Deliberation SAN-2022-019 of October 17, 2022 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Thursday October 20, 2022 Deliberation of the restricted committee n° SAN-2022-019 of 17 October 2022 concerning the company CLEARVIEW AIThe National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr Alexandre LINDEN, President, Mr Philippe-Pierre CABOURDIN, Vice-President, Mrs Anne DEBET, Mr Bertrand du MARAIS and Mr Alain DRU, members; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 relating to the protection of personal data and the free movement of such data; Having regard to Law No. 78-17 of January 6, 1978 amended relating to data processing, files and freedoms, in particular its articles 20 and following; Considering the decree n ° 2019-536 of May 29, 2019 taken for the application of the law n ° January 6, 1978 relating to data processing, files and freedoms; Having regard to deliberation no. 2013-175 of July 4, 2013 adopting the internal regulations of the National Commission for Data Processing and Freedoms; Having regard to decision no. 2020 -116C of the President of the National Commission for Computing and Liberties of August 26, 2020 to instruct the Secretary General to carry out or have carried out a mission to verify the processing implemented by the company CLEARVIEW AI; Having regard to the decision No. MED 2021-134 of November 26, 2021 giving formal notice to the company CLEARVIEW AI; Having regard to the decision of the President of the National Commission for Computing and Liberties appointing a rapporteur before the restricted formation, dated 2 June 2022; Having regard to the report of Mr. Claude CASTELLUCCIA, commissioner rapporteur, notified to CLEARVIEW AI on July 14, 2022; Having regard to the oral observations made during the restricted training session of October 13, 2022; Having regard to the other documents in the file; Was present, during the session of the restricted formation, Mr Claude CASTELLUCCIA, auditor, heard in his report. Duly convened, by fold delivered against signature on September 20, 2022, the company CLEARVIEW AI was not represented during the Restricted Committee. After deliberation, the Restricted Committee adopted the following decision:I. Facts and procedure1. The company CLEARVIEW AI (hereinafter "the company" or "Clearview AI"), established in the United States, was established in 2017. It has developed facial recognition software, the database of which is based on the aspiration of images publicly accessible on the Internet, which makes it possible to identify a person from a photograph representing him.A. The origin of the procedure2. Between May and December 2020, the National Commission for Computing and Freedoms (hereinafter "the CNIL") received several complaints relating to the difficulties encountered by the complainants in exercising their rights of access and erasure with society.3. Pursuant to decision no. 2020-116C of August 26,

2020 of the President of the CNIL, a delegation from the Commission carried out a documentary inspection mission by sending a questionnaire on October 27, 2020, to which the company replied by letter of the following November 27. This questionnaire focused on the various processing operations implemented by the company, the organizations using the company's services (current or former) having their main establishment in France or within the European Union, as well as complaints no. […] and No […].4. On May 27, 2021, the CNIL received a complaint from the organization Privacy International (request no. […]).5. As part of the mutual assistance provided for in Article 61 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter the "GDPR" or the "Regulation), the CNIL is seen to communicate useful information by its European counterparts.B. The formal notice sent to the company CLEARVIEW AI by the president of the CNIL6. By decision n° 2021-134 of November 26, 2021, the president of the CNIL issued remains the company CLEARVIEW AI to comply within two months with the provisions of Articles 6, 12, 15 and 17 of the GDPR.7 In the absence of a response to the formal notice from the President of the CNIL and to two reminders, the President of the Commission, on June 2, 2022, appointed Mr. Claude CASTELLUCCIA as rapporteur, on the basis of Article 22 of the law of January 6, 1978 as amended.8. , the rapporteur notified the company, on July 14, 2022, of a report detailing the breaches of the provisions of the GDPR that he considered constituted in this case.9. The company has not produced any written observations in response to this report and the file has been placed on the agenda of the restricted committee meeting of October 13, 2022.10. The rapporteur presented oral observations during the session of the Restricted Committee.C. The treatment in question11. It appears from the information transmitted within the framework of the cooperation between supervisory authorities, from publicly accessible information as well as from the complaints received by the CNIL that the company uses its own technology to index the freely accessible web pages. It collects all the images on which faces appear, on millions of websites. Photographs are thus extracted in particular from social