies.

The representative, as explained in recital 80, must act on behalf of the controller, and any supervisory authority may be addressed to him. The representative shall be appointed by written instruction of the controller to act on its behalf in respect of its obligations under the GDPR. The EDPB Guidelines 3/2018 on the territorial scope of the GDPR stipulate that this mainly entails obligations relating to the exercise of the rights of data subjects, and in this context the provision of the representative's identity and contact details to data subjects in accordance with the provisions of Articles 13 and 14 GDPR. Although he/she is not responsible for complying with the rights of data subjects, the representative should facilitate communication between the subjects and the represented controller in order to ensure the effective exercise of the rights of the subjects. As explained in recital 80, the representative should also be subject to enforcement procedures in case of non-compliance by the controller. This means, in practice, that it must be ensured that a supervisory authority is able to communicate with the representative on any matter relating to the compliance obligations of a controller established outside the EU and that the representative must be able to facilitate any exchange of information or procedures between the requesting supervisory authority and the controller or processor established outside the EU.

7. Article 5(1) of the GDPR lays down the principles that should govern a processing operation. In particular, paragraph 1 provides that: *"1. Personal data are: (a) processed lawfully and fairly in a transparent manner in relation to the data subject ("lawfulness, objectivity and transparency"), [...] (e) kept in a form that allows the identification of the data subjects only for the period necessary for the purposes of the processing of personal data ("limitation of the storage period").* In order to ensure that the data are kept no longer than necessary, recital 39 clarifies that the controller should set deadlines for their deletion or for their periodic review.

In accordance with the principle of accountability introduced by the second paragraph of that Article, it is expressly stated that the controller "*shall be responsible and able to demonstrate compliance with paragraph 1 ("accountability"*). This principle, which is a cornerstone of the GDPR, entails the obligation for the controller to be able to demonstrate compliance,

including the legal documentation of any processing operation carried out in accordance with the legal bases provided by the GDPR and national data protection law.

Any processing of personal data shall be lawful only if at least one of the conditions set out in Article 6(1) GDPR applies, such as: "*(a)* the data subject has consented to the processing of his or her personal data for one or more specific purposes*; (b) the processing is necessary for the performance of a contract to which the data subject is party or to take measures at the request of the data subject prior to entering into a contract; (c) processing is necessary to comply with a legal obligation of the controller; (d) the processing is necessary to safeguard the vital interest of the data subject or other natural person; (...),(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, unless those interests override the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular if the data subject is a child*." If one of the above conditions is met, it is also the legal basis for processing.

In that regard, with the principle of transparency, recital 39 of the GDPR provides, inter alia, that *"it should be clear to individuals that personal data concerning them are collected, used, taken into account or otherwise processed, and to what extent personal data are or will be processed. That principle requires that any information and communication relating to the processing of such personal data be easily accessible and understandable and use clear and simple language"*. As also stated in recital 60, which refers to the rights of information, which implement, inter alia, the principle of transparency[7], "*the principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes*".

8. Furthermore, as stated in recital 51 of the GDPR, special categories of data require special protection, since the context of their processing could create significant risks to fundamental rights and freedoms. While, therefore, in order for the processing of "simple" personal data to be lawful, it is sufficient to have one of the legal bases of Article 6, the processing of special categories of data is, in principle, prohibited and allowed only if one of the legal bases of Article 6 and one of the exceptions of Article 9(2) GDPR apply. This view is endorsed both by Opinion 6/2014 of Article 29 WP on the concept of legitimate interests of the controller under

[7] See also the Transparency Guidelines under Regulation 2016/679 of Art. 29 WP, WP 260, p. 7.

Article 7 of Directive[8] 95/46 and by the EDPB in its Guidelines 8/2020 on targeting social media users[9]. It is therefore not lawful to process special categories of data if Article 6 is not adhered to and only the exceptions referred to in Article 9 are met. In this spirit, Article 29 WP Opinion 6/2014 on the concept of legitimate interests of the controller in Article 7 of Directive 95/46 states that *"it would be wrong to conclude that the fact that someone has manifestly disclosed specific categories of data pursuant to Article 8(2)(e) of Directive 95/46 (now Article 9(2)(e) GDPR) would be — always in itself — a sufficient condition to allow any kind of data processing without an assessment of the balancing of the interests and rights at stake, as required by Article 7(f) of Directive 95/46 (now Article 6(1)(f) of the GDPR*)[10].

