Deliberation SAN-2022-009 of April 15, 2022 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Thursday April 21, 2022 Deliberation of the restricted committee no. SAN-2022-009 of 15 April 2022 concerning DEDALUS BIOLOGY 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. Bertrand du MARAIS and Mr Alain DRU, members; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 modified relating to data processing, files and freedoms, in particular its articles 20 and following; Considering the decree n ° 2019-536 of May 29, 2019 taken for the application of 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 information technology and freedoms; Having regard to decision no. 2021-028C of the President of the National Commission for Information Technology and Freedoms of February 24, 2021 to instruct the Secretary General to carry out or to have carried out a verification mission of all processing accessible from the domains […] or relating to personal data collected from them; Having regard to decision no. to instruct the Secretary General to carry out or have carried out a verification mission with the companies DEDALUS FRANCE and DEDALUS BIOLOGY; Having regard to decision no. ertés of March 2, 2021 to instruct the Secretary General to carry out or have carried out a mission to verify any processing of personal data accessible online and which would be related to the facts reported by the newspaper Liberation in its article entitled Les confidential information of 500,000 French patients stolen from laboratories; Having regard to decision no. a verification mission with the company […]; Having regard to decision no. a verification mission with the company […]; Having regard to the decision of the President of the National Commission for Computing and Liberties appointing a rapporteur before the a restricted formation, dated October 6, 2021; Having regard to the report of Mr. François PELLEGRINI, reporting auditor, notified to the company DEDALUS BIOLOGY on December 9, 2021; Having regard to the written observations submitted by the board of the company DEDALUS BIOLOGY on January 24, 2022 Having regard to the rapporteur's response to these observations notified on February 7, 2022 to the board of the company; Having regard to the written observations submitted by the board of the company DEDALUS BIOLOGY received on February 21, 2022; Having regard to the oral observations made during the meeting of the restricted committee; Having regard to the other documents in the file; Were present at the restricted committee meeting of March 10,

2022:- Mr. François PELLEGRINI, commissioner, heard in his report; As representatives of DEDALUS BIOLOGY:- […] DEDALUS BIOLOGY having the last word; After having deliberated, the Restricted Committee adopted the following decision: I. Facts and procedure1. DEDALUS BIOLOGY (hereinafter "the company") is a simplified joint-stock company with a single shareholder registered with the Strasbourg Trade and Companies Register under number 348 585 233 since December 1, 1988. Its business is the publishing application software. It has between ten and nineteen employees.2. DEDALUS BIOLOGY is part of the DEDALUS group, which employs approximately nine hundred people and which is made up of five companies in France.3. DEDALUS BIOLOGY markets software solutions for medical analysis laboratories, called laboratory management solutions. About three thousand private medical biology laboratories and between thirty and fifty analysis laboratories of public health establishments are equipped with solutions produced by DEDALUS BIOLOGY.4. To date, five software programs have been marketed, including the KALISIL software. Two solutions previously marketed by DEDALUS BIOLOGY are no longer maintained and are considered obsolete, including MEGABUS, whose "end of life" was reached in September 2019 according to the company. Customers using the MEGABUS solution received a letter sent by the company NETIKA (former name of DEDALUS BIOLOGY) in 2018 to inform them of the "definitive cessation of maintenance" of this solution.5. For the use of software marketed by the companies DEDALUS FRANCE and DEDALUS BIOLOGY, customers acquire a license. DEDALUS BIOLOGY also provides installation, start-up and support services for customers in the use of the software. A maintenance contract is generally concluded to ensure the updates of the solutions, which notably include new functionalities and make it possible to maintain the solutions in conformity with the standards in force.6. On February 23, 2021, a press article entitled "Confidential information of 500,000 French patients stolen from laboratories and disseminated online" was published by the newspaper Liberation. This article reported on the presence on a forum of a download link to a file containing the medico-administrative data of nearly 500,000 people: "According to specialists, the leak is on an unprecedented scale in France for data The file in question, which "CheckNews" was able to consult, contains the complete identity of nearly half a million French people, often accompanied by critical data, such as information on their state of health or even their passwords. Initially shared on hacker forums, this database is becoming more and more widely distributed. Pursuant to Decision No. 2021-028C of the President of the National Commission for Computing and Liberties (hereinafter the "Commission" or the "CNIL") of February 24, 2021, the CNIL carried out a online control in order to verify compliance with law n ° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms (hereinafter the "Data Protection Act") and with the regulation

(EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the "GDPR" or the "Regulation") of any processing accessible from the domains […] or relating to personal data collected from the latter.8. As part of the diligent online check, the file containing the medical-administrative data was downloaded. It appeared that the personal data of 491,840 patients were included, including:- identification data: social security number, surname, first names, gender, postal address, telephone number, e-mail address, date of last medical visit, date of birth; - two columns of free comments containing in particular information relating to the pathologies of the patients (HIV, cancers, genetic diseases), the state of pregnancy, the drug treatments followed by the patient or even data genetics;- identification data of the prescribing physician: last name, first name, postal address, telephone number, e-mail address;- data relating to the sampler: last name, first name, address, telephone number;- data relating to the health insurance of the patient: "Paying third party ID" (sequence of numbers), postal address, telephone number; - a "SR identifier" column and a "MP" column, corresponding, with regard to its content, the identifiers and passwords used by the patient to connect to his space.9. Pursuant to Decision No. 2021-029C of the President of the Commission of February 25, 2021, the CNIL carried out a documentary inspection mission to the companies DEDALUS FRANCE and DEDALUS BIOLOGY, in order to verify compliance with the Data Protection Act and Freedoms and the GDPR of the processing implemented by medical analysis laboratories using the solutions or services marketed by these companies. This mission was carried out by sending a questionnaire to DEDALUS FRANCE, sent by email on February 25, 2021.10. On the following February 26, the company sent elements of its response to the CNIL, in particular the names and addresses of the medical analysis laboratories concerned by the aforementioned data breach.11. Pursuant to the same decision, a delegation from the CNIL carried out, on March 1, 2021, an on-site inspection mission to the premises of DEDALUS FRANCE, located at 22, avenue Galilée in PLESSIS-ROBINSON (92350), after informing the territorially competent public prosecutor and the data protection officer of DEDALUS FRANCE and DEDALUS BIOLOGY.12. On March 5, March 10, April 1, April 6 and April 19, 2021, the companies DEDALUS FRANCE and DEDALUS BIOLOGY sent the additional information requested by the delegation during the on-site inspection.13. At the same time, on March 1, 2021, the CNIL had an interim summons issued from hour to hour to the various Internet access providers, so that the effective blocking of the file containing the data of nearly 500,000 patients is ensured. 14. Pursuant to Decision No. 2021-031C of the President of the Commission of March 2, 2021, the CNIL carried out an online verification mission the same day, in order to verify the presence of the disputed file online, by searching for it at from different search engines.15. By order of March 4, 2021, the judge in chambers of the PARIS court

ordered "SA ORANGE, SAS FREE, SA SFR and SA BOUYGUES TELECOM to implement or have implemented, without delay and for a period of 18 months from this decision, all the most appropriate and effective targeted surveillance measures likely to ensure the effective blocking of the online public communication service "[...]" on their networks".16 . Pursuant to Decisions No. 2021-034C and No. 2021-035C of the President of the Commission of March 5, 2021, the CNIL carried out on-site inspections of companies […] and […] on March 10, 2021.17 . The two laboratories having been affected by the aforementioned data breach, it was a question of verifying compliance by these two companies with the provisions of the Data Protection Act and the GDPR.18. By email dated June 11, 2021 sent to the data protection officer of the companies DEDALUS FRANCE and DEDALUS BIOLOGY, the CNIL delegation requested additional information from these companies, which was sent on June 24, 2021.19. For the purposes of examining this case, the President of the Commission, on October 6, 2021, appointed Mr François PELLEGRINI as rapporteur on the basis of Article 39 of Decree No. 2019-536 of May 29, 2019 taken as the application of the amended law of January 6, 1978.20. At the end of his investigation, the rapporteur, on December 9, 2021, had the company DEDALUS BIOLOGY notified of a report detailing the breaches of the GDPR that he considered constituted in this case.21. This report proposed that the restricted committee of the Commission impose an administrative fine on the company, with regard to the breaches of Articles 28 paragraph 3, 29 and 32 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.22. By letter dated December 10, 2021, the company, through its counsel, requested additional time to provide its observations in response. By letter dated December 15, 2021, the chairman of the Restricted Committee granted him additional time until January 24, 2022.23. On January 24, 2022, the company filed submissions in response to the sanction report.24. The rapporteur responded to the company's observations on February 7, 2022. A letter was also sent to the company, informing it that the file was on the agenda of the restricted meeting of March 10, 2022.25. On February 21, 2022, the company produced new observations in response to those of the rapporteur.26. The company and the rapporteur presented oral observations during the session of the restricted committee.II. Reasons for decisionA. On the quality of society with regard to the processing in question27. According to Article 4 of the GDPR, the controller is defined as "the natural or legal person, public authority, service or other body which, alone or jointly with others, determines the purposes and means of processing" (point 7) and the processor is "the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (point 8).28. The rapporteur notes that DEDALUS BIOLOGY markets

