Deliberation SAN-2023-006 of May 11, 2023 National Commission for Computing and Liberties Legal status: In force Date of publication on Légifrance: Wednesday May 17, 2023 Deliberation of the restricted committee no SAN-2023-006 of May 11, 2023 concerning the company DOCTISSIMOLa National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr. Philippe-Pierre CABOURDIN, vice-president, Mrs. Christine MAUGÜÉ, Mrs. Anne DEBET, Mr. Alain DRU and Mr. Bertrand du MARAIS, members; Having regard to the rules (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 Directive 2002/58/EC of the European Parliament and of the Council of July 12 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; Having regard to law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms, in particular its articles 20 et seq.; Having regard to Decree No. 2019-536 of May 29, 2019 as amended, taken for the application of Law No. 78-17 of 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 Computing and Liberties; Considering referral no. 20010597; Considering decision no. 2020-123C of August 14, 2020 of the President of the National Commission information technology and freedoms to instruct the Secretary General to carry out or have carried out a mission to verify the processing of personal data accessible from the domain name "doctissimo.fr", and any related processing; Having regard to the decision of the President of the National Commission for Computing and Liberties appointing a rapporteur to the restricted committee, dated November 29, 2021; Having regard to the report of Mrs Valérie PEUGEOT, rapporteur commissioner, notified to the company DOCTISSIMO on July 19, 2022 Having regard to the written observations submitted by the company DOCTISSIMO on October 5, 2022; Having regard to the response of the rapporteur to these observations, notified on November 21, 2022 to the board of the company; Having regard to the written observations submitted by the company DOCTISSIMO on January 5, 2023; Having regard to the other documents in the file; Were present at the restricted committee meeting of February 9, 2023: - Mrs. Valérie PEUGEOT, commissioner, heard in her report; As representatives of the company DOCTISSIMO:[...] The the DOCTISSIMO company having the floor last;The Restricted Committee adopted the following decision:I. Facts and procedure1. The company DOCTISSIMO (hereinafter "the company"), whose registered office is located at 1 Quai du Point du Jour in BOULOGNE-BILLANCOURT (92100), is a wholly-owned subsidiary of the company UNIFY. It was registered in the Trade and Companies Register on November 17, 1994 and the delegation was informed that it was created in May 2000. In 2020, it

employed around thirty employees. In 2020, it achieved a turnover of around [...], for a net profit of around [...] then in 2021, a turnover of around [...] , for a negative net result of [...].2. The UNIFY company was directly owned by the French media group TF1 until June 28, 2022, the date on which the TF1 group sold to the REWORLD MEDIA group "the media assets and digital activities of the Publishers division of [the company] UNIFY" , of which DOCTISSIMO.3 is a member. The DOCTISSIMO company publishes the French-speaking website www.doctissimo.fr (hereinafter "the website"), which mainly offers articles, tests, quizzes and discussion forums related to health and well-being. The company's website is only available in French but is accessible from all countries of the European Union and also outside Europe. The DOCTISSIMO company claimed approximately […] unique visitors to the website between the months of May 2021 and April 2022 and approximately […] registered users, having a user account created from the doctissimo.fr website, on the date of April 8, 2022. Users, registered or visitors, are located mainly in France and Belgium. Finally, the company counts approximately […] users who answered at least one question of a health-themed questionnaire between the months of February 2020 and January 2021. The delegation was informed that among these users, […] are located in France and […] are located in Belgium.4. On June 26, 2020, the National Commission for Computing and Liberties (hereinafter "the CNIL" or "the Commission") received a complaint no. […] by the association PRIVACY INTERNATIONAL concerning the all the processing of users' personal data implemented by the company DOCTISSIMO on its website and, in particular, the methods of depositing cookies on the user's terminal when they visit the website; the legal basis for processing users' personal data that may be collected on the website when a user performs health-themed tests; the obligation of transparency and provision of information to users of the website as well as the security of user data.5. The association PRIVACY INTERNATIONAL having publicly communicated on its complaint, the company DOCTISSIMO provided details to the knowledge of the CNIL by letter of July 7, 2020, indicating in particular, not to proceed with any deposit of cookies and other tracers before the consent of the user and work to establish consent for access to tests likely to reveal special categories of data.6. Four control missions took place pursuant to decision no. 2020-123C of August 14, 2020 of the President of the CNIL. On September 9, 2020, the CNIL services first carried out an online check from the domain www.doctissimo.fr. On October 1, 2020, the CNIL services then carried out an on-site inspection of the company DOCTISSIMO, in its premises located at 8 rue Saint-Fiacre in Paris (75002), before carrying out, on December 1, 2020, a new online control from the "doctissimo.fr" domain. Finally, on February 8, 2021, a documentary check was carried out by sending a questionnaire to the company.7. These missions gave rise to the establishment of minutes n° 2020-123/1, 2020-123/2 and

123/3 and to letters and information communicated by the company on October 13 and 21, 2020, November 19, 2020 , December 8, 2020, January 18, 2021 and February 24, 2021.8. The main purpose of these missions was to investigate the complaint referred to the CNIL and to verify the compliance of the processing of personal data accessible from the domain name "doctissimo.fr", as well as of any related processing, to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter "the GDPR") and of Law No. 78-17 of January 6, 1978 relating to data processing , files and modified freedoms (hereinafter "the Data Protection Act").9. In accordance with Article 56 of the GDPR, on December 3, 2020, the CNIL informed all the European supervisory authorities of its competence to act as lead supervisory authority concerning the cross-border processing implemented by the company, resulting from the fact that the main establishment of the company is in France. After discussion between the CNIL and the European data protection authorities within the framework of the one-stop-shop mechanism, they are all concerned by the processing since the website includes visitors from all the Member States of the European Union.10 . On April 8, 2021, DOCTISSIMO made a request for advice and support to the CNIL. He was told on April 30, 2021 that the support charter for professionals provides for the impossibility of supporting organizations in their compliance when a control procedure is in progress.11. On October 27, 2021, the company DOCTISSIMO sent the CNIL a letter summarizing the actions related to the processing of personal data accessible from the domain "doctissimo.fr" and any related processing, carried out by the company DOCTISSIMO since the July 2020.12. For the purposes of examining these elements, the President of the Commission, on November 29, 2021, appointed Mrs Valérie PEUGEOT as rapporteur on the basis of Article 22 of the law of January 6, 1978 as amended.13. At the end of her investigation, the rapporteur, on July 19, 2022, notified the company of a report detailing the breaches of Articles 5-1-e), 9, 13, 26 and 32 of the GDPR and Article 82 of the Data Protection Act which it considered constituted in this case. This report proposed that the Restricted Committee impose an administrative fine on the company, as well as an injunction, accompanied by a penalty to bring the processing into compliance with the provisions of Articles 5-1-e) and 32 GDPR and Article 82 of the law. This report also proposed that this decision be made public but no longer allow the company to be identified by name after the expiry of a period of two years from its publication.14. On October 5, 2022, the company filed its observations in response to the sanction report.15. The rapporteur responded to the company's observations on 21 November 2022.16. On 5 January 2023, the company produced new observations in response to those of the rapporteur.17. By letter dated January 19, 2023, the rapporteur informed the company's board that the investigation was closed, pursuant to Article 40,