9. The right to information enshrined in Articles 13 and 14 GDPR provides, where the data have not been collected from the data subject (art. 14(3)(a) that the controller shall provide the information referred to in paragraphs 1 and 2 (identity of controller, purposes and legal basis for processing, categories of data, etc.) *"within a reasonable period of time from the collection of personal data, but no later than one month, taking into account the specific circumstances in which the personal data are processed*". In particular, as clarified by the Transparency Guidelines under Regulation 2016/679 of the Art. 29 WP, "*the data subject should be able to determine in advance the scope of the processing and the consequences it entails, and should not be surprised at a later stage as to the ways in which his or her personal data have been used".*

10. According to Article 15(1), (3) and (4) of the GDPR "*1. 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, if so, the right of access to personal data to the following information"*.

Article 12(2), (3) and (4) GDPR provides that *"The controller shall facilitate the exercise of the rights of data subjects provided for in Articles 15 to 22. [...]* 3. *The controller shall provide the data subject with information on the action taken on request pursuant to Articles 15 to 22*

[8] See Opinion 6/2014 on the concept of legitimate interests of the controller within the meaning of Article 7 of Directive 95/46, p. 14.
[9] See Guidelines 8/2020 on targeting social media users, p. 40.
[10] See CJEU, C-13/16, Valsts *policijas Rīgas repiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'*, 4 May 2017, concerning the cumulative conditions to be satisfied in order for data processing to be lawful on the basis of 'legitimate interests'.

without delay and in any event within one month of receipt of the request. That period may be extended by a further two months, if necessary, taking into account the complexity of the request and the number of requests. The controller shall inform the data subject of such extension within one month of receipt of the request and of the reasons for the delay. [...] 4. If the controller does not act on the data subject's request, it shall inform the data subject within one month of receipt of the request of the reasons why it did not act and of the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy".

11. In the present case, as it is apparent from the defendant's privacy policy (available at https://www.clearview.ai/privacy-policy), the latter collects *"Information derived from publicly available photos: As part of Clearview's normal business operations, it collects photos that are publicly available on the Internet. Clearview may extract information from those photos including such geolocation metadata as the photo may contain and information derived from the facial appearance of individuals in the photos*.

Those photographs are indisputably personal data as defined in Article 4(1) GDPR, in so far as they allow the identification of a natural person by reference to one or more factors specific to his or her physical or physiological identity. The same conclusion has been reached by the CJEU, which has held that *"the image of a person recorded by a camera constitutes personal data within the meaning of that provision (Article 2(a) of Directive 95/46) in so far as it enables the person* concerned *to be identified."*[11]

Furthermore, it follows from the defendant's privacy policy that it collects photographs that are publicly available on the internet without applying any geographical selection criterion. This wideness of the collection is an inherent feature of the service which the defendant sells. It is worth noting that in previous versions of its privacy policy, it explicitly[12] stated that it collects data from subjects located in the EU.

12. As regards the link between the defendant's processing activities and the monitoring of the behavior of subjects in the EU, it is crucial whether these subjects are monitored online.

The processing, carried out by the defendant, results in the production of a search outcome — on the basis of a photograph posted by the user of its services — which contains all the

[11] Case C-212/2013, František Ryneš v Úřad pro ochranu osobních údajē.
[12] In force on 29.1.2020.

photographs that have a shared fragmented vector with the photo posted by the user. In this way, a profile is created about a person, which consists of the photographs in which that person appears, as well as their metadata, i.e. the URLs of the websites where those photos are located. The association of these photographs and the context in which they are presented on a website allows the collection of much information about the person, his/her habits and preferences. In particular, when a photo is posted on social networks or on a website that publishes articles, or on a blog, this may result in the collection of information that allows the person's behavior to be determined. The analysis of the above information that a person chooses to make public on the internet and the context in which he or she chooses to make it public, ultimately enables that person's online behavior to be determined on the basis of his or her own personal or professional life exposure options.

Consequently, the automated processing of personal data described above for the purpose of assessing the personal aspects of a natural person constitutes profiling and the making available to users of the defendant's services, who search the defendant's facial recognition platform, constitutes surveillance on the internet. Moreover, the purpose of the tool marketed by the defendant is to enable the identification and collection of information in relation to a particular person. Biometric processing techniques used by the defendant to enable a person to be targeted ultimately lead to profiling as a result of a search by a user of the defendant's tool. This search is renewed over time, as the database is constantly updated, which makes it possible to establish the possible evolution of information relating to a particular person, in particular if the results of successive searches are compared with each other.

13. Clearview AI, Inc., is based in the United States and has no establishment in the EU. The GDPR cooperation mechanism (art. 60 et seq. GDPR) applies only in the case of a controller or processor with one or more establishments in the EU[13]. Similarly, recital 122 of the GDPR states that "*Each supervisory authority should be competent, in the territory of its Member State, to exercise the powers and perform the tasks conferred on it in accordance with this Regulation. This should cover in particular processing (....) carried out by a controller or processor not established in the Union, when targeting data subjects residing in its territory*".

