Athens, 13-07-2022 Prot. No.: 1809 DECISION 35/2022 The Personal Data Protection Authority convened in a meeting via video conference on 04-19-2022, following the meeting of 03-29-2022, at the invitation of Its President, in order to examine the case referred to in the present history. The President of the Authority, Konstantinos Menudakos, and the regular members of the Authority, Grigorios Tsolias and Christos Kalloniatis, were present as rapporteurs, Spyridon Vlachopoulos, Konstantinos Lambrinoudakis, Charalambos Anthopoulos and Aikaterini Iliadou. Present, without the right to vote, were Fotini Karvela, Maria Alikakou, Anastasia Kaniklidou, Kyriaki Karakasi, legal auditors - lawyers as well as Georgios Rousopoulos and Pantelis Kammas, IT auditors, as assistant rapporteurs and Irini Papageorgopoulou, employee of the administrative affairs department, as secretary. The Authority took into account the following: With the no. prot. C/EIS/3458/26-05-2021 complaint, which was submitted to the Authority by the Civil Non-Profit Company with the name "Homo Digitalis" on behalf of the complainant, A, a violation of the right of access exercised by the latter before the registered office in the U.S. of Clearview AI (214 W 29th St, 2nd Floor, New York City, NY, 10001). The complaint in question, which also requests the examination of the practices of each company from the point of view of personal data protection, was filed at the same time as four others of related content, namely before the supervisory authorities of Austria, France, Italy and of the United Kingdom, in order to seek a coordinated response to the practices of the above company by the competent supervisory bodies. 1-3 Kifisias St., 11523 Athens, Tel: 210 6475600, Fax: 210 6475628, contact@dpa.gr / www.dpa.gr In the context of the case under consideration, the complainant sent on 03-24-2021 an email to the complained-about company, exercising the right of access to its personal data, which is processed by the said company, pursuant to Article 15 of the General Data Protection Regulation (Regulation (EU) 2016/679 – hereinafter, GDPR), while on the same date it received confirmation of successful receipt of said request by its recipient. Subsequently, on 26-04-2021, the complainant reiterated the above request with a relevant reminder message to the complainant. On 04-30-2021 the above complainant was informed by a representative of Clearview AI that her request submitted via email was not found and she was asked to attach her photo, in order to forward her request as urgent, in case she has used another e-mail address than the one through which he submitted the disputed request for the first time. The complainant, on 05-05-

2021 and in response to the above sent the 24-03-2021 electronic confirmation of receipt of her request from the defendant, while on 26-05-2021 she submitted the complaint under review to the Authority. The Authority, in the context of examining the above complaint, with no. prot. C/EIS/4752/16- 07-2021 her document, addressed the complained company and, after

reminding the provisions of articles 3 par. 2 and 27 of the GDPR regarding the territorial scope of application of the GDPR and regarding representatives of data controllers or those performing the processing of non-residents in the European Union (hereinafter: EU), requested from the company in question information about 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 number of questions were asked to be answered regarding the identity of the controller or processor for the processing under consideration, the possibility of more than one establishment of the controller or processor on the ground EU. and the indication of the main installation in case of the existence of several such. In addition, and in continuation of the above questions, clarification was requested of the nature of the processing as cross-border, either in the sense that it is carried out in the context of the activities of any more facilities of the complainant in several Member States, or in the sense that it affects or may significantly affect 2 data subjects in more Member States. Finally, the above questions also included information on whether the complainant exercised any of her rights as a data subject and, if so, what was the response of the complainant in this regard and within what time frame. Following this, with the no. prot. C/EIS/5303/16-08-2021 its response document, the complained company, after claiming that it is not subject to the GDPR, stated that it is based in the USA. and does not have an establishment in the EU. It subsequently challenged the application of Article 3, paragraph 2 of the GDPR, since, according to its claims, it 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 complainant emphasized that its services are provided to government law enforcement authorities outside the EU, while denying that its own search engine's creation of links to photos available on the internet constitutes behavioral monitoring of data subjects, as these are instantaneous views images without systematic/continuous observation of each person. According to the complainant, there is no GDPR scope for her, as she has a search engine that automatically displays results based on the most relevant algorithm in relation to the query entered by a third party. In fact, the complainant came to the conclusion of a violation of public international law in the case where a company that provides online services is obliged to comply with all laws at a global level. Subsequently, and in the context of good faith and voluntary assistance, as noted by the complainant, regarding the case under consideration, he confirmed that the access request was submitted on 03-24-2021 by the complainant, who also submitted a reminder message on 04-26-2021 . Next, she cited a technical problem that did not allow her representative to read the file submitted by the complainant with her photo in order to respond to her request and while the company's standard practice in such cases is to request a photo again by the subject, however, in this case, mistakenly replied