III, of amended decree no. 2019-536 of May 29, 2019.18. By letter dated January 19, 2023, the company was informed that the file was on the agenda of the restricted meeting of February 9, 2023.19. The rapporteur and the company presented oral observations during the session of the restricted committee.II. Reasons for decisionA. On the European cooperation procedure20. Pursuant to Article 60(3) of the GDPR, the draft decision adopted by the Restricted Committee was sent on March 30, 2023 to the European supervisory authorities concerned.21. As of 27 April 2023, none of the supervisory authorities concerned had raised a relevant and reasoned objection to this draft decision, so that, pursuant to Article 60(6) of the GDPR, these latter are deemed to have approved it.B. On the breach of the obligation to retain personal data for a period not exceeding that necessary for the purposes for which they are processed pursuant to Article 5, paragraph 1, e) of the GDPR22. According to Article 5-1-e) of the GDPR, personal data must be "kept in a form allowing the identification of the persons concerned for a period not exceeding that necessary with regard to the purposes for which they are processed; personal data may be stored for longer periods of time insofar as they will be processed exclusively for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with the 89(1), provided that the appropriate technical and organizational measures required by this Regulation are implemented to safeguard the rights and freedoms of the data subject (restriction of storage) ".a. On the retention periods for data relating to tests and "quizzes" carried out by users of the doctissimo.fr23 website. The rapporteur noted that the delegation noted during the checks on 9 September, 1 October and 1 December 2020 that tests and "quizzes" (hereinafter "questionnaires" or "tests") were available on the website of the society. During the inspection of October 1, 2020, the delegation was informed that these questionnaires were drafted by the company but that their implementation and hosting were carried out by a subcontractor, the company [...].24. Firstly, the rapporteur notes that until 11 October 2020, the company [...] kept the responses from the tests carried out by all logged-in and unlogged users as well as their IP addresses for a period of period of 24 months from their completion. The rapporteur thus noted that a file contained the answers resulting from the tests carried out by the users on the subject of colon cancer, associated with their IP address.25. The rapporteur then notes that a statement below the questionnaires relating to health subjects indicates that carrying out a test allows the user to know the result and, if necessary, to share it with his friends. This also allows the company DOCTISSIMO to produce aggregated statistics on the use of the tests.26. With regard to the first two purposes, the rapporteur observes that it emerges from the observations made that the result of the test is displayed immediately at the end of the sequence of questions asked. It therefore considers that the retention of the user's answers to

the questionnaire as well as his IP address does not appear necessary after the communication of the result to the user and its possible sharing by the latter with his friends. These purposes cannot in any case justify a storage period of 24 months of the personal data concerned.27. With regard to the third purpose, the rapporteur observes that in this case the aggregated statistics are produced independently of the responses to the questionnaires, by means of audience measurement tools, which notably involve the filing and/or reading of cookies or other tracers on the user's terminal for the purpose of audience measurement and the use of the user's IP address. It therefore considers that keeping the answers to the questionnaires after the end of the test is not necessary for the production of aggregate statistics on the use of the tests, which is carried out over time by other means.28. Secondly, the rapporteur notes that since October 11, 2020, the company DOCTISSIMO has asked the company [...], to anonymize the data relating to the tests and "quizzes" as soon as they are collected. The DOCTISSIMO company indicates that since this date, its subcontractor hashed the IP addresses - for which the company indicates that these are the "only identifying data to which the information relating to the participations is attached" - with the HMAC-SHA256 algorithm and that all data relating to participation in the tests dating back more than three months from their completion has been deleted in order to meet the three aforementioned purposes. In view of the information communicated by the company, the rapporteur noted that the hashing algorithm used by the company [...] actually corresponds only to a SHA256 function, without a hash key. The rapporteur notes that the sole use of the SHA256 function, while ensuring the integrity of personal data, does not ensure their anonymisation.29. In defence, the company maintains that the breach complained of is unintentional since it results from the poor performance of the contract concluded with its subcontractor who did not respect its contractual obligations relating to the deletion of data from the tests at the end of their display on the one hand, and those providing for the use of a random variable in the function of anonymization of IP addresses on the other hand. The DOCTISSIMO company specifies that it terminated the contract which bound it with [...] as of March 16, 2021. Next, the company maintains that the rapporteur invokes a hypothetical possession of the information allowing re-identification and that the risk of attack in terms probability and severity is not qualified. It considers that the likelihood of the risk of an attack on its own systems by [...] is negligible and that its severity would be very limited in the absence of sensitive data. Finally, DOCTISSIMO concludes that as of October 11, 2020, the test data contained only non-identifying data and that the latter could be kept without time limit.30. Firstly, the Restricted Committee recalls that the retention period of personal data must be determined according to the purpose pursued by the processing and that when this purpose is achieved, the data must in