networks (for example, Twitter or Facebook), professional sites containing photographs of their employees, blogs and all websites on which photographs of people are publicly accessible. Images are also extracted from videos available online, for example on the site www.youtube.com. This collection concerns images of adults and minors, no filter being applied in this regard. Only hundreds of URLs, associated with "adult" sites with the largest audiences, are blocked and excluded from collection.12. The collection of these images on social networks covers all the images accessible at the time of collection to a person not connected to the network in question. Apart from social networks, the collection concerns all the images accessible at the time of collection to a search engine. The company has thus collected more than twenty billion

images worldwide.13. From each photograph collected, the company calculates a biometric template. A unique digital fingerprint, specific to the face as it appears on the photograph (based on the points of the face) is thus generated. The billions of images are then stored in a database in a searchable form (using the digital fingerprint).14. The company markets access to an online platform on which there is a search engine. This tool works by uploading a photograph of a face to it. From this photograph, the tool calculates the digital fingerprint corresponding to it and searches the database for photographs to which similar fingerprints are linked. The software produces a search result, composed of photographs, to which is associated the URL of the web page from which they were extracted (social network, press article, blog, etc.). This search result thus compiles all the images collected by the company about a person as well as the context in which these images are online, such as, for example, a social network account or a press article. 15. This processing aims to uniquely identify the person from a photograph of the individual. It is therefore a facial recognition device.16. The company describes the service it offers as "a research tool used by law enforcement to identify perpetrators and victims of crime" from a photograph. It is indicated on its website that this tool allows, for example, "analysts" to carry out a search by downloading images of crime scenes in order to compare them with those which are publicly accessible. According to the company, law enforcement can thus use this tool to identify a person for whom they have an image (for example, from a video surveillance recording) but whose identity they do not know. identity.17. It should be noted that the processing operations implemented by the company in order to collect data and constitute a database, which a search engine accesses to provide a result, are analyzed here as a whole, with regard to their common purpose, which is to market a search engine based on facial recognition (hereinafter "the processing in question"). II. Reasons for decisionA. On the applicability of the GDPR18. Pursuant to Article 3(2) of the GDPR: "This Regulation applies to the processing of personal data relating to data subjects who are located within the territory of the Union by a controller or -processor not established in the Union, where the processing activities are related to: […] b) the monitoring of the behavior of these persons, insofar as this is behavior that takes place in the within the Union. The Restricted Committee emphasizes that the GDPR does not require, in order to be applicable, that the purpose of the processing be the monitoring of behavior, but that it be "linked" to the monitoring of the behavior of persons residing in Europe.19. Recital 24 of the GDPR specifies in this respect that "The processing of personal data of data subjects who are located in the Union by a controller or a processor who is not established in the Union should also be subject to this Regulation where such processing is related to the monitoring of the behavior of such persons insofar as it relates to their behavior within the Union In order to determine whether

a processing activity can be considered as monitoring of behavior of data subjects, it should be established whether natural persons are tracked on the internet, including the possible subsequent use of personal data processing techniques which consist of profiling a natural person, in order to in particular to make decisions concerning him or to analyze or predict his preferences, behaviors and attitudes".20. By way of clarification, in its guidelines 3/2018 relating to the territorial scope of the GDPR in their version of 12 November 2019, the European Data Protection Board (hereinafter "the EDPS") notes that, " contrary to the provision of Article 3(2)(a), neither Article 3(2)(b) nor recital 24 expressly introduces a necessary degree of "intent to target" of the controller or processor to determine whether the monitoring activity would trigger the application of the GDPR to the processing activities.However, the use of the word "monitoring" implies that the controller is pursuing a specific objective in view to the collection and subsequent reuse of relevant data relating to an individual's behavior within the Union The