[13] See Guidelines of Art. 29 WP for the identification of the lead authority of a controller or processor, WP 244, https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=44102

Therefore, in the case of Clearview AI, Inc., which does not have an establishment in the EU but falls within the scope of the GDPR on the basis of the targeting criterion set out in Article 3(2) GDPR, each national supervisory authority is competent to verify compliance with the GDPR on the territory of its Member State, as stated above.

14. Furthermore, in the present case, since Clearview AI, Inc. falls within the scope of the GDPR, under Article 3(2)(b) without having an establishment in the EU, it is obliged to appoint a representative in the EU in accordance with Article 27 GDPR, but has not fulfilled it.

15. In the present case, the data subjects whose data are processed by the defendant do not receive any information from the defendant, through that privacy policy, in relation to any of the elements referred to in Article 14 GDPR, either before or even after the processing. In fact, data subjects may never learn that their data has been processed by the defendant unless they randomly read a publication about Clearview AI, Inc.

16. The principle of the lawfulness of processing has the meaning that, in order to be lawful, the processing to which the data are subject must be based on one of the legal bases provided for in Article 6 GDPR.

In the present case, none of the documents in the file reveals the existence of any of the legal bases provided for in Article 6.

In particular, it is not established —neither would it be possible on the basis of the characteristics of the processing in question— that there is consent of the subjects (6 (1)(a) GDPR), or performance of a contract between the data subject and the controller (6(1)(b) GDPR), or compliance with a legal obligation of the controller (6(1)(c) GDPR), or the safeguarding of a vital interest of the subject (6(1)(d) GDPR).

As regards, in particular, the possible application of the legal basis referred to in paragraph 1(f) of this Article, it is provided that processing is lawful where it is necessary for the purposes of the legitimate interests pursued by the controller or a third party, provided that the interests or fundamental rights and freedoms of the data subject which require the protection of personal data do not prevail over those interests. In relation to that provision, recital 47 of the GDPR states that, after balancing the legitimate interests of the controller or third party and the interests or fundamental rights of the subject, the legitimate interests of the former must not prevail over the interests or rights of the data subject, taking into account the

legitimate expectations of the data subject on the basis of his or her relationship with the controller.

The legitimate expectations of the data subject in relation to the processing of his or her data are highlighted as a factor taken into account in the above balancing also by the WP of Article 29 in Opinion 6/2014 on the concept of the legitimate interests of the controller under Article 7 of Directive 95/46. The same Opinion also clarifies that personal data are still considered personal data and subject to the necessary protection requirements, even if they have become public. That said, the fact that personal data is publicly available can be considered a critical factor when assessing legitimate interests, especially if the publication was made with a reasonable expectation of re-use of the data for specific purposes (e.g. for research purposes or for purposes related to transparency and accountability).

In the present case, given that there is no relationship between the subjects and the defendant, nor can there be any reasonable expectation of the subjects that their online photographs will be processed by a facial recognition platform, the existence of which they are likely to be unaware of, the conditions for the application of Article 6(1)(f) GDPR are not fulfilled.

From all the information brought to the attention of the Authority, it emerged that the processing in question does not concern a simple collection of data, but results in the conversion of the photographs collected into biometric data, the processing of which is subject to the strictest provisions of Article 9 GDPR. In that regard, bearing in mind that the processing of special categories of data is in principle prohibited and permitted only if one of the legal bases referred to in Article 6 and one of the exceptions set out in Article 9(2) GDPR cumulatively apply and that none of the legal bases of Article 6 GDPR exist in relation to the processing of critical data, it appears that the processing of biometric data carried out by the defendant does not meet the legal requirements laid down by the GDPR.

17. From the information brought to the attention of the Authority, it emerged that, although the complainant exercised the right of access to her personal data under Article 15 GDPR, via e-mail to the defendant on 24 March 2021, with which the defendant agrees (ref. no. G/IN/5303/16.08.2021 its reply to the Authority), however, she has never received any reply and her right of access has never been satisfied by the defendant, in accordance with document with ref. no. G/IN/4976/22.03.2022 from the complainant to the Authority and

contrary to what the defendant claims in its above letter to the Authority, in which it states that it sent the complainant a standardized message.

18. In the light of the above, from the information in the file, the Authority finds on behalf of the complainant company, Clearview AI, Inc.:

A) Breach of the obligation to designate a representative in the EU (Article 27 GDPR) because, although the defendant falls within the scope of the GDPR, under Article 3(2)(b) without having an establishment in the EU and is therefore obliged to appoint a representative in the EU in accordance with Article 27 GDPR, it has not fulfilled its obligation.