principle be deleted or anonymised.31. In this case, the Restricted Committee notes that it is not disputed by the company that before October 11, 2020, the subcontractor of the company DOCTISSIMO kept the answers resulting from the tests carried out by the users as well as their address. IP, for 24 months from their completion. The Restricted Committee considers that the retention of the user's answers to the questionnaire as well as his IP address does not appear necessary after the communication of the result to the user and its possible sharing by the latter with his friends. Similarly, keeping the answers to the questionnaires after the end of the test as well as its IP address is not necessary for the production of aggregated statistics on the use of the tests since they can, and in this case are , carried out over time using audience measurement tools. In this regard, the Restricted Committee notes that the company does not justify the need to retain this data.32. The Restricted Committee notes that the subcontracting agreement provided that the IP addresses of the participants were not to be collected by [...] concerning "anonymous so-called "sensitive" quizzes". Nevertheless, the Restricted Committee notes that the company DOCTISSIMO had access to dashboards, established by its subcontractor, including the answers of the participants to the tests and the "quizzes" as well as their IP addresses in pseudonymised form. The Restricted Committee notes that it was only following the complaint by the association PRIVACY INTERNATIONAL that the company DOCTISSIMO questioned its subcontractor in order to find out what measures it was implementing, when it had knowledge of the collection of IP addresses by the latter, via said dashboards. Next, the Restricted Committee notes that, while the company DOCTISSIMO asked its subcontractor to delete the test results as soon as they were displayed, it did not oppose the alternative solution proposed by the company [...], consisting of proceeding from October 11, 2020, to the sole anonymization of IP addresses.33. If the data controller may decide to use a specialized service provider, in particular by entrusting it with the task of subcontracting personal data, within the meaning of the GDPR, he remains responsible for ensuring, through reasonable diligence, that compliance with the protection of personal data is effectively ensured. The sufficiency of this diligence depends in particular on the skills and resources of the data controller. The Restricted Committee recalls that the controller may be held liable for the lack of implementation by the latter of regular monitoring of the technical and organizational measures taken by its subcontractor (EC, 10th chamber , April 26, 2022, Société Optical Center, No. 449284). The Restricted Committee held in particular the responsibility of a data controller for not having exercised sufficient control over the service provided, considering that a simple contractual commitment by its broker aimed at "respecting the GDPR and the applicable rules in terms of commercial prospecting" is not a sufficient measure, in its deliberation SAN-2022-021 of November 24, 2022 against the

company […].34. It follows from the foregoing that the Restricted Committee considers that the company DOCTISSIMO, which is a company with skills in the digital field, has not sufficiently followed the execution of its contractual instructions by its subcontractor and does not did not exercise satisfactory control over the technical and organizational measures it implemented to ensure compliance with the GDPR and, in particular, to ensure the absence of collection of personal data or even the anonymization of such data. Furthermore, the Restricted Committee notes that the data in question and the IP addresses of the users were accessible to the company DOCTISSIMO.35. Consequently, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 5-1-e) of the GDPR since, until October 11, 2020, the answers to the tests and "quizzes" as well as the IP addresses , which could be associated with user account information, were kept for a period of twenty-four months from their completion, which exceeded the purposes for which the data were processed.36. Secondly, the Restricted Committee notes that since October 11, 2020, the company [...] has been hashing IP addresses with the SHA256 function without a hash key, and that all of the data relating to participation in tests dating back more than three months from the date they were carried out had been deleted.37. The Restricted Committee notes that the Commission has communicated publicly on its website on the use of the SHA function256. The Commission thus considered that, while it ensures the integrity of personal data, the use of the SHA256 function without an associated hash key does not ensure their anonymization. The Restricted Committee therefore considers that the hashing function used by the subcontractor of the company DOCTISSIMO cannot constitute a solution for the anonymization but only for the pseudonymization of users' personal data, in that the company [...] who knew the parameters of the hash, and given the fact that the number of IP addresses is known and limited, could find by brute force and within a reasonable time, the IP addresses of the people who responded to the tests.38. Since the data relating to the participation of users in the tests and "quizzes" are not anonymised, the Restricted Committee considers, as it has previously developed, that their conservation does not appear necessary after the communication of the result to the user and his possible sharing since the result of the test is displayed immediately at the end of the course of the questions asked. Similarly, the Restricted Committee considers that their retention is not necessary for the production of aggregate statistics on the use of the tests. The Restricted Committee therefore considers that the company does not justify any need to retain this data for a period of three months.39. Consequently, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 5-1-e) of the GDPR for the facts noted as of October 11, 2020 when the answers to the tests and "quizzes" are kept for a period of three months from their completion due to an ineffective

anonymization procedure for IP addresses, which exceeds the period necessary for the purposes for which they are processed.40. The Restricted Committee notes that during the procedure, the company DOCTISSIMO indicated that it had complied with the requirements of Article 5-1-e) since since March 16, 2021, its subcontractor no longer collects the IP addresses of the users, so that there is no need to address any injunction to the company on this point. The Restricted Committee nevertheless considers the violation established for past events.b. On the retention periods for accounts created by users of the doctissimo.fr41 site. The rapporteur notes that it emerges from the guidelines relating to the retention periods of the company that it anonymizes "the data relating to the member account after 3 years of inactivity". The rapporteur also notes that during the on-site inspection of 1 October 2020, the delegation was informed that after three years of inactivity, the “directly identifying information of the accounts is deleted or replaced by random data for the purpose of anonymisation” . However, the rapporteur notes that the anonymization procedure put in place by the company does not satisfy the criterion of impossibility of individualization due to the retention of the user's unique identifier, "id_user", and of his pseudonymized user name which allows indirect re-identification of the latter.42. The rapporteur considers that the procedure put in place by the company does not constitute an anonymisation solution, but a simple pseudonymisation of the user's data.43. In defence, the company does not dispute that the user's unique identifier, "id_user", is retained. Nevertheless, the company considers that it does not make it possible to re-identify the account holders since it is not linked to any other data and that the pseudonym of the users is anonymized after 3 years of inactivity by being replaced by a sequence of numbers and random letters. DOCTISSIMO therefore maintains that the possibility and the risk of the re-identification of persons has not been demonstrated. Finally, the company has indicated that it is implementing a new procedure for anonymizing all user accounts that have been inactive for more than 3 years from the end of October 2022. It specifies in this regard that the unique identifiers of users inactive for more than 3 years and pseudonyms will be deleted, including those present on the forums and those appearing in the publications of other forum members.44. The Restricted Committee recalls that the pseudonymisation of personal data is a reversible operation and that it is possible to find the identity of a person by having additional information.45. The Restricted Committee notes in this case that the company does not dispute that its data anonymization policy provided, with regard to accounts inactive for more than 3 years, for the retention of the users' unique identifier, "id_user", as well as of their pseudonymised user name. However, the Restricted Committee considers that the retention of the user's unique identifier, "id_user", associated with his pseudonymised username did not prevent the data associated with the

