Deliberation SAN-2022-020 of November 10, 2022 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Thursday November 17, 2022 Deliberation of the restricted committee no SAN-2022-020 of November 10 2022 regarding DISCORD INC. The 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, Mrs. Christine MAUGÜÉ, Mr. Alain DRU and Mr. Bertrand du MARAIS , 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 relating to data processing, files and freedoms, in particular its articles 20 and following; Having regard to decree no. 2019-536 of May 29, 2019 adopted for the application of law no. information technology, files and freedoms; Having regard to deliberation no. 2013-175 of July 4, 2013 adopting the internal regulations of the National Commission for Information Technology and Freedoms; the President of the National Commission for Computing and Liberties to instruct the Secretary General to carry out or have carried out a mission to verify any processing of personal data relating, in whole or in part, to data relating to the marketing or use of products or services associated with the "DISCORD" brand; Having regard to the decision of the President of the National Commission for Computing and Liberties appointing a rapporteur before the restricted committee, dated 24 December 2021; Considering the report of Mrs. Valérie PEUGEOT, commissioner rapporteur, notified to the company DISCORD INC. on February 25, 2022; Having regard to the written observations submitted by DISCORD INC. on April 15, 2022; Having regard to the rapporteur's response to these observations notified on May 12, 2022 to the company's board; Having regard to the written observations of DISCORD INC. received on July 12, 2022; Having regard to the other documents in the file; Were present, during the restricted committee session of September 15, 2022: - Mrs. Valérie PEUGEOT, auditor, heard in her report; As representatives of the company DISCORD INC . :- […] The company DISCORD INC. having spoken last;The Restricted Committee adopted the following decision:I. Facts and procedure1. DISCORD INC. (hereinafter "the company"), whose registered office is at 444 De Haro Street #200, San Francisco, CA 94107 (USA), was created in 2015. In January 2021, it had approximately 300 employees. 2. For the years 2019 and 2020, the company achieved a turnover of approximately […] dollars and approximately […] dollars respectively.3. DISCORD is a voice over IP (technology that allows users to chat via their microphone and/or their webcam via the Internet) and instant messaging software, allowing users to create servers, as well as text, voice and video channels . DISCORD is thus a platform allowing

people with similar interests to share and communicate. This software is available on Windows, Mac, Linux, iOS and Android and can also be accessed directly through a web browser, from the URL "https://discord.com", or via an application. Popular among the gaming community for providing a way for them to communicate with each other and grow a community outside of the games themselves, DISCORD has become a comprehensive social network with a wide range of ways to interact. The application was very popular during the confinement linked to the Covid-19 pandemic, in particular with a young audience.4. The use of the software is free as a whole, but DISCORD offers the possibility of subscribing to improve its profile, add functionalities on servers, have more speed for the exchange of files, etc.5. As of January 2021, approximately […] DISCORD user accounts were registered worldwide, including more than […] in France.6. The company does not have an establishment in the European Union but has appointed a representative, in accordance with Article 27 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter the "GDPR "), namely the Irish company VERASAFE.7. Pursuant to Decision No. 2020-272C of the President of the National Commission for Computing and Liberties (hereinafter the "Commission" or the "CNIL") of August 14, 2020, the CNIL carried out a online control on the "discord.com" website and on the DISCORD mobile application on November 17, 2020.8. On December 29, 2020, a document inspection mission to the company was also carried out by sending a questionnaire to the company.9. On February 5 and 12, 2021, the company sent response elements to the CNIL. By email of March 8, 2021, the CNIL delegation requested additional information from the company's board, which was sent by the company's board on March 23 and 24, 2021.10. For the purposes of examining these elements, the President of the Commission, on December 24, 2021, appointed Mrs Valérie PEUGEOT as rapporteur on the basis of Article 39 of Decree No. 2019-536 of May 29, 2019.11. On February 25, 2022, the rapporteur notified the company of a report detailing the breaches of the GDPR that she considered constituted in this case. This report proposed that the restricted formation of the Commission impose an administrative fine with regard to the breaches of Articles 5, paragraph 1, e), 12, 13, 21, paragraph 1, 25, paragraph 2, 32 and 35 of the GDPR. It also proposed that the sanction decision be made public, but that it would no longer be possible to identify the company by name after the expiry of a period of two years from its publication.12. On April 15, 2022, the company produced its observations in response to the sanction report.13. The rapporteur responded to the company's observations on May 12, 2022.14. On 12 July 2022, the company produced new observations in response to those of the rapporteur.15. By letter dated August 10, 2022, 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,