Committee does not consider that the online collection or analysis of personal data relating to in the Union would automatically be considered as "follow-up". It will be necessary to take into account the purpose of the data processing by the data controller and, in particular, any subsequent behavioral analysis or profiling techniques involving this data. The Board takes into account the wording of recital 24, which indicates that in order to determine whether the processing involves the monitoring of the behavior of a data subject, the monitoring of natural persons on the Internet, including the potential subsequent use of profiling techniques , constitutes an important factor". personal character relating to data subjects on the territory of the European Union and whether this processing is linked to the monitoring of the behavior of these persons.22 Firstly, it appears from the company's privacy policy that it collects in particular :- photographs publicly accessible on the Internet;- information that can be extracted from these photographs, such as geolocation metadata that the photograph may contain;- information derived from the facial appearance of the persons appearing in these photographs.23. These three categories of data constitute personal data of the person whose face appears in the photograph in question. Indeed, the notion of personal data is defined in the GDPR as "any information relating to an identified or identifiable natural person [...]", this identification may relate in particular "to one or more specific elements specific to his identity. physical ". The image of the photographed or filmed person constitutes personal data as soon as the person is identifiable, that is to say that he can be recognized (see CJEU, fourth chamber, 11 December 2014, Rynes, C -212/13, point 22 and CJEU, second chamber, February 14, 2019, F.K., C-345/17). In addition, this image can be compared (by an automated process or not) with an image held elsewhere and attached to an identified person so that the identity of this person can be deduced.24. The company also

processes biometric data associated with these images. Indeed, personal data resulting from specific technical processing, relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm their unique identification, such as facial images, constitute biometric data, meaning of Article 4.1.14 of the Regulations. These data are generally referred to as “biometric templates” and constitute separate data from the source images (see CNIL, SP, June 25, 2020, Opinion on draft decree, PASP, n° 2020-064, published).25. In addition, the images collected relate to people located in the European Union. Indeed, this collection is not geographically limited to the American territory on which the company is established, since this data is collected on the Internet, in particular from global social networks.26. Therefore, the company processes personal data of natural persons located in the European Union and, in particular, in France.27. Secondly, it should be checked whether the processing activity in question can be considered as "linked to the monitoring of the behavior" of the persons concerned within the meaning of Article 3 of the GDPR. It should be noted that the GDPR is not only applicable to processing whose primary purpose is to monitor the behavior of a person residing in the European Union, but to all processing which is "linked" to such tracking, ie which are carried out by means of or in connection with operations to track persons residing in Europe.28. In accordance with recital 24 of the GDPR, the notion of Internet tracking includes the possible subsequent use of personal data processing techniques which consist of the profiling of a natural person. Profiling is defined in Article 4.1.4 of the GDPR as "any form of automated processing of personal data consisting of the use of such personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict elements concerning the work performance, economic situation, health, personal preferences, interests, reliability, behavior, whereabouts or movements of that natural person”.29. First, the processing in question leads to the creation of a behavioral profile of each of the people whose data is collected.30. It is apparent from the information transmitted in the context of cooperation between supervisory authorities that the tool in question makes it possible to generate, from an image and subject to a margin of technical error, a search result containing all the photographs collected by the company, on which appears a face with a biometric template sufficiently close to the face appearing on the photograph used for research.31. The profile thus created, relating to a person, is composed of photographs but also of the URL address of all the web pages on which these photographs are found. However, the linking of photographs and the context in which they are presented on a website makes it possible to collect a lot of information about a person, their habits or their preferences. With regard to social networks in particular, a photograph as well as the original URL of this photograph are highly likely to make it possible to identify the account of the person concerned.