accounts from being linked. The Restricted Committee thus notes that the procedure put in place by the company allowed the retention of non-identifying data associated with accounts, such as publications on forums; however, the Restricted Committee considers that it is common for users to communicate with each other using their usernames. The Restricted Committee considers that it was therefore possible in the present case to find the identity of a person by having access to additional information.46. Consequently, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 5-1-e) of the GDPR since the measures taken by the company to correctly anonymize the user's personal data to the after a period of three years did not correspond to anonymization but to a simple pseudonymization of the data. The Restricted Committee notes that the company complied during the procedure with the implementation of a new anonymization procedure, so that there is no need to issue an injunction to the company on this point, but nevertheless recalls that this cannot exonerate the company from its responsibility for the past.C. On the breach of the obligation to obtain the consent of the persons concerned to the processing of special categories of personal data pursuant to Article 9 of the GDPR47. Under the terms of Article 9 of the GDPR, the processing of personal data which reveals data concerning the health of a natural person is prohibited unless it falls under one of the conditions provided for in Article 9-2- a) to j) of the GDPR.48. According to Article 4-15 of the GDPR, “data concerning health” is “personal data relating to the physical or mental health of a natural person […]”.49. The rapporteur notes that it appears from the findings made during the inspections of 9 September, 1 October and 1 December 2020 that the company processes health data when people answer the various health-themed questionnaires offered to them on the doctissimo.fr.50 website. The rapporteur then notes that the delegation noted during its online check of September 9, 2020 that the company did not obtain the Internet user's consent to the use of his "sensitive" data in order to proceed with the processing of his data. relating to his health since only a text including a link to the personal data protection policy appeared below the test.51. The rapporteur nevertheless notes that the delegation was informed, by letter dated 19 November 2020, that the tests likely to lead to the collection of health data were withdrawn from the site on 12 September 2020. These tests have been accessible again since 15 October 2020 and their participation is conditional on the fact that Internet users consent, by means of a checkbox, to the processing of their information. The rapporteur notes that it appears from the findings of 1 December 2020 that the checkbox is accompanied by the following statement "I accept that any sensitive data that I provide through my answers to the test will be used as described below. below and detailed in the Personal Data Protection Policy ".52. In defense, the company first argues that the material scope of the notion of health data is not defined

by the GDPR and that its imprecision led the company to seek, in vain, the advice of the CNIL more than 6 months before the appointment of the rapporteur, on April 8, 2021. Next, the company argues that the rapporteur has not provided proof of the systematic processing of health data by DOCTISSIMO in violation of Article 6 of the ECHR. The company argues that, having access only to users' hashed IP addresses, it cannot identify those affected. Finally, only a very small proportion of the tests offered on the DOCTISSIMO website, around 5%, would be likely to allow the collection of health data, assuming that this legal qualification is actually applicable.53. Firstly, the Restricted Committee considers that the file demonstrating the collection of users' responses to a test entitled "Colon cancer: what are your risks" associated with their IP addresses makes it possible to note the collection of information concerning medical history (breast or endometrial cancer) or the physiological state of the persons concerned (body mass index). The Restricted Committee notes that the company offered other tests accessible on its website and relating to the theme of health, such as, in particular, the tests entitled "where are you with alcohol?", "do you miss iron?", "Are you eating too much sugar?", "What if it was asthma?", "Varicose veins: are you at risk?", "What if it was Alzheimer's disease? ?", “Cerebrovascular accident: what are your risks?”, “Hypertensive patients: do you exercise enough?” or even “Do you have good hearing?.54. The Restricted Committee notes that it has been demonstrated that the IP address hashing system put in place did not make it possible to prevent the re-identification of users of the website and that the company DOCTISSIMO was able to associate the answers resulting from the tests carried out with the IP address, from a hand, to the information of a holder of an account on the doctissimo.fr website, on the other hand.55 The Restricted Committee considers, therefore, that by having such information on the people who responded to the tests, the company processes health data within the meaning of article 4-15 of the GDPR.56. Secondly, in the absence of other conditions that can be mobilized to allow said processing in the present case under Article 9-2-b) to j) of the GDPR, the Restricted Committee considers that such processing does not can be implemented only on the basis of the explicit consent of the data subject, to the processing of his personal data for one or more specific purposes, pursuant to Article 9-2-a) of the GDPR. The Restricted Committee recalls that the explicit nature of consent is analyzed on a case-by-case basis and depends on the context of the processing of health data. When the service requested by the user necessarily involves the processing of health data, it is however necessary for the user to be fully aware that his health data will be processed and sometimes stored by the data controller, which implies in principle explicit information on this point when obtaining consent.57. The Restricted Committee notes that, until the withdrawal from the website of the tests likely to generate the collection of health data on September 12, 2020, no particular warning or

mechanism for obtaining consent appeared on the questionnaires in order to ensure that the person was aware of and consented to the processing of their health data.58. The Restricted Committee recalls that it has already adopted corrective measures against data controllers who do not obtain the express consent of individuals to the collection and processing of their sensitive data, in particular in its deliberations No. 2016-405 of December 15, 2016 and n° 2016-406 of December 15, 2016.59. Thirdly, the Restricted Committee notes that the refusal of support from the CNIL, materialized by the letter from the Commission's legal support department of April 30, 2021 in response to the company's request of April 8, 2021, falls within the framework provided by the CNIL's support charter for professionals, which provides for the impossibility of supporting organizations in their compliance when a control procedure is in progress. The Restricted Committee notes that if the CNIL can respond to a request for advice at the end of the control if the repressive phase has not been initiated, such is not the case in this case since a sanction procedure has subsequently been engaged.60. Fourthly, the Restricted Committee notes that according to the company, the share of the tests offered on the DOCTISSIMO website concerned by the collection of health data is around 5%. The Restricted Committee notes, therefore, that said processing of sensitive data concerns approximately […] responses.61. Consequently, the Restricted Committee considers that the aforementioned facts constitute a breach of the obligations of Article 9 of the GDPR since, until September 12, 2020, the data was processed in disregard of the conditions defined by this article.62. Finally, the Restricted Committee notes that the tests likely to lead to the collection of health data have been accessible again since October 15, 2020 and that participation in these tests is conditional on the fact that Internet users consent, by means of a check box. tick, to the processing of their information. It notes that the company brought itself into compliance during the control procedure, which does not, however, call into question the existence of the breach for past facts.D. On the breach of the obligation to inform individuals pursuant to Article 13 of the GDPR63. Pursuant to Article 13 of the GDPR, the controller must provide the data subject with various information at the time the data is obtained.64. In her initial report, the rapporteur noted that the information provided by the company on the website www.doctissimo.fr did not specify the legal basis of the processing carried out. The rapporteur also noted that there was no mention of whether the provision of information was mandatory in that it was of a regulatory or contractual nature or whether it conditioned the conclusion of a contract and whether the person concerned was required to provide the personal data.65. In defence, the company communicates its "Data Protection Policy" and indicates that it contains references to the applicable legal bases.66. During the meeting, taking into account the elements communicated by the company within the framework of the investigation, the