to the complainant by sending the standard email message for cases where the request as such is not detected. Finally, the 3rd complainant stated that she has satisfied the submitted access request by sending, as she claims, her relevant response to the complainant. However, it is noted that from the no. prot. C/EIS/4976/22-03-2022 supplementary document of the complainant, it appears that the last no response was received from the complained company. From all the information in the file, the following emerges for the company in question: The company with the name Clearview AI, Inc. is based in the US and was founded in 2017. Its unique product is a facial recognition platform, which allows users to match photos of people in the company's database with photos of them online. Its platform, according to what it states on its website1, "is powered by facial recognition technology and includes the largest known database containing more than ten (10) billion images of faces, which are taken from public online sources, including news, websites, signage photos, public social media and other public sources." The complaint under consideration states that according to publicly available sources2 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 works as follows: 1. The company collects, through the use of "web scraping" techniques (a term rendered in Greek as "web harvesting"), images containing human faces from social networks (especially Facebook and Twitter), blogs and websites in general at 1 https://www.clearview.ai/overview (retrieved 26/5/2022 - translated from English) 2 See Clearview joint investigation by the Canadian, Quebec, British Columbia and Alberta Privacy Supervisors, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/#toc7. Also see Search US Register https://tmsearch.uspto.gov/bin/showfield?f=doc&state=4803:tnmzul.2.1 Hamburg 3 See Decision of the Personal Data Protection Supervisory Authority Decision of https://noyb.eu/sites/default/files/2021-01/545_2020_Anh%C3%B6rung_CVAI_ENG_Redacted.PDF. Garante https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur- 20-million_en. CNIL decision https://www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet. Trademark Office Patents of and 4 of which there are publicly accessible photographs, as well as from videos available on the internet (eg Youtube). Along 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 facial appearance of the people in the photos4. The above information is stored in Clearview's database. 2. The company processes the images using special