The photographs may also have been posted online to illustrate a press or blog article, which is therefore likely to contain specific information relating to the data subject and thus elements relating to his or her behavior.32. In addition, the displayed search result may also include metadata, such as geolocation metadata, which may be contained in the photographs or videos. These data make it possible to complete a person's profile.33. In addition, such a search result also makes it possible to identify a person's behavior on the Internet, by analyzing the information that this person has chosen to put online as well as their context. Indeed, the posting of photographs online constitutes in itself a behavior of the data subject, by reflecting choices on the level of exposure that he wishes to give to elements of his private or professional life.34. Therefore, it should be considered that the search result which is associated with a photograph must be qualified as a behavioral profile of the person concerned insofar as it contains a lot of information relating to this person, and in particular to his behavior, or provides access to them. The processing in question thus constitutes profiling within the meaning of Article 4.1.4 in that it makes it possible to evaluate certain personal aspects relating to a natural person, in particular to analyze elements concerning his personal preferences, his interests, his behavior or its location.35. Finally, it should be noted that such a behavioral profile mainly concerns behavior that took place within the European Union. Indeed, insofar as they are persons residing in the Union, they carry out most of their online activity in the Union. In addition, insofar as these persons reside in the Union, the information relating to their private and professional life relates mainly to conduct which takes place in the Union.36. Assuming that the very purpose of the processing is not behavioral monitoring, the means implemented to enable the biometric identification system of the company involve the constitution of such a profile, and the processing must be regarded as "linked to the monitoring of the behavior " of the persons concerned.37. Secondly, the automated processing of data allowing the creation of this behavioral profile and its availability to the persons making the queries in the company's search engine must be classified as Internet tracking.38. Indeed, the very purpose of the tool marketed by Clearview AI is to be able to identify and collect certain information relating to a person. The implementation of the different stages of the processing described above, and in particular of biometric techniques making it possible to single out an individual, lead to the creation of a behavioral profile. However, this profile is created in response to a search carried out by a person and relating to an individual appearing in a photograph.39. In addition, the search can be renewed over time, which makes it possible to note an evolution of the information relating to a person, in particular if the results of successive searches are compared. Indeed, since the database is updated regularly, successive searches make it possible to follow the evolution of a profile over time.40. Consequently, the fact

that a specific search allows, at any time, access to a person's profile as described above must be considered as the monitoring of the behavior of persons.41. The Restricted Committee therefore considers that the processing implemented is linked to the monitoring of the behavior of the persons concerned within the meaning of the provisions of Article 3.2.b) of the GDPR and falls within the territorial scope of the GDPR.42. It also follows from all of the above that the company Clearview AI, which defines the purposes and means of the processing, must be considered as data controller with regard to the creation of the database, which is then used to market its service.B. On the competence of the CNIL and the lack of applicability of the one-stop shop43. Article 55.1 of the GDPR provides that "each supervisory authority is competent to exercise the tasks and powers vested in it in accordance with this Regulation on the territory of the Member State to which it belongs".44. Article 56.1 provides: "Without prejudice to Article 55, the supervisory authority of the main establishment or of the sole establishment of the controller or processor is competent to act as lead control concerning the cross-border processing carried out by this controller or processor, in accordance with the procedure provided for in Article 60. “45. Recital 122 of the GDPR specifies: "Each supervisory authority should be competent in the territory of the Member State to which it belongs to exercise the tasks and powers vested in it in accordance with this Regulation. This should cover, in particular, [… ] the processing carried out by a controller or a processor who is not established in the Union when this processing is aimed at data subjects residing on the territory of the Member State to which it belongs. […] “46. It emerges from a combined reading of Articles 55 and 56 of the GDPR that, in the event that a data controller based outside the European Union implements cross-border processing subject to the GDPR but does not have neither a main establishment nor a single establishment, the one-stop-shop mechanism provided for in Article 56 of the GDPR is not intended to apply. Each national supervisory authority is therefore competent to monitor compliance with the GDPR on the territory of the Member State to which it belongs.47. In the present case, the company is established in the United States of America and has no establishment in the territory of a Member State of the European Union.48. Consequently, the Restricted Committee considers that the one-stop-shop mechanism is not applicable and that the CNIL is competent to ensure, on French territory, that the processing is carried out in accordance with the provisions of the GDPR.C. On the breach of the obligation to have a legal basis for the processing carried out49. Article 6 of the GDPR provides that: "Processing is only lawful if and insofar as at least one of the following conditions is fulfilled: 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 a party or for the performance of pre-contractual