rapporteur proposed to the restricted committee not to retain the breach in connection with the information provided by the company on the website, considering that the "Data protection policy" accessible from the website www.doctissimo.fr, contains information on the legal basis applied for the processing implemented and the fact that certain information conditions the creation of a user account or are of a regulatory nature.67. The Restricted Committee considers that the breach of Article 13 of the GDPR is not established.E. On the breach of the obligation to regulate by a formalized legal act the processing carried out jointly with another data controller pursuant to Article 26 of the GDPR68. Under Article 26 of the GDPR, “1. Where two or more controllers jointly determine the purposes and means of processing, they are joint controllers. Joint controllers shall define their respective obligations in a transparent manner for the purposes of ensuring compliance with the requirements of this Regulation, in particular with regard to the exercise of the rights of the data subject, and their respective obligations with regard to the communication of the information referred to in Articles 13 and 14, by means of an agreement between them, unless and to the extent that their respective obligations are defined by Union law or by the law of the Member State to which the controllers are subject. be named in the agreement.2 The agreement referred to in paragraph 1 duly reflects the respective roles of the joint controllers and their relationship vis-à-vis the data subjects. The outline of the agreement is made available to the data subject.3. Irrespective of the terms of the agreement referred to in paragraph 1, the data subject may exercise the rights conferred on him by this Regulation with regard to and against each of the controllers". transmitted by the company DOCTISSIMO that it considers itself jointly responsible for [...] and [...] However, the rapporteur notes that no contract concluded between the company and these two entities contains any provision relating to the definition of the respective obligations of the parties pursuant to Article 26 of the GDPR. The rapporteur nevertheless notes that the company sent, on 24 February 2021, amendments to the existing contracts which define the respective obligations of the parties.70. In defence, the company does not call into question the reality of the alleged breach but maintains that no person concerned has complained of not having received the necessary information or that their rights have not been respected and that thus the exercise of the rights of people was guaranteed. Consequently, the company maintains that this failure must be dismissed.71. The Restricted Committee notes that it emerges from the elements transmitted by the company DOCTISSIMO that the latter is jointly responsible with the companies [...], on the one hand, with regard to processing related to the marketing of advertising space on the website www.doctissimo.fr and […], on the other hand, concerning the processing of data using the technical tools and functional structures made available by the latter.72. If the elements transmitted by the company DOCTISSIMO certify that

amendments relating to the protection of personal data, defining the respective obligations of the parties, have been concluded since February 24, 2021, in accordance with the requirements of Article 26 of the GDPR, the Restricted Committee notes that the relationship of joint responsibility was not regulated at the time of the CNIL inspections.73. Therefore, in view of the foregoing, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 26 of the GDPR, the absence of complaint or prejudice for users being ineffective. The Restricted Committee notes the compliance measures taken during the procedure, which do not exempt the company from its liability for the failure observed.F. On the breach of the obligation to ensure the security of personal data pursuant to Article 32 of the GDPR74. According to Article 32 of the GDPR, "1. Taking into account the state of knowledge, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks, including the degree of probability and seriousness varies, for the rights and freedoms of natural persons, the controller and the processor implement the appropriate technical and organizational measures to guarantee a level of security appropriate to the risk, including between others, as required: (a) pseudonymization and encryption of personal data; (b) means to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; […] ".To. On the lack of security relating to the navigation of users on the website75. The rapporteur notes that during the on-site inspection of 1 October 2020, the company indicated to the delegation that before October 2019, the pages relating to the tests implemented on the website www.doctissimo.fr by the company [.. .], used the "HTTP" communication protocol by default. The rapporteur therefore notes that this communication protocol was present on the test pages from which personal data – including health data – were entered by users.76. The rapporteur nevertheless notes that the delegation noted on 9 September 2020 that the said pages were now using the "HTTPS" communication protocol.77. In defence, the company argues that the GDPR does not provide for an obligation to implement the HTTPS protocol and that the CNIL cannot therefore sanction the use of the "http" protocol on the basis of a simple recommendation even though it has not been subject to any data breaches. The company also specifies that the absence of an "HTTPS" protocol before October 2019 was the dominant market practice and in accordance with the "state of the art" in this area. Finally, the company maintains that the CNIL delegation was unable to ascertain the facts since the breach is based solely on statements by company employees which cannot be used to found a sanction, except to disregard the right of DOCTISSIMO not to incriminate themselves.78. Firstly, the Restricted Committee recalls that, pursuant to Article 32 of the GDPR, it is the responsibility of the data controller to take "appropriate technical and organizational measures to guarantee a level of security appropriate to the risk".79. The

Restricted Committee considers first of all that the occurrence of a data breach is not necessary for the characterization of a breach and that it has repeatedly adopted pecuniary sanctions in which the constitution of a breach of Article 32 GDPR is based on the absence of sufficient measures to guarantee the security of personal data, in particular in the deliberations n° SAN-2019-006 of June 13, 2019 and n° SAN-2021-021 of December 28 2021 against the company […].80. In this case, the Restricted Committee notes that the "HTTP" protocol is a communication protocol which does not allow the authentication of the website, nor the encryption of data during their transmission to the servers of the company [...], which does not guarantee the authenticity of the site consulted, nor the integrity and confidentiality of the data exchanged, exposing the personal data processed via these pages to the risk of listening, interception or modification without the knowledge of the user, which may lead to a breach of the privacy of the persons concerned.81. The Restricted Committee notes by way of clarification that the need to ensure the confidentiality of the transmission channels of personal data has been underlined by the National Agency for the Security of Information Systems (ANSSI) since 2013, in particular in its " Recommendations for the implementation of a website: master the security standards on the browser side" which specifies that "The implementation of HTTPS on a website or a web application is a guarantee of security which relies on TLS to ensure confidentiality. and the integrity of the information exchanged, as well as the authenticity of the server contacted. The absence of this guarantee can lead to numerous abuses without the intention being malicious ".82. The Restricted Committee also notes that the Commission has consistently recommended since the publication of its guide "The security of personal data" in 2018, to implement, as elementary precautions, the "TLS" protocol by using only the most recent versions. more recent and verifying its proper implementation.83. The Restricted Committee considers that although the ANSSI recommendations and the CNIL guide are not imperative, they are used for clarification and nevertheless set out the basic safety precautions corresponding to the state of the art. The Restricted Committee therefore considers that the use of the "HTTPS" protocol was state of the art before October 2019, contrary to what the company maintains.84. The Restricted Committee also notes that the personal data in question is sensitive data since it concerns the responses of users to tests involving the collection of data concerning their health associated with their IP address. Therefore, taking into account these risks for the protection of personal data and the privacy of individuals leads the Restricted Committee to consider that the measures deployed to guarantee data security, in this case, were insufficient as soon as when personal data passed through the company's servers [...].85. Consequently, the Restricted Committee considers, with regard to the personal data subject to processing, that the absence of implementation of the basic