2019.16. By letter dated August 11, 2022, the company was informed that the file was on the agenda of the restricted meeting of September 15, 2022.17. The company and the rapporteur presented oral observations during the session of the restricted committee.II. Reasons for decisionA. On the processing in question and the applicability of the GDPR18. Article 3, paragraph 2, a) of the GDPR provides that "This Regulation applies to the processing of personal data relating to data subjects who are located on the territory of the Union by a controller or a processor who is not established in the Union, where the processing activities are related to: (a) the provision of goods or services to such data subjects in the Union, whether or not payment is required of the said persons […] ".19. DISCORD INC. processes users' personal data (hereinafter "the processing in question") when they create a DISCORD account and for the provision of the functionalities permitted by the software.20. The Restricted Committee notes, without this being disputed by the company in the context of these proceedings, that DISCORD INC. processes personal data of users located in France. According to the information provided by the company during the inspection procedure, DISCORD had more than […] users in France in January 2021. In addition, it appears from the online report of findings of November 17, 2020 that, both on computer from the "discord.com" URL and on the DISCORD mobile phone application, all pages are accessible in French, with the exception of the privacy policy which was available in English only at the time of the findings in line, but which is now available in French. Furthermore, the various processing implemented by the company DISCORD INC. through its website and its application are directly linked to the range of services it offers. These include, for example, processing in connection with the creation of an account, the provision of the messaging platform and the DISCORD social network or purchases made. Finally, the privacy policy of DISCORD INC. refers to the GDPR and the company VERASAFE located in Ireland has been appointed as representative under Article 27 of the GDPR.21. Consequently, the Restricted Committee holds that the processing in question concerns an offer of services intended for persons residing in the European Union and deduces from this that this processing is subject to the GDPR pursuant to Article 3, paragraph 2, a) of this Regulation.B. On the competence of the CNIL22. 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 within the territory of the Member State to which it is subject".23. Article 56(1) of the GDPR provides that, "without prejudice to Article 55, the supervisory authority of the main establishment or single establishment of the controller or processor is competent to act as lead supervisory authority with regard to the cross-border processing carried out by this controller or processor, in accordance with the procedure provided for in Article 60 ".24. Furthermore, under the terms of article 16 of the Data Protection Act, "the

restricted committee takes measures and pronounces sanctions against data controllers or subcontractors who do not comply with the obligations arising from the regulations. (EU) 2016/679 of April 27, 2016 and this law […] ".25. The Restricted Committee notes, without this being contested by the company in the context of this procedure, that the "one-stop shop" mechanism provided for in Article 56 of the GDPR is not intended to apply in this case. , DISCORD INC. not having an establishment on the territory of a Member State of the European Union. Therefore, each national supervisory authority is competent to monitor compliance with the GDPR on the territory of the Member State to which it reports in accordance with Article 55 of the Regulation, for the processing implemented by DISCORD INC. aimed at persons residing in this territory. The CNIL is thus competent to control the compliance with the GDPR of the processing implemented by DISCORD INC. targeting persons residing on French territory.C. On the breach of the obligation to define and respect a data retention period proportionate to the purpose of the processing26. According to Article 5, paragraph 1, e), of the GDPR, personal data must be "kept in a form allowing the identification of the data subjects for a period not exceeding that necessary for the purposes for which they are processed […] ".27. The rapporteur notes that the company has not defined a data retention period policy and that its register of processing activities does not mention any retention period for the personal data processed. Thus, the data has been kept for more than six years, the date on which the DISCORD service was launched, the company not carrying out any erasure or regular archiving of the data at the end of a defined period. It notes that within the DISCORD database there are 2,474,000 million accounts of French users who have not used their account for more than three years and 58,000 accounts which have not been used for more than five years, without the company has provided any particular explanation or justification for keeping these inactive accounts.28. The rapporteur recalls that the CNIL's reference system relating to the processing of personal data implemented for the purposes of managing commercial activities of 3 February 2022 specifies - with regard to commercial activities involving the creation of an online account by customers - that the data is intended to be kept until the account is deleted by the user. However, he points out that it is common for users to no longer use these accounts without deleting them, which leads them to persist indefinitely. In this case, the Commission recommends that the accounts be considered inactive after two years and be deleted at the end of this period, unless the user expresses the wish to keep his account active.29. In defense, the company indicates that it did not have a written data retention policy in February 2021, but maintains that it was however in compliance with Article 5 of the GDPR, since it had determined and implemented retention periods directly encoded in the DISCORD service itself. It indicates that the retention period implemented