measures taken at the latter's request; c) the processing is necessary for the compliance with a legal obligation to which the controller is subject; d) the processing is necessary to protect the vital interests of the data subject or of another natural person; e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, unless than the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child, prevail. "50. Recital 47 of the GDPR specifies that "The legitimate interests of a data controller, including those of a data controller to whom the personal data may be communicated, or of a third party may constitute a basis legal basis for the processing, unless the interests or fundamental rights and freedoms of the data subject prevail, taking into account the reasonable expectations of the data subjects based on their relationship with the controller. Such a legitimate interest could, for example, exist where 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 of the controller or works for him. . In any case, the existence of a legitimate interest should be carefully assessed, in particular in order to determine whether a data subject can reasonably expect, at the time and in the context of the collection of the data of a personal nature, that they are processed for a given purpose. The interests and fundamental rights of the data subject could, in particular, prevail over the interest of the data controller when personal data are processed in circumstances where the data subjects do not reasonably expect further processing. […] "51. The rapporteur considers that the company has no legal basis for the processing in question, in breach of Article 6 of the Regulation.52. The company has not submitted any observations in defence.53 The Restricted Committee recalls that, to be lawful, the processing of personal data must therefore be based on one of the legal bases referred to above.54 It emerges from the information transmitted in the context of cooperation between supervisory authorities that the facial recognition software implemented by the company is based on the systematic and widespread collection, from millions of websites around the world, of images containing faces, using proprietary technology to index freely accessible web pages.55 The company then proceeds to process the data collected in order to constitute a database and to allow searches for photographs in this database from another image.56 This processing is carried out by the company for exclusively commercial purposes, regardless of the fact that the search engine would be used by law enforcement agencies in certain States.57. As part of the investigations carried out by the CNIL, the company was questioned about the legal basis of this processing, within the meaning of Article 6 of the GDPR. The company has not provided any

response on this point. The company's confidentiality policy, mentioned above, does not mention the legal basis of said processing either.58. It can be noted from the outset that the company did not obtain the consent of the persons concerned to the processing of their personal data.59. In addition, the Restricted Committee notes that, given the nature of the processing in question, the legal bases provided for by the provisions of Article 6.1 under b), c), d) and e), of the GDPR and linked to the performance of a contract, compliance with a legal obligation, safeguarding the vital interests of the data subject or another natural person and the performance of a task in the public interest are not subject to apply in this case.60. With regard to the legal basis linked to the legitimate interests pursued by the data controller, provided for in Article 6. 1. f) of the Regulation, it should be recalled that the "publicly accessible" nature of data n does not affect the qualification of personal data and that there is no general authorization to reuse and re-process publicly available personal data, in particular without the knowledge of the data subjects.61. By way of illustration, the Article 29 working group (known as "G29" which has become the EDPS), in its Opinion 06/2014 on the concept of the legitimate interest pursued by the data controller within the meaning of Article 7 of Directive 95/46/EC, noted in this regard that "personal data, even if they have been made public, are still considered personal data" and that "their processing therefore continues to require appropriate safeguards". While acknowledging that the fact that personal data are publicly available may be a relevant factor in concluding that there are legitimate interests, the EDPS then cautioned that this would only be the case "if their publication is accompanied by a reasonable expectation of further use of the data for certain purposes, for example, for research work or for the sake of transparency and accountability."62. Furthermore, for the controller to rely on this legal basis, the processing must be necessary for the purposes of the legitimate interests pursued by the controller, unless the interests or the fundamental rights and freedoms of the data subjects prevail.63 . Even if the interest of the company were based on the economic interest it derives from the exploitation of the database in question, this interest would however have to be weighed against the interests or the fundamental freedoms and rights of individuals data subjects, taking into account the reasonable expectations of data subjects based on their relationship with the controller, in accordance with Article 6.1.f) of the GDPR, read in the light of recital 47 and the aforementioned opinion on the notion of interest legitimate.64. In this case, the processing is particularly intrusive: the company collects a large amount of photographic data on a given person, to which are associated other personal data likely to reveal various aspects of private life. From this data, a biometric template is created, i.e. biometric data allowing, if it is reliable, to identify the person in a unique way from a photograph of the person: the detention of such data by a third party constitutes a strong invasion of privacy. Finally, this