security measure constituted by the use of the "HTTPS" protocol or of another security measure equivalent characterizes a breach of Article 32 of the GDPR. The Restricted Committee nevertheless notes that the delegation noted during its inspection of September 9, 2020 that the pages relating to the tests implemented on the website www.doctissimo.fr used the "HTTPS" communication protocol. It nevertheless points out that the compliance measures carried out cannot exonerate the company from its liability for the breach found.86. Secondly, the Restricted Committee recalls that if the right for a person not to participate in his own incrimination implies that the prosecution cannot base its argument by resorting to evidence obtained by coercion or pressure, it considers that all the information collected by the CNIL was collected as part of the control procedure based on article 19 of the Data Protection Act. The Restricted Committee notes that the company was given the opportunity to issue observations following the drafting of the minutes, but also to challenge the analysis made of these statements. However, the Restricted Committee notes that the company does not dispute having used the "HTTP" protocol until October 2019. Finally, the Restricted Committee notes that the company's counsel, [...], was present during the on-site inspection carried out on October 1, 2020 by the CNIL. The Restricted Committee considers that there was no coercion contrary to Article 6 of the European Convention on Human Rights when the employees of the company DOCTISSIMO voluntarily made statements concerning the use of the protocol " HTTP" during the control procedure.87. Consequently, since DOCTISSIMO has disregarded an elementary security measure and incurs risks for the security of the personal data of its users until October 2019, the Restricted Committee considers that the aforementioned facts constitute a breach of the obligations of Article 32 of the GDPR for past events.b. On the lack of security relating to the storage of website user passwords88. The rapporteur notes that the delegation observed that the company keeps the passwords of users of the website in a format obtained by a three-step process: the passwords are transformed a first time using the MD5 hash, then the result obtained is transformed a second time via the "password_hash" function of the PHP programming language used by default with the Bcrypt algorithm and finally, the result obtained is stored in the company's database. The rapporteur considers that these methods of storing passwords are insufficient to ensure the security of the personal data to which they allow access (personal space containing in particular the surname, first name, date of birth, e-mail address and sex of the person concerned).89. In defence, the company recognizes that the MD5 algorithm does not provide sufficient guarantees to keep secure password hashes, which is why it decided to couple it with the Bcrypt function. The company indicates that this technique would make it possible to create longer and therefore more robust passwords. She maintains that this technique is still widely used by websites and that it was

considered until very recently as a valid technique in terms of security since it is only since 2020 that certain researchers point out the limits of this method. In addition, the company indicates that no attack has been documented and therefore that the high risk mentioned by the rapporteur is hypothetical and does not justify the imposition of a sanction. Finally, the company indicated that it had removed the pre-hash since September 7, 2022 as well as all the passwords of users who will have to update their password on their next connection. The company clarified that new passwords will be stored according to the terms of this new method which represents a "non-reversible and secure" encryption function.90. Firstly, the Restricted Committee points out that storing passwords in a secure manner constitutes an elementary precaution in terms of the protection of personal data.91. The Restricted Committee also recalls by way of clarification that since 2013, ANSSI has specified good practices with regard to the storage of passwords by indicating that they must "be stored in a form transformed by a one-way cryptographic function unique (hash function) and slow to compute such as PBKDF2" and that "the transformation of passwords must involve a random salt to prevent an attack by precomputed tables".92. The Restricted Committee also notes that the Commission recommends in its deliberation on the adoption of a recommendation relating to passwords, n° 2017-012 of January 19, 2017, "that it be transformed by means of a non-reversible cryptographic function and secure (i.e. using a public algorithm known to be strong whose software implementation is free of known vulnerabilities), incorporating the use of a salt or key.”.93. The Restricted Committee considers that the recommendations of the ANSSI and the CNIL are used for clarification and set out the basic safety precautions corresponding to the state of the art.94. The Restricted Committee recalls that if it is technically possible, the combination of cryptographic algorithm to ensure the storage of personal data is not recommended.95. The Restricted Committee notes, in this case, that the MD5 algorithm is no longer considered state-of-the-art since 2004 and that its use in cryptography or security is prohibited. She recalls that ANSSI then withdrew it from the general security repository in 2014, recalling that the MD5 algorithm was considered "definitively broken".96. The Restricted Committee also considers that the process consisting in first transforming the password by means of the MD5 function then introduces a vulnerability in the Bcrypt function. It recalls that the Open Web Application Security Project (OWASP) advises against this practice because it introduces a risk of a particular form of attack by stuffing identifiers when the Bcrypt function is combined with another function, such as the MD5 function. . The Restricted Committee notes that such a configuration exposes the data to a risk of attack based on the reuse of MD5 pairs and passwords from leaked databases.97. Therefore, the Restricted Committee considers that the company's password management policy does not

mobilize satisfactory measures to ensure the security of the personal data to which they allow access.98. Secondly, the Restricted Committee recalls that the occurrence of an attack or a data breach is not necessary to characterize a breach of Article 32 of the GDPR.99. Consequently, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 32 of the GDPR. It nevertheless notes that the company DOCTISSIMO has indicated that it has implemented a new method of storing passwords using a non-reversible and secure encryption function since September 7, 2022, so that there is no there is no need to issue an injunction to the company on this point. The Restricted Committee recalls, however, that the compliance measures carried out cannot exonerate the company from its responsibility for the past.G. On the breach of the obligations of article 82 of the Data Protection Act100. Under the terms of article 82 of the Data Protection Act, transposing article 5, paragraph 3, of the "ePrivacy" directive, it is provided that: "any subscriber or user of an electronic communications service must be informed in a clear and complete manner, unless it has been done beforehand, by the data controller or his representative: 1° The purpose of any action seeking to access, by electronic transmission, information already stored in his electronic communications terminal equipment, or to register information in this equipment; expressed, after having received this information, his consent which may result from appropriate parameters of his connection device or of any other device placed under his control. These provisions are not applicable if access to the information stored in the terminal equipment of the user or the registration of information in the user's terminal equipment: 1° Either, has the exclusive purpose of allowing or facilitating communication by electronic means; 2° Or, is strictly necessary for the provision of an online communication service at the express request of the user ".a. On the deposit of cookies on the user's terminal without obtaining their consent101. The rapporteur notes that during the online check of 1 December 2020, the delegation noted during two different browsing sessions, from a blank browsing history and before any action on her part, that two cookies were placed on her terminal as soon as it arrives on the home page of the www.doctissimo.fr website. The rapporteur notes that the company has indicated that one of these cookies, the cookie called "af_session", was intended for the dissemination of targeted advertising.102. In defence, the company does not dispute the facts described by the rapporteur. It nevertheless maintains that the deposit of the advertising cookie before any action by the user resulted from its dual purpose, technical and advertising, and indicates that it finalized its compliance as of December 21, 2020. During the exchanges, it demonstrates by the communication of a bailiff's report, that from August 29, 2022, no cookie other than strictly technical is no longer placed on the user's terminal before their consent is obtained.103. The Restricted Committee recalls that Article 82 of the Data Protection