corresponds to the duration of the contractual relationship with its users, as well as to periods determined according to its legal obligations and its security obligations that it is required to respect. without however specifying them.30. In addition, the company raises the unenforceability of the recommendations of the CNIL, in particular the CNIL reference system of February 3, 2022, which is subsequent to the online control carried out on November 17, 2020 and reserves the hypothesis "for commercial activities which involve the creation of an online account by customers (e.g. dating sites or social networks), [where] the data may be kept until the account is deleted by the user". The company also underlines the specific nature of the Discord Service, which is a communication service involving the maintenance of so-called inactive accounts in the very interest of the users.31. The Restricted Committee notes that, in the context of the review procedure, the company indicated: "Discord does not have a written data retention policy. […] The company […] is currently developing a data retention policy to delete inactive accounts when the company can conclude that the user has abandoned their account". In this respect, the register of processing activities communicated by the company during the control procedure does not mention any retention period for the personal data processed.32. The observations made by the CNIL's delegation of control confirm that there were, within the DISCORD database, 2,474,000 accounts of French users who had not used their account for more than three years and 58,000 accounts not used for more than five years.33. The Restricted Committee recalls that the obligation not to retain data "for a period not exceeding that necessary for the purposes for which they are processed […]" results from Article 5, paragraph 1, e) of the GDPR which is a mandatory provision. The Commission consistently considers that the retention of online accounts created free of charge without action by users beyond a certain period leads to the retention of data indefinitely, in breach of the GDPR. The Restricted Committee considers that the company cannot rely in this case on the maintenance of a contractual relationship to keep indefinitely the accounts of users who are totally inactive, but who have not unsubscribed, since the account was created free of charge. and that an inactive user who would like to use the service again can do so by recreating an account at any time.34. Thus, the Restricted Committee considers that the company has disregarded its obligations resulting from Article 5, paragraph 1, e) of the GDPR, the nature of the service offered to users being ineffective.35. It nevertheless acknowledges that DISCORD INC. now has a written policy for the retention of personal data processed, which provides in particular for the deletion of accounts after two years of user inactivity. The Restricted Committee therefore considers that the company has complied with the obligations arising from Article 5, paragraph 1, e) of the GDPR.D. On the breach of the obligation of transparency36. Article 12, paragraph 1, of the GDPR provides that "the controller shall take

appropriate measures to provide any information referred to in Articles 13 and 14 as well as to carry out any communication under Articles 15 to 22 and Article 34 with regard to the processing to the data subject in a concise, transparent, comprehensible and easily accessible manner, in clear and simple terms, in particular for any information intended specifically for a child ".37. The rapporteur noted that, as part of the due diligence on November 17, 2020, the CNIL delegation noted that after clicking on the link entitled "Confidentiality" located in the footer, a page opened in the browser, denominated in these terms "DISCORD PRIVACY POLICY". While the "privacy policy" was easily accessible from the registration form, it was only available in English, in its version dated June 23, 2020 at the time of the online check. 38. In defence, the company specifies that the privacy policy was already communicated to users in French at the time of the CNIL inspection. However, a technical issue that occurred on November 16, 2020 temporarily prevented the French translation of the privacy policy from appearing on the website during checkout. It adds that it identified the technical problem and quickly implemented the necessary measures to resolve it, specifying that the French version of the privacy policy became accessible again on December 3, 2020.39. In view of these elements, the rapporteur proposes to the Restricted Committee not to retain the breach of Article 12 of the GDPR.40. The Restricted Committee takes note of the elements provided by the company and considers that this breach is not established.E. On the breach of the obligation to inform persons41. Article 13 of the GDPR lists the information that must be communicated by the data controller to the data subjects when their personal data is collected directly from them. Article 13(2) of the GDPR provides that "in addition to the information referred to in paragraph 1, the controller shall provide the data subject, at the time the personal data is obtained, with the following additional information which is necessary to ensure fair and transparent processing: (a) the retention period of the personal data or, where this is not possible, the criteria used to determine this period […]". The guidelines on transparency within the meaning of Regulation (EU) 2016/679, which shed light on the provisions of Article 13, specify that "the retention period […] should be formulated in such a way that the data subject can assess , depending on the situation it is in, what the storage period will be in the case of specific data or in the case of specific purposes. The controller cannot simply state in a general way that the personal data will be kept for as long as the legitimate purpose of the processing requires. Where appropriate, different storage periods should be mentioned for the different categories of personal data and/or the different processing purposes, in particular periods for archival purposes". 43. The rapporteur notes that the retention periods were stated in a generic way, without being sufficiently explicit, since they were specified in these terms: "We generally keep personal data for the time necessary for the purposes defined in this document.