software solutions for medical analysis laboratories. As part of the service it offers to laboratories, the company does, on the one hand, only provide laboratories with the tools, in particular computer tools, to facilitate the implementation of processing and, on the other hand, acts only in the name and under the responsibility of the laboratories for the maintenance of the software and, if necessary, the migration to another software for example. The company must therefore be regarded as acting as a subcontractor of the laboratories within the meaning of Article 4, point 8, of the GDPR according to the rapporteur.29. In defence, the company does not dispute the rapporteur's analysis on this point.30. The Restricted Committee considers that the notions of data controller and subcontractor must be the subject of a concrete assessment taking into account all the elements making it possible to attribute one or other of these qualities to a entity. In this respect, it notes that it appears from the elements communicated to the CNIL that the company DEDALUS BIOLOGY acts as a subcontractor for the processing carried out on behalf of its customers, the laboratories, which are responsible for processing, in insofar as it provides laboratories with computer tools allowing them to implement their processing and that it acts, in general, solely on the basis of their instructions.31. It is therefore up to the Restricted Committee to examine, with regard to this capacity, the grievances formulated by the rapporteur against the company.B. On breaches of the GDPR1. On the breach of the obligation to regulate by a formalized legal act the processing carried out on behalf of the data controller32. According to Article 28(3) of the GDPR, "Processing by a processor is governed by a contract or other legal act under Union law or the law of a Member State, which binds the processor vis-à-vis the controller, defines the object and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, and the obligations and the rights of the data controller This contract or other legal act provides, in particular, that the processor: a) only processes personal data on documented instructions from the data controller, including with regard to transfers personal data to a third country or to an international organisation, unless he is required to do so under Union law or the law of the Member State to which the processor is subject ; in this case, the subcontractor informs the manager ble of the processing of this legal obligation before the processing, unless the law concerned prohibits such information for important reasons of public interest; b) ensures that the persons authorized to process the personal data undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality; c) take all the measures required under Article 32; d) comply with the conditions referred to in paragraphs 2 and 4 to recruit another processor; […] ".33. The rapporteur considers that it appears from the information provided by the company DEDALUS BIOLOGY that the various documents governing the contractual relations between the