Act expressly provides that operations to access or register information in a user's terminal can only take place after the latter has expressed his consent. , only cookies whose exclusive purpose is to allow or facilitate communication by electronic means, or cookies that are strictly necessary for the provision of an online communication service at the express request of the user, being exempt from this obligation .104. The Restricted Committee considers that advertising cookies, not having the exclusive purpose of allowing or facilitating communication by electronic means and not being strictly necessary for the provision of an online communication service at the express request of the user, cannot be deposited or read on the terminal of the person, in accordance with article 82 of the Data-processing law and Freedoms, as long as it did not provide its consent.105. Consequently, the Restricted Committee considers that by allowing the deposit and reading of the "af session" cookie on the terminal of people when they arrive on the doctissimo.fr site, without obtaining their consent beforehand, whereas its purpose is purpose the dissemination of targeted advertising, the company has deprived them of the possibility granted to them by article 82 of the Data Protection Act, to exercise a choice as to the deposit of tracers on their terminal equipment. The Restricted Committee notes that several million people were affected, the company claiming approximately 276 million unique visitors to the doctissimo.fr website between February 2020 and February 2021106. The Restricted Committee notes that the company DOCTISSIMO demonstrated to the during the procedure, that as of August 29, 2022, no cookie other than strictly technical is no longer placed on the user's terminal before their consent is obtained, so that there is no need to address injunction to society on this point. It nevertheless recalls that the compliance measures carried out cannot exonerate the company from its responsibility for the past.b. On the inadequacy of the mechanism offered to users to refuse the deposit of cookies107. The rapporteur notes that the delegation noted, during the online check of 1 December 2020, the presence of a mechanism allowing users to "set cookies" (mechanism known as "Consent Management Platform", hereinafter CMP). During this check, the delegation clicked on the box entitled "REFUSE ALL", located at the bottom right of the CMP displayed on the site. However, the rapporteur noted that the cookie for advertising purposes "af_session", which had already been deposited, remained stored on the user's terminal equipment. Then, the rapporteur noted that after navigating to another page of the site to view an article online, the delegation noted that the same "af_session" cookie previously deposited remained stored on the user's terminal equipment. Finally, the rapporteur also noted that the delegation noted the deposit on the user's terminal equipment of two new cookies whose purpose is the dissemination of targeted advertising called "UID" and "GED_PLAYLIST_ACTIVITY", respectively deposited by third parties, the partners […], under the domain names

“.scorecardresearch.com” and “www.doctissimo.fr”, despite the refusal expressed by the user.108. In defence, the company does not dispute the facts described by the rapporteur. Nevertheless, the company recalls the particular context in which the online control took place since the CNIL had published on September 17, 2020 its new guidelines concerning cookies which had significant consequences on the tools for collecting consent and refusing Cookies. In addition, the company maintains that unintentional technical malfunctions led to the deposit of the two advertising cookies after the delegation refused and produces an exchange extracted from a Google Groups forum dating from January 2021 in which a publisher of a website reports a malfunction to Google's services relating to the cookie called "GED_PLAYLIST_ACTIVITY". It therefore maintains that the breach is unintentional. Finally, the company demonstrates by the communication of the aforementioned bailiff's report, that from August 29, 2022, in the event of the user's refusal, no cookie other than strictly technical is no longer placed on his terminal.109 . In the first place, the Restricted Committee first notes that operations for reading and/or writing information in the user's electronic communications terminal equipment take place after he has expressed his refusal to file and when reading cookies for advertising purposes and navigated to another page of the website. The Restricted Committee considers that the means provided to people to enable them to refuse any action seeking to access information already stored in their terminal equipment or to enter information in this equipment are ineffective.110. Then, the Restricted Committee considers that the company DOCTISSIMO, as it publishes the doctissimo.fr website, has a share of responsibility in respecting the obligations of article 82 of the Data Protection Act for reading operations and / or writing of information made in the terminal of users when visiting its website, including those made by third parties who are its business partners. The Restricted Committee recalls that the Council of State has ruled that the obligations incumbent on the site editor include that of ensuring with its partners, on the one hand, that they do not issue , through its site, tracers who do not comply with the regulations applicable in France and, on the other hand, that of taking any useful steps with them to put an end to breaches (CE, June 6, 2018 , Editions Croque Futur, n°412589). The Restricted Committee recalls that it has already penalized a breach of Article 82 of the aforementioned law in connection with operations to read and / or write information carried out by third parties in the user's terminal in deliberation no. ° SAN-2021-013 of July 27, 2021 against […].111. Secondly, the Restricted Committee recalls that the CNIL has implemented a compliance plan on the issue of cookies spread over several years and that it has communicated in particular on these developments, in particular from 2019 on its website, or again on October 1, 2020 on the occasion of the publication of the guidelines and the recommendation of September 17, 2020. Compliance was to have taken place by April 1, 2021 and