processing concerns an extremely large number of people.65. Furthermore, it is necessary in particular to determine whether the persons concerned could reasonably expect, at the time and in the context of the collection of the personal data, that they would be subject to such processing by the Clearview AI company. In this regard, there is no relationship between the company and the data subjects. Although they can reasonably expect that third parties will access the photographs in question from time to time, the publicly accessible nature of these is not sufficient to consider that the persons concerned can reasonably expect that their images will feed data processing software. facial recognition. Finally, the software operated by the company is not public and the vast majority of those concerned are unaware of its existence.66. It must therefore be considered that persons who have published photographs representing them on websites, or consented to this publication with another data controller, do not expect that these will be reused for the purposes pursued by the company, i.e. the creation of facial recognition software (which associates the image of a person with a profile containing all the photographs in which he appears, the information that these photographs contain as well as the websites on which they are found) and the marketing of this software to law enforcement agencies.67. Therefore, in view of all of these elements, the Restricted Committee considers that the invasion of the privacy of individuals appears disproportionate to the interests of the data controller, in particular his commercial and pecuniary interests. The legal basis of the legitimate interest of the company cannot therefore be accepted.68. Finally, the company has not provided any response to the requests made on this point in formal notice No. MED 2021-134 of November 26, 2021. The Restricted Committee therefore considers that the company has not complied with the expiration of the fixed period, or later.69. Consequently, the Restricted Committee considers that the company has no legal basis for the processing in question, in breach of Article 6 of the Regulation.D. On the breach of the obligation to respect the right of access70. Article 15 of the GDPR provides that "the data subject has the right to obtain from the controller confirmation as to whether personal data relating to him or her are being processed and, when they are, access to said data. personal data". This article also provides for the different categories of information that the data controller must provide to the data subject in the event of an access request.71. Article 12 specifies that: "the controller shall facilitate the exercise of the rights conferred on the data subject under Articles 15 to 22"72. The rapporteur criticizes the company for not responding effectively to the requests for access sent to it and for not facilitating the exercise of the right of access by the persons concerned.73. The company did not submit any observations in defence.74. The Restricted Committee notes that it emerges from referral No. […] that the complainant at the origin of this referral asked the company for access to the data concerning her and to all the information

relating to this data at the meaning of Article 15.1, by electronic means. Indeed, the complainant mandated a third party to make her request for access to the company. Clearview AI acknowledged receipt while inviting the complainant to use an online platform to exercise her request. More than two months after the initial request and following three other e-mails sent by the mandated third party, the company demanded the transmission of a photograph and an identity document of the complainant and again invited the complainant to use an online platform to exercise her claim. Four months after the initial request, after new exchanges relating to the transmission of an identity document and in the absence of a satisfactory response, the mandated third party sent a letter of formal notice to the company.75. The Restricted Committee notes that the response communicated by the company to the request is, first of all, partial. Indeed, it only contains the result of the search in the tool marketed by the company, that is to say the images and the information associated with them. All of the information provided for in Article 15.1 of the GDPR is thus lacking, the company having contented itself with providing a link to its privacy policy.76. Next, the Restricted Committee considers that, by only agreeing to respond to the complainant's request for access after seven letters and more than four months after her initial request and by demanding a copy of her identity when the complainant had already provided identifying information and a photograph of her, Clearview AI did not facilitate the exercise of the complainant's rights.77. Finally, it appears from the company's privacy policy that it limits the exercise of the right of access to data collected during the twelve months preceding the request and restricts the exercise of this right to twice a year. However, the company's privacy policy does not specify the data retention period and it does not appear from the elements of the file that the retention of the data in question would be limited to twelve months. Thus the limitation of the right of access has no basis.78. In addition, the Restricted Committee notes that the company has not provided any response to the injunctions formulated on this point in formal notice No. MED 2021-134 of November 26, 2021, making it possible to establish that the company would have complied with them within the prescribed period of two months or later.79. Consequently, the Restricted Committee considers, on the one hand, that the company failed in its obligations by refraining from providing a satisfactory response to the complainant and, on the other hand, that the company does not respond effectively to requests for access addressed to it and does not facilitate the exercise of the right of access by data subjects, in violation of Articles 12 and 15 of the Regulation.E. On the breach of the obligation to respect the right to erasure80. Article 17 of the GDPR provides: "The data subject has the right to obtain from the controller the erasure, as soon as possible, of personal data concerning him and the controller has the obligation to erase such personal data without undue delay, where one of the following grounds applies:

[…] the personal data has been unlawfully processed”.81. The rapporteur considers that the company disregarded a data subject's right to erasure by failing to respond to his request to erase his data.82. The company did not submit any observations in defence.83. The Restricted Committee notes that it appears from referral No […] that the complainant at the origin of this referral did not receive any response from the company concerning the request to erase her data.84. However, the Restricted Committee emphasizes that, since the processing implemented cannot be based on any valid legal basis with regard to European regulations, the deletion was by right. The company should therefore have responded favorably to the complainant's request for erasure.85. In addition, the Restricted Committee notes that the company has not provided any response to the injunctions formulated on this point in formal notice No. MED 2021-134 of November 26, 2021, making it possible to establish that the company would have complied with them within the time limit of two months.86. Consequently, the Restricted Committee holds that the company disregarded the complainant's right to erasure by refraining from providing her with an answer, in violation of Article 17 of the Rules.F. On the breach of the obligation to cooperate with the services of the CNIL87. Article 31 of the GDPR provides that "the controller and the processor as well as, where applicable, their representatives cooperate with the supervisory authority, at the latter's request, in the performance of its tasks. ".88. The rapporteur complains that the company did not respond satisfactorily to the CNIL's requests within the time allowed.89. The company did not submit any observations in defence.90. The Restricted Committee notes that the company received a monitoring questionnaire from the Commission delegation, to which it replied only very partially.91. Next, the company received a formal notice dated November 26, 2021. This formal notice included various requests aimed at bringing the processing into compliance and respecting the rights of individuals.92. The Restricted Committee points out that the company did not respond to this formal notice, nor to the reminder sent by the President of the CNIL on March 3, 2022, nor to the reminder sent by the Commission services on April 4, 2022.93. Under these conditions, the Restricted Committee considers that these elements constitute a breach of the provisions of Article 31 of the Regulation since the company has not provided any response to the requests of the CNIL.III. On the sanction and publicity94. Under the terms of III of article 20 of the amended law of January 6, 1978, "When the data controller or its subcontractor does not comply with the obligations resulting from regulation (EU) 2016/679 of April 27, 2016 or the this law, the president of the National Commission for Computing and Liberties may also, if necessary after having sent him the warning provided for in I of this article or, if necessary in addition to a formal notice provided for in II, seize the restricted formation of the commission with a view to the pronouncement, after

adversarial procedure, of one or more of the following measures: […] 2° An injunction to bring the processing into conformity with the obligations resulting from the regulation (EU ) 2016/679 of April 27, 2016 or of this law or to satisfy the requests presented by the data subject with a view to exercising their rights, which may be accompanied, except in cases in which the treatment is implemented by the State, of a penalty payment the amount of which may not exceed €100,000 per day of delay from the date set by the restricted body; 7° With the exception of cases where the processing is implemented by the State, an administrative fine not to exceed 10 million euros or, in the case of a company, 2% of the total worldwide annual turnover of the previous financial year, whichever is higher. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of April 27, 2016, these ceilings are increased, respectively, to 20 million euros and 4% of said turnover. The restricted committee takes into account, in determining the amount of the fine, the criteria specified in the same article 83 […] ". A. On the pronouncement of an administrative fine and on its amount95. Article 83 of the GDPR further provides that "each supervisory authority shall ensure that the administrative fines imposed […] are, in each case, effective, proportionate and dissuasive", before specifying the elements to be taken into account to decide whether there is place of imposing an administrative fine and to decide on the amount of this fine.96 The restricted committee must therefore take into account, in determining the amount of the fine, criteria such as the number of violations, their nature and seriousness, the degree of cooperation with the supervisory authority, the number of persons concerned and the categories of personal data concerned.97 The Restricted Committee notes that the breaches committed are particularly serious, in particular with regard to the breach of principles provided for by the GDPR, the number of data subjects and the particularly intrusive nature of the processing in question.98. The Restricted Committee thus underlines that the processing concerns more than twenty billion images as well as a considerable number of data subjects, worldwide. There are therefore several million people in France whose face appears in a photograph or video publicly accessible on the Internet, and in particular on a social network account, who are likely to be affected by this processing. As the database is also updated very regularly to integrate newly available information, the number of these images and these people is constantly changing.99. This massive processing is also particularly intrusive in that it collects a potentially very large number of photographic data on a given person, with which are associated other personal data likely to reveal various aspects of their private life such as their tastes and preferences (for example, in terms of hobbies), their political opinions or their religious convictions, expressed on social networks, in blog articles or press articles.100. From this data, a biometric template is also created, i.e. biometric data considered sensitive under the terms of article 9 of the GDPR.101. The