techniques, so that each face that appears in a photo is converted into a certain numerical sequence, which is called a "vector" and is recognizable by machines. 3. The above numerical sequences are stored in the company's database and are fragmented on the one hand for the cataloging of the database, on the other hand for the future identification of persons. So each person in the database has a separate vector and a hash value associated with it. 4. When a user of Clearview's services wishes to identify a person, they upload a picture of that person and conduct a search. Clearview analyzes this image and outputs a vector for the face in the image, which it then hashes and compares against all the hashed vectors stored in its database. Finally, the company extracts each identified image from its database and provides a list of results, containing all matching images and metadata. If a user clicks on any of these results, they are directed to the original image source page. Finally, the Authority called with no. prot. C/EXE/887/11-04-2022 summons the complained-about company, sending at the same time a translation into English and the complaint in question, so that it can be heard in the context of the hearing from 19-04-2022 - 4 See current (at the date of the conference) https://www.clearview.ai/privacy-policy 5 Privacy Policy of Clearview AI, Inc. teleconferencing of the Authority's Plenary Session. However, the complained-about company did not appear and subsequently the Authority proceeded to examine the elements of the file, and, after hearing the rapporteurs and the clarifications from the assistant rapporteurs, and after a thorough discussion, DECIDED IN ACCORDANCE WITH THE LAW 1. According to the provision of article 3 par. 2 item 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 are related to: b) the monitoring of their behavior, to the extent where such conduct takes place within the Union.' In this regard, recital 24 of the GDPR provides, in relation to the inclusion of a processing in the territorial scope of the GDPR based on article 3 par. 2 item. b', that "...to determine whether a processing activity can be considered to monitor the behavior of a data subject, it should be ascertained whether natural persons are being monitored on the Internet, including the potential subsequent use of personal data processing techniques which consist in the formation of a 'profile' of a natural person, in particular with a view to making decisions concerning him or to analyzing or predicting his personal preferences, behaviors and attitudes.' The EDPS Guidelines 3/2018 on the territorial scope of the GDPR clarify that "contrary to the provision of Article 3(2)(a), neither Article 3(2)(b) nor Recital 24 expressly establishes required degree of "targeting intent" on the part of the controller or processor in order to determine whether the tracking activity could trigger the application of the GDPR to the processing activities. However, the use of the word "tracking" implies that the controller has a specific intention in mind for the collection and subsequent

further use of the relevant data about a person's behavior within the EU. The EDPS does not consider that every online collection or analysis of personal data of individuals in the EU automatically counts as "tracking". It is necessary to consider the controller's purpose for processing the data and, in particular, for any subsequent use of behavioral analysis or profiling techniques involving said data. The EDPB takes into account the wording of recital 24, which states that in order to determine whether processing can be considered as monitoring the behavior of a data subject, a key parameter is the monitoring of natural persons online, including the potential subsequent use of techniques profiling.". 2. Article 4 par. 1 of the GDPR defines as personal data any information concerning an identified or identifiable natural person ("data subject"); an identifiable natural person is one whose identity can be ascertained, directly or indirectly, in particular by reference to an identifier , such as name, identification number, location data, online identifier or one or more factors that characterize the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person. 3. Furthermore, according to article 4 par. 4 GDPR, 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 analyze or predict aspects related to work performance, financial situation , the health, personal preferences, interests, reliability, conduct, location or movements of that natural person". In this regard, the Guidelines on Automated Decision-Making and Profiling for the Purposes of Regulation 2016/679 of the Article 29 Working Party specify that profiling must: a) be an automated form of processing, b) concern personal data , and c) aim to assess personal aspects of a natural person, while stressing that "the wide availability of personal data on the internet and from Internet of Things (IoT) devices, as well as the ability to find associations and make links, can enable the identification, analysis and 7 prediction of aspects of a natural person's personality or behavior and interests and habits"5. 4. According to article 4 par. 14 of the GDPR, biometric data means "personal data resulting from special technical processing linked to physical, biological or behavioral characteristics of a natural person and which allow or confirm the indisputable identification of said natural person person, such as facial images or fingerprint data." In addition, according to article 9 par. 1 GDPR, the special categories of personal data that need special protection include biometric data for the purpose of indisputable identification of a person. In this regard, Recital 51 of the GDPR clarifies that photographs of persons are covered by the definition of biometric data only in case of processing by means of specific technical means that allow the unequivocal identification or verification of the identity of a natural person. 5. According to article 55 par. 1 GDPR, "each supervisory authority is competent to carry out the tasks and exercise the powers assigned to it in accordance with this regulation in the