hundreds of thousands of players, from the smallest sites to the most important, have complied and have introduced a "Refuse" or "Continue without accepting" button on their consent collection interface. The Restricted Committee notes that the shortcomings observed during the online check of December 1, 2020, which relate to the deposit of cookies on the user's terminal without his consent and before any action as well as after he has clicked on the button "REFUSE ALL", were practices identified by the CNIL as being contrary to article 82 of the Data Protection Act from 2013. It considers that the context of publication by the CNIL of its new guidelines concerning cookies, in which the control of December 1, 2020 falls within therefore does not make it possible to attenuate the scope of the breaches noted and that the company had to be both particularly vigilant with regard to compliance with its obligations in terms of cookies and also attentive to the changes in the regulations in this area, in particular following the strengthening of the conditions of consent following the entry into application of the GDPR.112. Thirdly, with regard to the exchanges and the documents communicated within the framework of the investigation, the Restricted Committee considers that the malfunctions invoked by the company do not make it possible to minimize its responsibility in that they are subsequent to the control of the CNIL and concern another website publisher. The Restricted Committee considers, in any event, that it was up to DOCTISSIMO to ensure compliance with the obligations of Article 82 of the Data Protection Act and thus to ensure with its partners that they do not did not issue, through its site, trackers that do not comply with the regulations applicable in France and to take any useful steps with them to put an end to breaches, which the company has only done 'after the CNIL inspection of December 1, 2020.113. Consequently, it follows from all of these elements that by depositing cookies subject to consent on the user's terminal before any action on his part and by rendering ineffectual the refusal to deposit and read cookies for advertising purposes, the company DOCTISSIMO has disregarded the provisions of article 82 of the Data Protection Act.114. The Restricted Committee notes that the company DOCTISSIMO has demonstrated during the procedure, that from August 29, 2022 no cookie other than strictly technical is deposited on the user's terminal before their consent has been obtained, nor in the event of refusal by users, so that there is no need to issue an injunction to the company on this point. It nevertheless recalls that the compliance measures carried out cannot exonerate the company from liability for the past.III. On corrective measures and their publicity115. Under the terms of III of article 20 of the modified 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 from 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: […] 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. 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. "116. Article 83 of the GDPR provides that "Each supervisory authority shall ensure that the administrative fines imposed in under this Article for breaches of this Regulation referred to in paragraphs 4, 5 and 6 are, in each case, effective, proportionate and dissuasive", before specifying the elements to be taken into account in deciding whether to imposition of an administrative fine and to decide on the amount of this fine.A. On the imposition of an administrative fine and its amounta. On the imposition of an administrative fine117. The company considers that the proposed administrative fine is disproportionate to to the alleged breaches relating to old facts and to its conduct since it has implemented the necessary remedial measures. in Article 83 of the GDPR, such as the nature, gravity and duration of the breach, the scope or purpose of the processing concerned, the number of data subjects affected, the measures taken by the controller to mitigate the damage suffered by the persons concerned, the fact that the violation was committed through negligence, the degree of cooperation with the supervisory authority and, in certain cases, the level of damage suffered by the persons.119. The Restricted Committee first notes the number and extent of breaches alleged against the company, five in number, including four breaches of the GDPR.120. Regarding the breach of the principle of limitation of the retention period of personal data, the company has shown negligence in keeping the data relating to the tests carried out by the users of the website www.doctissimo.fr for a duration exceeding the purposes for which they were processed. The Restricted Committee notes, however, that this is a breach resulting from the subcontractor's non-compliance with its own contractual obligations and that the company DOCTISSIMO has severed all contractual ties with it. Regarding the retention periods for accounts created by users of the website, the Restricted Committee recalls that the measures taken by the company did not make it possible to anonymize the personal data of the user whose account had been inactive for more than three years. It notes that this failure concerns a large number of people, the company claiming approximately […] users with an account created from the website and […] users who answered a question in a test on the subject of health .121. With regard to the breach of the obligation to

obtain the consent of the persons concerned to the processing of sensitive data relating to health, the Restricted Committee notes first of all that the company was negligent in refraining from obtaining the consent users when it offered them tests involving the collection of data relating to their health. It then notes that this failure concerns a significant number of people, the company indicating that 5% of the tests offered would be likely to allow the collection of health data, which represents approximately […] responses. The Restricted Committee also considers that, with regard to this breach, it is appropriate to take into account the nature of the actor concerned and his sector of activity. Indeed, since DOCTISSIMO broadcasts digital content relating to health, it cannot avoid such an obligation.122. With regard to the breach of the obligation to ensure the security of personal data, the Restricted Committee considers that it contributed to accentuating the fact that the personal data of persons processed in this context did not benefit from the protection offered by the GDPR.123. With regard to the breach relating to the cookies placed on the user's terminal when visiting the company's website, the Restricted Committee considers that the absence of obtaining consent concerned each of the people who visited the website. in question, i.e. necessarily several million people, given that the company claims approximately […] unique visitors to the doctissimo.fr website between the months of February 2020 and February 2021.124. Finally, the Restricted Committee notes that the compliance measures put in place following notification of the sanction report do not exonerate the company from its liability for the breaches noted.125. Consequently, the Restricted Committee considers that an administrative fine should be imposed with regard to the breaches constituted in Articles 5-1-e), 9-2, 26 and 32 of the GDPR and with regard to the breach constituted Article 82 of the Data Protection Act.b. On the amount of the administrative fine126. The Restricted Committee first notes that the breaches relating to Articles 5-1-e) and 9-2 of the GDPR are breaches of key principles of the GDPR, likely to be the subject, under Article 83 of the GDPR, an administrative fine of up to €20,000,000 and up to 4% of annual turnover, whichever is higher.127. The Restricted Committee then recalls that administrative fines must be both dissuasive and proportionate. The Restricted Committee notes that the company DOCTISSIMO achieved, in 2021, a turnover of approximately […] for a negative net result of […].128. The Restricted Committee notes that DOCTISSIMO is 100% owned by the unipersonal simplified joint-stock company UNIFY, which is itself owned by the REWORLD MEDIA group. In 2021, the latter achieved consolidated revenue of approximately €496.8 million and a net profit up by €42.2 million.129. Therefore, with regard to the liability of the company, its financial capacity and the relevant criteria of Article 83 of the Rules mentioned above, the Restricted Committee considers that an administrative fine of two hundred and four- twenty thousand euros, with regard to the breaches constituted in articles

5-1-e), 9-2, 26 and 32 of the GDPR and that an administrative fine of an amount of one hundred thousand euros with regard to the breaches constituted in article 82 of the Data Protection Act appear justified.B. On advertising130. The company disputes the rapporteur's proposal to make this decision public. It considers that in view of the age of the facts and the compliance of the company, the educational and informative virtue of the measure of publicity of the sanction no longer exists. To justify this request for publicity, the rapporteur relies in particular on the number of people concerned and the age of certain data.131. The Restricted Committee considers that the publication of this decision is justified in view of the seriousness of the breaches in question and the number of people concerned. The Restricted Committee also considers that the publicity of the sanction will in particular inform all the persons concerned of the follow-up to the breaches.132. Finally, the measure is proportionate when the decision no longer identifies the company by name at the end of a period of two years from its publication. to: pronounce against the company DOCTISSIMO an administrative fine in the amount of two hundred and eighty thousand euros (€280,000) with regard to the breaches constituted in articles 5-1-e), 9-2, 26 and 32 of Regulation (EU) No. 2016/679 of April 27, 2016 on data protection; pronounce against the company DOCTISSIMO an administrative fine of one hundred thousand euros (€100,000) with regard to the breach of article 82 of the law of January 6, 1978 as amended; make public, on the website of the CNIL and on the Légifrance site, its deliberation, which will no longer identify the company by name at the end of a period of two years from its publication. the subject of an appeal before the Council of State within two months of its notification.