Restricted Committee then recalls the extreme seriousness of the breach of Article 6 of the GDPR. Indeed, the company implements this processing in all unlawfulness since it has no legal basis for this purpose: neither legitimate interest of the data controller, nor consent of the interested parties.102. In addition, the company has demonstrated a clear desire not to cooperate with the services of the CNIL. Indeed, it provided only a very partial response to the control questionnaire sent by the CNIL delegation and provided no response to the formal notice from the president, despite several reminders.103. Consequently, the Restricted Committee considers that all of these breaches justify the imposition of an administrative fine.104. With regard to the determination of the amount of the fine, the Restricted Committee first notes that the breaches relating to Articles 6, 12, 15 and 17 of the GDPR are breaches of fundamental principles likely to be the subject, in under Article 83 of the GDPR, an administrative fine of up to 20,000,000 euros and up to 4% of annual turnover, whichever is higher.105. The Restricted Committee notes that, despite the requests of the CNIL, the company did not provide any information relating to its turnover. It notes that, however, it appears from journalistic sources that the company was valued at 130 million euros at the beginning of the year 2021.106. In any event, the Restricted Committee considers that the extent of the processing in question, the seriousness of the breaches and the biometric nature of the personal data concerned require that the administrative fine be particularly large in order to be effective, dissuasive and proportionate.107. In view of all of these elements, the Restricted Committee considers that the imposition of a fine of twenty million euros is justified.B. On the issuance of an injunction accompanied by a penalty payment108. Firstly, the Restricted Committee notes that the company has not provided any evidence that would tend to demonstrate its compliance with Articles 6, 12, 15 and 17 of the GDPR following the formal notice from the President of the CNIL of November 26, 2021. The company therefore continues to implement the processing in question in all unlawfulness since it has no legal basis for this purpose. Moreover, it did not respond satisfactorily to the requests addressed to it by the complainant.109. Consequently, since the breaches noted in this decision persist and in view of their degree of seriousness, the Restricted Committee considers it necessary to issue an injunction so that the company complies with its obligations.110. Secondly, the Restricted Committee points out that a daily fine is a financial penalty per day of delay that the data controller will have to pay in the event of non-compliance with the injunction at the expiry of the deadline for execution. Its pronouncement may therefore sometimes prove necessary to ensure compliance of the data controller within a certain period.111. The Restricted Committee adds that in order to keep the penalty payment its comminatory function, its amount must be both proportionate to the seriousness of the alleged breaches but also adapted to the financial capacities of

the data controller. It also notes that, in determining this amount, account must also be taken of the fact that the breach concerned by the injunction indirectly contributes to the profits generated by the data controller.112. In view of these two elements, the Restricted Committee considers proportionate the pronouncement of a penalty payment in the amount of 100,000 euros per day of delay and liquidable at the end of a period of two months.C. On the publicity of the decision113. The Restricted Committee considers that the publication of this Decision is justified in view of the seriousness of the breaches, the scope of the processing and the number of data subjects.114. In particular, the Restricted Committee stresses that publication of the sanction decision is necessary to inform the persons concerned of the existence of this system, which is unknown to the vast majority of them.115.Finally, it considers that this measure does not is not disproportionate since the decision no longer identifies the company by name at the end of a period of two years from its publication. FOR THESE REASONS The restricted formation of the CNIL, after deliberation, decides to: pronounce against the company CLEARVIEW AI an administrative fine of 20,000,000 (twenty million) euros;- pronounce against the company CLEARVIEW AI an injunction not to proceed without a legal basis to the collection and to the processing of personal data relating to data subjects who are on French territory in the context of the operation of the facial recognition software that it markets, and to delete all the personal data of these persons, in particular the data of the complainant in question who requested erasure (complaint no. […]), after having responded to the access requests already made by the persons, where applicable; - attaching the injunction to a penalty payment of one hundred thousand euros (100,000 euros) per day of delay at the end of a period of two months following the notification of this deliberation, the proof of compliance must be sent to the restricted training within this period; - make public , on the CNIL website and on the Légifrance website, its deliberation, which will no longer identify the company by name at the end of a period of two years from its publication. The chairman Alexandre LINDEN This decision is likely to the subject of an appeal before the Council of State within four months of its notification.