territory of its member state.". Article 56 para. 1 GDPR states that "subject to Article 55, the supervisory authority of the main or sole establishment of the controller or processor is competent to act as the lead supervisory authority for the cross-border processing operations of the said controller or processor in accordance with the procedure provided for 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 EU6. Recital 122 of the GDPR similarly provides,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 7, https://ec.europa.eu/newsroom/article29/items/612053 6 See Guidelines of the OE of art. 29 to determine the lead authority controller 244, https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=44102 February 6 revised processing, executor finally issued 2018, pp. on WP on and 5, or 8 according to which, “Each supervisory authority should be competent, in the territory of the Member State to which it is subject, to exercise the powers and perform the tasks assigned to it in accordance with this regulation. This should in particular cover processing (….) carried out by a controller or processor not established in the Union, when it targets 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 by the provision of Article 3 para. 2 GDPR, each national supervisory authority is competent to check its compliance with the GDPR on the territory of its member state. 6. In cases where article 3 para. 2 of the GDPR applies, article 27 provides that the data 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 with the offer of goods or services to them or whose behavior is monitored, unless one of the exceptions provided for in paragraph 2 of said article 27 applies. The representative, as explained in recital 80 , must act on behalf of the controller, and can be addressed by any supervisory authority. The representative is appointed by written order of the data controller to act on his behalf in carrying out his obligations under the GDPR. The Guidelines 3/2018 of the EDPS regarding the territorial scope of the GDPR stipulate that this mainly entails the obligations concerning the exercise of the rights of the data subjects, and in this context the provision of the identity and contact details of the representative to data subjects in accordance with the provisions of articles 13 and 14 GDPR. Although not himself responsible for compliance with the rights of the data subjects, the representative must facilitate communication between the subjects and the represented controller in order to ensure the effective exercise of the subjects' rights. As explained in recital 80, the representative should also be subject to enforcement procedures in the event of non-compliance by the controller. This

means in practice that it must be ensured that a supervisory authority can contact the representative on any matter concerning 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 para. 1 GDPR sets out the principles that must govern a processing. In particular, paragraph 1 states that: "1. Personal data: a) are processed lawfully and legitimately in a transparent manner in relation to the data subject ("legality, objectivity and transparency"), […] e) are kept in a form that allows the identification of the data subjects only for the period required for the purposes of processing the personal data ("storage period limitation")'. And to ensure that the data is not kept longer than necessary, recital 39 clarifies that the controller must set deadlines for their deletion or for their periodic review. In accordance with the principle of accountability introduced by the second paragraph of the aforementioned article, it is expressly defined that the data controller "bears the responsibility and is able to demonstrate compliance with paragraph 1 ("accountability")". This principle, which is a cornerstone of the GDPR, entails the obligation of the data controller to be able to demonstrate compliance, including the legal documentation of each processing operation carried out in accordance with the legal bases provided by the GDPR and national data protection law. Any processing of personal data is lawful, only if at least one of the conditions set out in Article 6 paragraph 1 of the GDPR applies, such as: "a) the data subject has consented to the processing of his 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 a party or to take measures at the request of the data subject prior to the conclusion of a contract, c) the processing is necessary for compliance with legal obligation of the controller, d) the processing is necessary to safeguard a vital interest of the data subject or another natural person, (…), f) the processing is necessary for the purposes of the legal interests pursued by the controller or a third party, unless these interests are overridden by interest or fundamental rights and freedoms of the data subject requiring the protection of personal data, in particular if the data subject is a child". If one of the above conditions is met, then this constitutes the legal basis for the processing. Regarding the principle of transparency, Recital 39 of the GDPR provides, among other things, that "it should be clear to natural persons that personal data concerning them are collected, used, taken into account or otherwise submitted to processing, as well as to what extent personal data is or will be processed. This principle requires that any information and communication regarding the processing of such personal data be easily accessible and understandable and use clear and simple language. As recital 60 also clarifies, which refers to information rights, which implement, among other things, the principle of transparency7, "the principles of fair