To dispose of the data personal information, we may anonymize it, delete it or take other necessary action. Data may persist for some time in the form of backup copies or for commercial purposes". The rapporteur therefore concludes that a breach of the obligation to inform is established.44. In defence, the company indicates that Article 13, paragraph 2, a) of the GDPR does not require the storage period to be provided as such, but on the contrary leaves the possibility for the data controller to provide the "criteria used to determine this duration". It adds that in order to comply with this obligation, DISCORD INC. has provided users with said criteria, namely the duration necessary to achieve the purposes otherwise explicitly described in the privacy policy. Finally, the company adds that it has developed an information note which provides more details regarding the retention of personal data and that a link to the page "How long Discord keeps your information" has been included directly in the privacy policy.45. The Restricted Committee considers that at the time of the online check carried out, the retention periods were stated in a generic manner and were not sufficiently explicit. The information was incomplete with regard to retention periods since it did not include any precise duration or criteria for determining these periods. In any event, the Restricted Committee recalls that recourse to the "criteria used to determine this duration" is only permitted when it is not possible to provide a precise duration. However, this is not the case in the present case with regard to the processing implemented by the company. As a result, people could not know the retention periods established by DISCORD INC., whereas this information is important in order to guarantee "equitable and transparent treatment" since it contributes to ensuring that users have control over the processing of their data.46. Therefore, the Restricted Committee considers that the company has failed to comply with its obligations resulting from Article 13, paragraph 2, a) of the GDPR. It nevertheless takes note of the measures taken by DISCORD INC. during the procedure and considers that the company has now complied on this point.F. On the breach of the obligation to respect the right of opposition47. Article 21, paragraph 1, of the GDPR provides that "the data subject has the right to object at any time, for reasons relating to his particular situation, to the processing of personal data concerning him based on the article 6, paragraph 1, point e) or f), including profiling based on these provisions. The controller shall no longer process the personal data, unless he demonstrates that there are legitimate grounds and imperative for processing which prevails over the interests and rights and freedoms of the data subject, or for the establishment, exercise or defense of legal claims". The rapporteur noted that, among the processing of personal data implemented by DISCORD INC., there is the processing "Use data to improve Discord", the purpose of which is to use the information collected via the services to " help [the company] improve the content and functionality of the services, better understand [its] users and improve the service”. It

appears from the company's processing register that the purpose of improving the service leads to the collection of the following data: IP address, user identifier, operating system, chat servers joined, contacts/friends, games played, possible subscription to the premium version of discord, purchases made, features used, activities in the platform, etc. The company adds that, when the user objects to their data being used for the purpose of improving the DISCORD service, they must go to the settings and deactivate the functionality. In this case, the company removes the association of the alias with the user's identifier, which then prevents it, according to it, from being able to associate the data collected with the pseudonymous alias with the user's identifier. 'user. The rapporteur noted that it appears from the information provided by the company that the personal data of the person concerned continue to be processed, even though the user has expressed his wish to oppose it. The simple breaking of the link between, on the one hand, the usage data processed and stored with the pseudonymous alias and, on the other hand, the user's identifier associated with his account does not appear sufficient to consider that the user's right to oppose the processing of his data for this purpose would be duly taken into account and effective.49. In defence, the company considers that the possibility of deactivating the "Use data to improve Discord" function with a slider button does not constitute the exercise of the right of opposition within the meaning of Article 21, paragraph 1, of the GDPR. It specifies that it clearly distinguished, in its responses to the delegation of control:- on the one hand, a configuration option which can be used via an online slider button without the need for justification relating to the particular situation of the user: in this case, the data is pseudonymised; - on the other hand, the right of opposition which is exercised under Article 21, paragraph 1, of the GDPR. In this case, users make their request to DISCORD or its representative, justifying reasons relating to their particular situation to allow the company to assess whether this condition is met. This right is not exercised via the slider button.50. The company considers that sanctioning it on this point would have the effect of dissuading organizations from implementing "privacy by design" and pushing them to provide only the opposition mechanism provided for in Article 21 of the GDPR.51. In view of these elements, the rapporteur proposes that the Restricted Committee not accept this breach.52. The Restricted Committee notes that it appears from the elements communicated by the company that the existence of the slider button allowing the "Use data to improve Discord" function to be deactivated is a setting which is not intended to constitute the exercise of the right of opposition within the meaning of Article 21 of the GDPR and that DISCORD INC. offers an opposition procedure in accordance with this article.53. Under these conditions, the Restricted Committee considers that the breach of Article 21 of the GDPR is not established.G. On the breach of the obligation to guarantee data protection by default54. Article 25(2) provides that "the