subcontracting company and the laboratories do not contain the information required by article 28 of the GDPR. It notes that the general conditions of sale proposed by DEDALUS BIOLOGY at the time the laboratories accept its service do not include any of the information required by this article. Similarly, it notes that the information required does not appear in the contracts either. maintenance contracts concluded between the company and the laboratories, as sent to the CNIL.34 In defence, if the company does not contest the materiality of the breach of Article 28 of the GDPR, it specifies that the conclusion of a maintenance contract subcontracting constitutes an obligation for both the data controller and the subcontractor. It concludes that the company DEDALUS BIOLOGY cannot be held solely responsible for this e breach. It also emphasizes the efforts made to comply with the GDPR from 2018 and indicates that new models of subcontracting contracts complying with the requirements of Article 28 are being deployed.35. Firstly, the Restricted Committee notes that the fact that the obligation resulting from Article 28(3) of the GDPR is incumbent on both the controller and the processor has no effect on the existence of liability owned by the subcontractor. It notes that it is the company itself which sends the laboratories its own general conditions of sale which serve as a contractual framework under the GDPR.36. Secondly, the Restricted Committee notes that the general conditions of sale proposed by DEDALUS BIOLOGY at the time the laboratories accept its service, sent by the company as part of the control procedure, do not include any of the statements required by Article 28 GDPR. Similarly, it notes that the required information does not appear either in the maintenance contracts sent to the CNIL, concluded between the company and the laboratories. By way of illustration, the maintenance contract concluded between NETIKA SAS (former name of DEDALUS BIOLOGY) and the company […], on September 13, 2019, certainly includes a part dedicated to personal data, but which does not meet the requirements of Article 28 of the GDPR and refers to obsolete provisions of the Data Protection Act. The Restricted Committee also notes that the sample assistance and maintenance contract, submitted by the company to the CNIL delegation during the on-site inspection of March 1, 2021, does not contain the mandatory information under GDPR Article 28. If it contains a section dedicated to personal data, this does not meet the requirements of this article.37. Thirdly, the Restricted Committee notes that DEDALUS BIOLOGY has deployed new subcontracting contract models and has taken steps to comply with the provisions of Article 28 of the GDPR. However, the fact remains that the company has taken steps with its customers in the context of this procedure and that it was not in compliance at the time of the findings made by the CNIL. Moreover, it is still not so with regard to certain contracts, since the company indicated, in its last observations, to continue its actions aimed at transmitting to all its customers the updated contracts and to negotiate them. if applicable.38. Therefore, in

view of all of these elements, the Restricted Committee considers that these facts constitute a breach of Article 28, paragraph 3, of the GDPR, which the company does not contest.2. On the breach of the obligation for the subcontractor to process personal data only on instructions from the controller39. According to Article 29 of the GDPR, "The processor and any person acting under the authority of the controller or the processor, who has access to personal data, cannot process these data, except on instructions from the controller, unless required to do so by Union law or the law of a Member State". The rapporteur notes that DEDALUS BIOLOGY extracted a larger volume of data than that required for the migration requested by its customers, the […] and […] laboratories. The rapporteur concludes that DEDALUS BIOLOGY has processed data beyond the instructions given by the data controllers, which constitutes a breach of Article 29 of the GDPR.41. In defence, the company specifies that the extraction tool available on the old DXLAB ONE software, used for these migrations, only made it possible to carry out a total extraction of the patient file of the laboratory concerned, without the possibility of adding filters on the fields to be exported to extract only some of them. She adds that DEDALUS BIOLOGY successfully migrated its customers' data to a new software solution in accordance with their instructions, since once the data file to be migrated had been compiled, the company always requested validation from the laboratory concerned before carrying out the migration. The company concludes that it has carried out the extraction operations necessary for the migration and that the scope of the data to be migrated has been defined in this respect in accordance with the instructions of the laboratories concerned and taking into account the technical limitations of the tools used at the period to carry out these migrations.42. In its last observations in response, the company indicates that it "does not intend to minimize the reality of its breach of the obligation to process personal data, as a subcontractor, only on the sole instructions of the data controller". It nevertheless recalls the significant investments made by the company, for several years, in particular to develop new software solutions. She adds that it is precisely because she was aware of the obsolete nature of the MEGABUS software and the associated migration tools that she set out to develop a more innovative solution that respected the requirements of the GDPR and that is how in 2018, it proposed to its customers to switch to KALISIL.43 software. Firstly, the Restricted Committee notes that, as will be established below, the various elements collected within the framework of the inspections of the laboratories […] and […] have made it possible to establish that DEDALUS BIOLOGY had extracted a volume of data greater than that required in the context of the migration requested by its customers.44. With regard to the laboratory […], the on-site inspection report mentions that it requested, "according to the recommendations of DEDALUS", the migration of data from the MEGABUS solution (also called