and transparent processing require that the data subject be informed of the existence of the processing operation and the its purposes." 8. Furthermore, as recital 51 of the GDPR clarifies, special categories of data need special protection, as the context of their processing could create significant risks for fundamental rights and freedoms. While, therefore, in order for the processing of "simple" personal data to be legal, it is sufficient that one of the legal bases of article 6 is met, as regards the special categories of data, their processing is, in principle, prohibited and permitted, only if cumulatively some of the legal bases of article 6 and some of the exceptions of article 9 par. 2 GDPR. This view is adopted both by 7 See and the Guidelines on transparency based on Regulation 2016/679 of the OE of art. 29, WP 260, p. 7. 11 Opinion 6/2014 of the OE of article 29 regarding the meaning of the legitimate interests of the data controller according to article 7 of Directive 95/468, as well as by the ESPD in Guidelines 8/ 2020 on the targeting of social media users9. Therefore, it is not legal to process special categories of data if article 6 is not respected, and only the exceptions mentioned in article 9 apply. In this spirit, Opinion 6/2014 of the OE of article 29 on the concept of legitimate interests of the data controller pursuant to Article 7 of Directive 95/46 emphasizes that "it would be wrong to conclude that the fact that someone has manifestly made public special categories of data in accordance with Article 8 paragraph 2 point e) of Directive 95/46 (currently Article 9 par. 2 par. e GDPR) would be - always in itself - a sufficient condition to allow any type of data processing without evaluating the weighting of the interests and rights at stake, as required by article 7 par. f of Directive 95/46 (today of article 6 par. 1 item in the GDPR)10. 9. The right to information enshrined in articles 13 and 14 of the GDPR provides, in the event that the data has not been collected by the data subject (art. 14 par. 3 letter a'), that the data controller provides the information referred to in paragraphs 1 and 2 (identity of controller, purposes and legal basis of processing, categories of data, etc.) "within a reasonable period of time from the collection of the personal data, but at the latest within one month, taking into account the special circumstances in which the personal dataare being processed'. In particular, as clarified by the Guidelines on transparency based on Regulation 2016/679 of the OE of art. 29, "the data subject should be able to determine in advance the scope of the processing and the consequences it entails, and will not 8 See Opinion 6/2014 regarding the meaning of the legitimate interests of the data controller pursuant to Article 7 of Directive 95/46 p. 14. 9 See Guidelines 8/2020 on the targeting of social media users, p. 40. 10 See In this regard, CJEU decision, C-13/16, Valsts policijas Rīgas regija pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA “Rīgas satiksme”, 4 May 2017, regarding the conditions that must be met cumulatively in order for the processing of data on on the basis of "legitimate interests". 12 should be surprised at a later stage as to the ways in which his personal data has been used.'

10. According to article 15 par. 1, 3 and 4 of the GDPR "1. The data subject has the right to receive from the controller confirmation as to whether or not the personal data concerning him is being processed and, if this is the case, the right to access the personal data to the following information.' Article 12 para. 2, 3 and 4 GDPR provides that "The data controller facilitates the exercise of the data subjects' rights provided for in articles 15 to 22. [...] 3. The data controller provides the data subject with information on the action taken upon request pursuant to articles 15 to 22 without delay and in any case within one month of receipt of the request. This deadline may be extended by a further two months if necessary, taking into account the complexity of the request and the number of requests. The data controller shall inform the data subject of said extension within one month of receipt of the request, as well as of the reasons for the delay. […] 4. If the data controller does not act on the data subject's request, he shall inform the data subject within one month of receiving the request of the reasons why he did not act and of the possibility of submitting a complaint to a supervisory authority and bringing legal action". at the latest https://www.clearview.ai/privacy-policy), the 11. In the present case, as follows from the privacy policy of the respective (available collects "information derived from publicly available photos: In the context of "In the ordinary course of business, Clearview collects photos that are publicly available on the Internet. Clearview may extract information from those photos, including geolocation metadata that the photo may contain and information derived from the facial appearance of the individuals in the photos." ("We collect: 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 13 including such geolocation metadata as the photo may contain and information derived from the facial appearance of individuals in the photos."). The above photographs are indisputably personal data, as defined in article 4 para. 1 of the GDPR, insofar as they allow the identification of a natural person through the reference to one or more factors that attribute to his physical or physiological identity. The CJEU has reached the same conclusion, which has judged that "the image of a person recorded by a camera constitutes personal data within the meaning of the above provision (of Article 2, letter a' of Directive 95/46) to the extent that it provides the possibility of identifying the specific person." 11 Furthermore, from the aforementioned privacy policy of the defendant, it follows that she collects photos that are publicly available on the Internet indiscriminately, without applying any geographic selection criteria. And this breadth of the collection is an inherent characteristic of the service that each of them markets. It is even worth emphasizing that in previous versions of its privacy policy12, it explicitly stated that it collects data of subjects located in the EU. 12. Regarding the correlation of its processing