controller shall implement appropriate technical and organizational measures to ensure that, by default, only personal data which are necessary in relation to each specific purpose of the processing are processed This applies to the amount of personal data collected, the extent of their processing, their retention period and their accessibility.In particular, these measures ensure that, by default, personal data does not are not made accessible to an indeterminate number of natural persons without the intervention of the natural person concerned".55. The rapporteur indicates that, by default, the user must perform several actions to exit the DISCORD application on Windows and Linux. The application is configured to remain active even when the user closes the main window (by selecting the "X" icon located at the top right), which makes it possible to continue communicating by voice while no longer occupying space. on the computer desktop. Only a small indicator makes it possible to understand that the application is active. This indicator was present in the taskbar, which is located at the bottom right of the screen in Microsoft Windows, next to the date and time. The rapporteur concludes that this configuration of the application led to the user's personal data being communicated to third parties through the voice channel, even though the latter thought, in the absence of sufficiently visible and clear specific information that their collection ceased when he chose to close the application window.56. In defense, the company indicates that one of the primary features of DISCORD is to be able to exchange with friends, often while doing something else, such as playing a video game or browsing the web. According to the company, the user only wants to see on his screen the game he is playing and any intrusion on his screen would impact his game and disturb him. It considers that, when a user connected to a voice chat room clicks on the "X" icon located at the top right, he has no intention of leaving the application in question and is well aware that he is still connected to said chat room. According to the company, he is informed on several occasions that, to leave a voice channel, he must click on the "disconnection" button (icon representing a telephone with a cross in a red circle).57. In addition, the company considers it essential to take into account the operation of similar applications in order to assess the level of expectation of DISCORD users. The company invokes the EDPS Data Protection by Design and Default Guidelines, which state that "processing should correspond to the reasonable expectations of data subjects". According to her, the rapporteur cannot conclude that there has been a breach of data protection by design without first determining whether users have been deceived or whether the processing and operation of the application is unexpected, harmful or discriminatory for its users. However, according to the company, the user can legitimately expect such operation of the DISCORD application since, on the one hand, the applications on Windows and Linux operating systems operate in the same way (according to it, when clicking on the "X" icon, the user

expects this action to only close a window and put the application in the background) and, on the other hand, the level of The user's expectation, when he clicks on the "X" icon, is to put the application in the background so that he can continue chatting while performing other actions on his computer. In addition, the company explains that the closing methods can be modified thanks to a setting made available to users, who can decide on a single action to be taken to close the application.58. Finally, the company specifies that it has now implemented a "pop-up" type window which indicates to users of Windows and Linux operating systems that the DISCORD application is still running when the window has been closed and that these parameters can be directly modified by the user.59. Firstly, the Restricted Committee points out that, if a user connected to a voice channel closes the application window by clicking on the "X" icon located at the top right (under Microsoft Windows), he does not in fact that put the application in the background and not quit it; he is therefore always connected in the voice room. However, under Microsoft Windows and, more generally, in the symbolism commonly used in computing, clicking on "X" at the top right of the last visible window of an application generally allows you to quit it. Minimizing the application, in the background, is usually achieved by clicking on a "-" icon. However, the behavior of DISCORD is different. Therefore, the Restricted Committee considers that the user should be given specific information, so that he is warned of this difference. However, that was not the case when the online check was carried out.60. The Restricted Training clarifies that, if there are applications with communication functions that are actually only reduced to the background after the user clicks the close cross, generally either applications that have such behavior informs the user with a pop-up window on the first click on the cross that the