B) Breach of the principle of the lawfulness of processing (Article 5(1)(a), 6 and 9 GDPR), because the processing carried out by the defendant is not based on any legal basis from the provisions of Article 6 GDPR, while none of the exceptions of Article 9 GDPR apply with regard to the special categories of data.

C) Breach of the principle of transparency of processing (Article 5(1)(a) GDPR) and of the related right of information of the subjects (Article 14 GDPR), because the defendant did not, as required, inform the subjects whose data is processed accurately and clearly about the collection and use of their personal data.

D) Breach of the complainant's right of access (Articles 12 and 15 GDPR), because the defendant did not comply with the request made by the complainant, as set out above.

19. In the light of the above, the Authority considers that it is appropriate to exercise its corrective powers under Articles 58(2)(i) and 83 GDPR (imposition of a fine) in respect of all the above infringements, its corrective powers under Article 58(2)(c) of the GDPR with regard to the satisfaction of the complainant's right of access and its corrective powers under Article 58(2)(g) and (f) with regard to the erasure of personal data of subjects located in the Greek territory and the prohibition of their processing. In determining the fine, which the Authority considers to be effective, proportionate and dissuasive, account shall be taken of the measurement criteria set out in Article 83(2) GDPR applicable in the present case, as interpreted in particular by the Guidelines *on the application and setting of administrative fines for the purposes of Regulation* 2016/679 of the Article 29 Working Party.

Especially, particular account shall be taken of:

A) the nature, gravity and duration of the infringement, which is not an isolated incident, but is systematic and concerns the basic principles of the lawfulness of the processing (art. 5, 6, 9 GDPR), which are fundamental to the protection of personal data, in accordance with the GDPR. It should be pointed out that compliance with the principles laid down in Article 5 of the GDPR is of paramount importance, and above all, the principle of lawfulness, so that, if it does not exist, the processing would be unlawful from the outset, even if the other principles of processing have been adhered, especially in the present case where none of the legal bases for the processing referred to in Articles 6 and 9 of the GDPR has not been established, as set out above.

B) the number of affected subjects in the Greek territory, which due to the data collection techniques used by the defendant is potentially very high. Indeed, it does not follow from the privacy policy of the defendant and the way in which personal data is collected that a relevant technique is applied which excludes some of the photographs of individuals with specific criteria.

C) The fact that the processing at issue concerns special categories of personal data (biometric).

D) The degree of responsibility of the defendant, which is high, taking into account that the processing in question continues despite the intervention of supervisory authorities inside and outside the EU.

E) The failure of the defendant to cooperate with the Authority, taking into account that the defendant did not attend the meeting of the Authority even though it was invited.

F) The fact that, in accordance with the provisions of Article 83(5)(a) and (b) of the GDPR, infringement of the basic principles for processing and the rights of the subjects falls within the upper category of the system of administrative fines.

G) The fact that data on the defendant's turnover are not available to the Authority.

On the basis of the aforementioned, the Authority unanimously decides that the administrative penalty referred to in the operative part of the decision, which is deemed, as mentioned above, proportionate to the gravity of the infringement, must be inflicted on the defendant, as controller.

FOR THESE REASONS

The Authority

A. Imposes on the defendant company Clearview AI, Inc., based in the USA, 214 W 29th St, 2nd Floor, New York City, NY, 10001, as controller, on the basis of Article 58(2)(i) GDPR, a total fine of EUR 20 million (EUR 20 000 000) for breaching the principles of lawfulness and transparency (art. 5 paras 1a, 6, 9 GDPR) and its obligations under Articles 12, 14, 15 and 27 of the GDPR.

B. Orders the defendant US-based company Clearview AI, Inc., 214 W 29th St, 2nd Floor, New York City, NY, 10001, as the controller, on the basis of Article 58(2)(c) GDPR to comply with the complainant's request for the exercise of her right of access.

C. Imposes on the defendant company under the name Clearview AI, Inc., based in the USA, 214 W 29th St, 2nd Floor, New York City, NY, 10001, as the controller, on the basis of Article 58(2)(f) of the GDPR, the prohibition of the collection and processing of personal data of persons located in the Greek territory, using the methods included in the facial recognition service which it trades.

D. Orders the defendant company under the name Clearview AI, Inc., based in the USA, 214 W 29th St, 2nd Floor, New York City, NY, 10001, as the controller, on the basis of Article 58(2)(g) of the GDPR, to erase the personal data of subjects located in the Greek territory, which it collects and processes using the methods included in the facial recognition service which it trades.

The President	**The Secretary**
Konstantinos Menoudakos	**Eirini Papageorgopoulou**