activities with the monitoring of the behavior of subjects in the EU, a crucial issue is whether these subjects are tracked online. The processing carried out by the defendant results in the production of a search result - based on a certain photo posted by the user of its services - which contains the set of photos that share a hash vector with the photo posted by the user Photo. In this way, a profile is created about a certain person, which consists of the photos in which that person appears, but also their metadata, i.e. the URLs of the websites where these photos are located. The association of these photos and the context in which they are presented on a certain website allows the collection of a lot of information 11 Case C-212/2013, František Ryneš v Úřad pro ochranu rosnych odáží. 12 In force on 29.1.2020. 14 about his face, habits and preferences. In particular, when a photo is posted on social networks or on a website, which publishes an article, or on a blog, this may result in the collection of information that allows the identification of the person's behavior. The analysis of the above information that a person chooses to make public on the Internet and the context in which he chooses to make it public, ultimately allows the determination of the behavior of that person on the Internet based on the exposure choices of his personal or professional life by him . Consequently, the automated processing of personal data described above with the aim of evaluating personal aspects of a natural person constitutes profiling and making it available to users of the defendant's services, who search on the defendant's facial recognition platform, is online tracking. After all, the purpose of the tool marketed by the defendant is to provide the possibility of identifying and collecting information in relation to a certain person. The biometric processing techniques applied by each of them that allow the targeting of a person, ultimately lead to the creation of a profile of him, as a result of the search made by a user of each of his tool. And this search is renewed over time, as the database is constantly updated, which allows the possible development of information concerning a specific person to be ascertained, in particular, if the results of successive searches are compared with each other. 13. Clearview AI, Inc. is based in the USA, while it has no facility in the EU. The cooperation mechanism of the GDPR (Art. 60 et seq. GDPR) applies only in the case of a controller or processor with one or more facilities in the EU13. Recital 122 of the GDPR similarly provides, according to which, "Each supervisory authority should be competent, in the territory of the Member State to which it belongs, to exercise the powers and perform the tasks assigned to it in accordance with this regulation. This should cover in particular the 13 See Guidelines of the OE of art. 29 to identify the lead authority of controller 244, https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=44102 processing, performing WP on or 15 processing (….) carried out by a controller or processor not established in the Union, when it targets data subjects residing in its territory."