application will go into the background but continue to function; or, by default, the background minimize behavior is not enabled and it is up to the user to set it manually. However, in this case and before the setting up of the "pop-up" type window mentioned above, the reduction in the background took place by default from the first use after installation, without any warning or information. clear.61. Consequently, the company cannot validly maintain that the operation of the application would correspond to the expectations of the user, insofar as other applications inform the person or allow the user to carry out this specific configuration himself. .62. Secondly, the Restricted Committee notes that this default configuration of the application – which provided that it was not quit when the main window is closed – led to the user's personal data being able to be communicated to third parties without his necessarily being aware of it. Indeed, the user was not necessarily aware that his words continued to be transmitted and heard by the other members present in the vocal room. The Restricted Committee notes that such a configuration, in the absence of sufficiently clear and visible information, presented significant risks for users,

in particular of intrusion into their privacy.63. Therefore, the Restricted Committee considers that the company has failed to comply with its obligations resulting from Article 25, paragraph 2, of the GDPR, which imposes data protection by default. 64. It nevertheless notes that DISCORD INC. has now implemented a "pop-up" window which, when the window has been closed for the first time, alerts people connected to a voice channel that the DISCORD application is still running and that these parameters can be modified directly by the user.H. On the breach of the obligation to ensure data security65. According to Article 32 of the GDPR, "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, the degree of which probability and severity 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, among other things, as required: (b) means to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) (d) a procedure for testing, analyzing and to regularly evaluate the effectiveness of the technical and organizational measures to ensure the security of the processing ".66. The rapporteur noted that, when creating an account on DISCORD, a password consisting of six characters including letters and numbers was accepted. The rapporteur considered that such passwords, without sufficient complexity criteria and not being associated with any additional security measure, do not make it possible to ensure the security of the personal data processed by the company and to prevent unauthorized third parties have access to this data.67. In defence, the company disputes the rapporteur's analysis and considers that it has implemented measures to guarantee a high level of security for its users' access to its system, including measures to prevent attacks by brute force: limiting login attempts to one per second; verification by email or SMS to validate the identifier when the company receives a connection request from an IP address located outside the zone of the previous connection IP address; rejecting commonly used and compromised passwords and implementing a "captcha" for logins from new IP address ranges.68. The company has also made changes to its password security processes as part of the sanction procedure: - it now requires French users to set passwords with a minimum length of eight characters, of which at least three of these characters are lowercase letters, uppercase letters, numbers or special characters;- after ten unsuccessful connection attempts, the company requires the resolution of a "captcha".69. The Restricted Committee considers that the length and complexity of a password remain basic criteria for assessing its strength. It notes in this regard that the need for a strong password is also emphasized by the National Information Systems Security Agency.70. By way of clarification, the Restricted Committee recalls that to ensure a sufficient

level of security and meet the robustness requirements of passwords, if the authentication provides for a restriction of access to the account, the CNIL recommends, in its deliberation n° 2017-012 of January 19, 2017, that the password contains at least eight characters, containing at least three of the four categories of characters (upper case, lower case, numbers and special characters) and that the authentication involves a restriction of access to the account, such as the delay in access to the account after several failures (temporary suspension of access, the duration of which increases as attempts are made), the establishment of a mechanism to protect against submissions automated and intensive attempts (such as a "captcha") and/or blocking of the account after several unsuccessful authentication attempts.71. In this case, the Restricted Committee notes that a password consisting of six characters including letters and numbers was accepted at the time of the online check. The Restricted Committee considers that in view of the undemanding rules governing their composition, as well as the volume of personal data to be protected, the robustness of the passwords accepted by the company was too weak, leading to a risk of compromise of the associated accounts and of the personal data they contain, despite the additional security measures put in place before the sanction procedure.72. Under these conditions, in view of the risks incurred by individuals, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 32 of the GDPR, since the company's password management policy was not sufficiently robust and binding to guarantee the security of the data, within the meaning of this article.73. It nevertheless notes that, as part of the sanction procedure, the company has made changes on this point and has complied with the provisions of Article 32 of the GDPR.I. On the failure to carry out a data protection impact assessment74. Article 35(1) of the GDPR provides that "where a type of processing, in particular through the use of new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to create a high risk for the rights and freedoms of natural persons, the controller shall, before the processing, carry out an analysis of the impact of the processing operations envisaged on the protection of personal data". Recital 91 of the GDPR provides in particular that an impact assessment "should apply, in particular, to large-scale processing operations which aim to process a considerable volume of personal data at regional, national or supranational level, which may affect a significant number of data subjects […]".76. The rapporteur considers that the company should have carried out an impact assessment relating to data protection (hereinafter "DPIA"), with regard to two criteria allowing it to be considered that the processing was likely to create a high risk: the large-scale data collection and data collection on vulnerable people. The rapporteur considers that the processing implemented by the company is likely to create a high risk for the rights and freedoms of natural persons and concludes that

the company DISCORD INC. disregarded the obligations of Article 35 of the GDPR by not carrying out a data protection impact assessment.77. In defense, the company DISCORD INC. indicates that it considered that a DPIA was not necessary insofar as it only processes very limited data, namely those necessary to allow users to create their account, to provide its services, to meet its commitments to its users and to meet its legal obligations; it does not carry out any of the processing operations listed in Article 35, paragraph 3, of the GDPR as requiring an impact analysis; it does not carry out any of the processing operations for which the CNIL has considered that a DPIA is required, in accordance with the list of processing operations for which such an analysis is necessary published on November 6, 2018; it does not process data on "children", since it is intended only for users over the age of fifteen who have a sufficient degree of maturity to use its services.78. The company also points out that the G29 guidelines on DPIA and how to determine whether processing is "likely to create a high risk" for the purposes of Regulation (EU) 2016/679 recall that a DPIA is not is not automatic even when the processing meets two of the nine criteria defined among those to be taken into account.79. Finally, the company explains that, even though it was not required to do so under the GDPR, it has since carried out two DPIAs for its processing related to the DISCORD service and its essential services, which concluded that the processing is not not likely to create a high risk for the rights and freedoms of individuals.80. Firstly, the Restricted Committee considers that by processing the data of more than […] users in France, the company DISCORD INC. implements personal data processing on a large scale. In addition, the Restricted Committee notes that the application is also intended to be used by children aged fifteen, which the company DISCORD INC. is fully aware, as it states itself that it is "committed to protecting the privacy of children and has therefore put in place measures to ensure that no child under the minimum age defined for each country can access Discord services and create a ".81. The Restricted Committee recalls that, according to recital 38 of the GDPR, "children deserve specific protection with regard to their personal data because they may be less aware of the risks, consequences and safeguards concerned and of their rights. related to the processing of personal data" and that pursuant to Article 1 of the International Convention on the Rights of the Child, "a child means any human being under the age of eighteen" . If, in application of article 8 of the GDPR and article 45 of the Data Protection Act, a minor can consent alone to the processing of personal data with regard to the direct offer of services by the company information from the age of fifteen, the fact remains that a minor between fifteen and eighteen remains a child, and therefore a vulnerable person.82. The Restricted Committee recalls, by way of clarification, that the aforementioned G29 guidelines concerning the DPIA, amended and last adopted on 4 October 2017, set a list of nine criteria

to be taken into account to give a more of processing operations which require an impact analysis due to a high inherent risk. These criteria include, in particular, the collection of personal data on a large scale and the collection of data concerning vulnerable persons. The guidelines add that, "in most cases, the controller may consider that processing satisfying two criteria requires DPIA".83. With regard to the first criterion relating to the collection of data on a large scale, the guidelines explain that account should be taken, in particular, of the number of data subjects, the volume of data and/or the range of different data items processed, the duration or permanence of the data processing activity and the geographical extent of the processing activity. With regard to the second criterion relating to the collection of data relating to vulnerable persons, the guidelines indicate that the processing of data relating to vulnerable persons is a criterion due to the increased power imbalance that exists between the data subjects and the data controller. processing, which means that the former may find themselves unable to consent or easily object to the processing of their data or to exercise their rights. Among these vulnerable persons, the guidelines cite