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 based on the targeting criterion set by the provision of Article 3 para. 2 GDPR, any national supervisory authority is competent to check its compliance with the GDPR in the territory of its member state, as discussed above. 14. Further, in the case at hand, since Clearview AI, Inc. falls within the scope of the GDPR, based on article 3 par. 2 item b' without having an establishment in the EU, has the obligation to appoint a representative in the EU. according to article 27 GDPR, which he has not fulfilled. 15. In the considered case, the subjects, whose data is processed by the defendant, do not receive any information from the defendant, through this privacy policy, in relation to any of the elements provided for in the article 14 GDPR, neither before nor even after processing. In fact, data subjects may never know that their data has been processed by them unless they happen to read a publication about Clearview AI, Inc.'s practices. 16. The principle of legality of the processing means that, in order to be legal, the processing to which the data is submitted must be based on one of the legal bases provided for in Article 6 GDPR. In this case, none of the elements in the file indicate the existence of any of the legal bases provided for in Article 6. In particular, it is not proven - nor would it be possible based on the characteristics of the processing in question - to provide consent by the subjects (6 par. 1 letter a GDPR), nor to execute a contract between the subject and the data controller (6 par. 1 para. b GDPR), nor the compliance with a legal obligation of the controller (6 para. 1 para. c GDPR), nor the safeguarding of the vital interest of the subject (6 para. 1 para. d GDPR). 16 Regarding in particular the possible application of the legal basis according to par. 1 item f of this article, it is provided that the processing is legal, when it is necessary for the purposes of the legal interests pursued by the controller or a third party with the reservation that the interest or the fundamental rights and freedoms do not prevail over these interests of the data subject that imposes the protection of personal data. In relation to this provision, recital 47 of the GDPR clarifies that, after weighing up 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 the rights of the subject, taking into account the legitimate expectations of the subject based on his relationship with the controller. The legitimate expectations of the subject in relation to the processing of his data are highlighted as a factor taken into account during the above weighting, and by the OE 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 is still considered personal data and subject to the necessary protection requirements, even if it has been made public. Having said that, the fact that personal data is publicly available may be considered a critical factor in

assessing supporting legitimate interests, especially if the publication was made with a reasonable expectation of further use of the data for specific purposes (e.g. for research purposes or for purposes related to transparency and accountability). In the case under consideration, given that there is no relationship between the subjects and the defendant, nor is the existence of reasonable expectations of the subjects that their photos published on the internet are going to be processed by a facial recognition platform, the existence of which in all probability they are unaware, the conditions for the application of article 6 par. 1 item are not met. in the GDPR. From all the elements brought to the attention of the Authority, it emerged that the critical processing does not concern a simple collection of data, but results in the conversion of the 17 collected photographs into biometric data, the processing of which is subject to the strictest provisions of Article 9 GDPR. In relation to the above, taking into account that the processing of special categories of data is in principle prohibited and permitted, only if one of the legal bases of article 6 and one of the exceptions of article 9 para. 2 GDPR are cumulatively met and that in this case none from the legal bases of article 6 GDPR in relation to critical processing, it follows that the processing of biometric data, which the defendant is carrying out, does not meet the conditions of legality set 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 according to Article 15 of the GDPR, through an electronic message sent to the defendant on 24-03-2021, a fact which she agrees with the no. prot. C/EIS/5303/16.08.2021 her response document to the Authority, however, she never received any response on this and her right of access was never satisfied by the defendant, according to prot. no. C/ EIS/4976/22.03.2022 document of the complainant to the Authority and contrary to what the defendant claims in her above document to the Authority, in which she states that she sent the complainant a standardized message. 18. Following the above, from the data in the file, the Authority finds on behalf of the complained-about company named Clearview AI, Inc.: A) violation of the obligation to appoint a representative in the EU. (article 27 GDPR), because, although the complainant falls within the scope of the GDPR, based on article 3 par. 2 item. b' without having an establishment in the EU. and, therefore, is obliged to appoint a representative in the E.U. according to article 27 GDPR, however, it has not fulfilled this obligation. B) violation of the principle of the legality of the processing (Article 5 para. 1 letter a', 6 and 9 GDPR), because the processing carried out by the complained of is not based on any legal basis from those provided for in Article 6 GDPR, while it does not occur none of the exceptions of Article 9 GDPR, regarding special categories of data. C) violation of the principle of transparency of the processing (Article 5 para. 1 letter a GDPR) and the related right to information of the subjects (Article 14 GDPR), because the