children "who may be seen as incapable of objecting or consenting knowingly and in a considered manner to the processing of their data".84. Consequently, the Restricted Committee considers that the company should have carried out an impact analysis of the data processing implemented, with regard to the volume of data processed by the company and the use of its services by children.85 . Secondly, the Restricted Committee notes that, if the processing carried out by the company does not appear in the "list of types of processing operations for which an analysis relating to data protection is required" published by the CNIL (deliberation 2018-327 of October 11, 2018), they also do not appear in the "list of types of processing operations for which an impact analysis relating to data protection is not required" (deliberation n ° 2019-118 of September 12, 2019).86. Thirdly, the Restricted Committee notes that the company has, in the context of this procedure, carried out two DPIAs, which were sent to the CNIL and concluded that the processing is not likely to generate a high risk to the rights and freedoms of individuals. It nevertheless notes that although the impact assessments carried out concluded that there was no high risk, the fact remains that they had to be carried out beforehand in order to be sure.87. Given all of these elements, the Restricted Committee considers that the company has disregarded the obligations of Article 35 of the GDPR.III. On corrective measures and their publicity88. Under the terms of article 20, III, 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 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. assumptions 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 "89. Article 83 of the GDPR provides that "each supervisory authority ensures that the fines administrative measures imposed 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 to decide whether there impose an administrative fine and to decide on the amount of this fine.90 Firstly, on the principle of imposing a sanction, the company asks the restricted committee not to impose a sanction on it, insofar as it disputes all of the breaches of which it is accused. With regard to the amount of the fine, the company considers that its good faith and its willingness to cooperate were not effectively taken into account in the proposal of the rapporteur.91. The Restricted Committee recalls that it must take into account, for the pronouncement of an administrative fine, the criteria specified in Article 83 of the GDPR, such as the nature, gravity and duration of the violation, the measures taken by the controller to mitigate the damage suffered by data subjects, the degree of cooperation with the supervisory authority and the categories of personal data affected by the breach.92. The Restricted Committee emphasizes that the breaches committed by the company relate to obligations relating to the fundamental principles of the protection of personal data and that five breaches have been established.93. The Restricted Committee then notes that the processing implemented by DISCORD INC. concern a very large number of people located in France, since more than […] DISCORD user accounts were registered in France in January 2021, including minors.94. Consequently, the Restricted Committee considers that an administrative fine should be imposed with regard to the breaches constituted in Articles 5, paragraph 1, e), 13, 25, paragraph 2, 32 and 35 of the GDPR.95. The Restricted Committee recalls that breaches relating to Articles 5, paragraph 1, e) and 13 of the GDPR are breaches of principles liable to be subject, under Article 83 of the GDPR, to an administrative fine which may amount to up to 20,000,000 euros or up to 4% of the worldwide annual turnover of the previous financial year, whichever is higher.96. The Restricted Committee also recalls that administrative fines must be both dissuasive and proportionate. It considers in particular that the activity of the company and its financial situation must in particular be taken into account for the determination of the

amount of the administrative fine. It notes in this regard that DISCORD INC. achieved a turnover of approximately […] dollars in 2019 and more than […] dollars in 2020.97. In addition, the Restricted Committee notes the efforts made by the company to comply throughout the procedure, as well as the fact that its business model is not based on the exploitation of personal data. 98. Therefore, in the light of these elements, the Restricted Committee considers that the imposition of an administrative fine in the amount of 800,000 euros appears justified.99. Secondly, with regard to the publicity of the sanction decision, the company maintains that such a measure would cause it unfair prejudice and does not appear justified in view of the level of protection of personal data that it guaranteed to its users at the time of the inspection and which it continues to provide to all of its users. It considers that such advertising would lead users to believe that the processing of their personal data is not compliant, whereas the latter are correctly informed of the processing of their data, that the security of their data is ensured via robust measures and that the exercise of their rights is respected.100. The Restricted Committee considers that the publicity of the sanction is justified in view of the number of people concerned, the number of breaches committed and their seriousness. against DISCORD INC. an administrative fine of 800,000 (eight hundred thousand) euros for breaches of Articles 5, paragraph 1, e), 13, 25, paragraph 2, 32 and 35 of the GDPR; 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 chairman Alexandre LINDEN This decision is likely to be the subject of a appeal to the Council of State within four months of its notification.