defendant 18 did not inform, as she should have, the subjects of which the data is processed, accurately and clearly for the collection and use of their personal data. D) violation of the complainant's right of access (Articles 12 and 15 GDPR), because the defendant did not satisfy the request submitted by the complainant, as stated above. 19. Based on the above, the Authority considers that there is a case to exercise its corrective powers in accordance with articles 58 par. 2 i and 83 GDPR (imposition of a fine) with regard to all of the above established violations, the according to article 58 par. 2 c GDPR its corrective powers regarding the satisfaction of the complainant's right of access and the corrective powers according to article 58 par. prohibition of their processing. In order to determine the fine, which the Authority considers to be effective, proportionate and dissuasive, the measurement criteria defined in article 83 par. 2 of the GDPR applicable to this case are taken into account, as they have been specifically interpreted by the Guidelines "for the application and determination of administrative fines for the purposes of regulation 2016/679" of the working group of article 29. In particular, the following are taken into account: A) the nature, gravity and duration of the violation, which is not an isolated incident, but it is systematic and concerns the basic principles of legality of the processing (art. 5, 6, 9 GDPR), which are fundamental for the protection of personal data, according to the GDPR. It is emphasized that the observance of the principles provided by the provision of article 5 of the GDPR is of capital importance, primarily, the principle of legality, so that, if this is missing, the processing becomes illegal from the outset, even if the other processing authorities, especially in this case where none of the legal bases provided for in article 6 and 9 of the GDPR were established for the disputed processing, as mentioned above. B) the number of affected subjects located in the Greek territory, which due to the data collection techniques used by the defendant, is potentially particularly high. In fact, from the privacy policy of each as 19 and the method of collecting personal data, it does not appear that a relevant technique is applied on the basis of which some of the photographs of natural persons are excluded with specific criteria. C) the fact that the disputed processing concerns special categories of personal data (biometrics). D) the defendant's degree of responsibility, which is great, considering that the disputed processing continues despite the intervention of supervisory authorities inside and outside the EU, E) the defendant's lack of cooperation with the Authority, considering that the defendant did not attend the Authority's meeting even though he was summoned to it, F) the fact that the violation of the provisions regarding the basic principles for the processing as well as the rights of the subjects falls under, in accordance with the provisions of article 83 par. 5 sec. a' and b' of the GDPR, in the highest prescribed category of the classification system of administrative fines, G) the fact that no information is available to the Authority on the turnover of the defendant. Based on the above, the Authority unanimously

decides that it should be imposed incomplained company, as controller, the one referred to in the ordinance administrative sanction, which is judged, as mentioned above, proportional to its gravity violation.

FOR THOSE REASONS

The beginning

A. It enjoins on the complained-of company named Clearview AI, Inc., which is domiciled in the USA, 214 W 29th St, 2nd Floor, New York City, NY, 10001, as responsible processing, based on article 58 paragraph 2 subsection i of the GDPR, a total fine of twenty million (€20,000,000) euros for the violation of the principles of legality and transparency (art. 5 par. 1 a', 6, 9 GDPR) and its obligations under articles 12, 14, 15 and 27 of the GDPR.

B. It orders the complainant company named Clearview AI, Inc., which located in the USA, 214 W 29th St, 2nd Floor, New York City, NY, 10001, as responsible

processing, based on article 58 paragraph 2 paragraph c of the GDPR to comply with the request of the complainant to exercise her right of access.

C. Enforces the Plaintiff named Clearview AI, Inc., located in in the USA, 214 W 29th St, 2nd Floor, New York City, NY, 10001, as responsible processing, based on article 58 paragraph 2 paragraph f of the GDPR, the prohibition of collection and processing of personal data of subjects located in Greek territory, using the methods included in the identification service of the person he is trading with.

D. It orders the complainant company named Clearview AI, Inc., which located in the USA, 214 W 29th St, 2nd Floor, New York City, NY, 10001, as responsible processing, based on article 58 paragraph 2 paragraph g of the GDPR, to delete the personal data of subjects located in Greek territory, which it also collects

processed using the methods included in the identification service

of a person, whom it markets.

The president

The Secretary

Konstantinos Menudakos

Irini Papageorgopoulou