DXLAB ONE) to the KALISIL for patients who underwent a medical analysis after May 7, 2017. However, the data extracted by DEDALUS BIOLOGY for this migration included 8,403 lines relating to patients whose last visit date was prior to May 7, 2017, which represents 6.5% of the total volume.45. With regard to the laboratory […], the Restricted Committee notes that, as part of a software change, the laboratory asked DEDALUS BIOLOGY to extract the patient database contained in the software DXLAB ONE in order to migrate to another software published and maintained by a third party company. To this end, the company […] provided the DEDALUS company with a list of fields to be extracted in order to be imported into the new software solution. The columns "comment P" (containing information such as "STERILITY 100%", etc.) and "comment D" (containing information such as "BONE TUBERCULOSIS UNDER RIFATER", "XARELTO" (medication), "DIABETES", etc.) were also extracted, even though they did not appear in the list of fields to be extracted.46. Thus, the Restricted Committee concludes that the data extracted by the company DEDALUS BIOLOGY, including in particular the columns "comment P" and "comment D" which should not have been, cover a wider field than the request of the manager treatment.47. Secondly, the Restricted Committee notes that, with regard to the validation of the extractions by the laboratories concerned, the company produces only two documents entitled "after-sales service tickets" in support of its declarations, which cannot in reality suffice to demonstrate that it has carried out the extraction operations in accordance with the instructions of the laboratories and that the laboratories have validated the content of the extractions carried out. These "after-sales service tickets" only make it possible to report on the steps taken by the DEDALUS company with two laboratories to send files with extractions and in no way demonstrate any validation that would have been given by the laboratories concerned.48. The Restricted Committee also notes that the company claims, with regard to […], to have had "a" return email "confirming the compliance of the said file with the instructions of the laboratory". This assertion is inaccurate since, according to the "after-sales service ticket", the "returned email" comes from the company […], a third-party company publishing and now another software to which the extracted data had to be migrated. Thus, this email cannot constitute validation of the extraction by the client, insofar as the company […] is a third-party company.49. Thirdly, the Restricted Committee considers that the company cannot rely on an unsuitable tool to justify having exceeded the instructions of the data controllers. It could, for example, have opted for another tool allowing it to comply with the instructions given by its customers, as it indicates it does now, or at the very least delete all the data which should not have been extracted.50. Given these elements, the Restricted Committee considers that DEDALUS BIOLOGY has processed data beyond the instructions given by the data controllers, which constitutes a breach of Article 29 of the GDPR.3.

On the breach of the obligation to ensure data security51. 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; means to restore the availability of personal data and access to them within an appropriate period of time in the event of a physical or technical incident; d) a procedure for testing, analyzing and evaluating Regularly monitor the effectiveness of the technical and organizational measures to ensure the security of the processing.2. When assessing the appropriate level of security, account is taken in particular of the risks presented by the processing, resulting in particular from the destruction, loss, alteration, unauthorized disclosure of personal data transmitted , stored or processed in any other way, or unauthorized access to such data, accidentally or unlawfully […] ".52. The rapporteur notes that, as of March 2020, a former employee of DEDALUS BIOLOGY had reported safety problems to his employer. According to the rapporteur, it is established that the latter had indeed made relevant reports, which emerges from internal exchanges between […].53. The rapporteur then notes that, on November 4, 2020, the National Information Systems Security Agency (hereinafter "ANSSI") observed that patient data from the laboratory […] were put up for sale on the darknet, under - Internet network provided with anonymous functions bet and in which not all resources are necessarily indexed by search engines. ANSSI sent the laboratory concerned a file containing 56 lines with the personal data of its patients. The same day, the file and the email from ANSSI were sent to DEDALUS BIOLOGY by the director of information systems for the network […], which includes the laboratory […].54. The rapporteur then notes that, on 23 February 2021, the confidential information of nearly 500,000 patients was disseminated on the Internet. As of February 24, 2021, DEDALUS BIOLOGY commissioned the company […] to carry out a forensic analysis mission. Said company submitted its investigation report on March 26, 2021.55. The rapporteur also notes that following its investigations, DEDALUS BIOLOGY established a correspondence between the data in the file transmitted by ANSSI and the data present on an FTP server hosted on the MEGABUS (MEGAEXT) remote maintenance server. Approximately 90% of the personal data of the breached file, published on the Internet in February 2021, was present on the MEGABUS FTP server (MEGAEXT).56. According to the rapporteur, many technical and organizational shortcomings in terms of security were observed during the

CNIL inspections and can be held against the company DEDALUS BIOLOGY. It notes in particular the absence of a specific procedure with regard to data migration operations, the absence of encryption of personal data stored on the MEGABUS FTP server, the absence of automatic deletion of data after migration to another software, the absence of authentication required from the Internet to access the public zone of the MEGABUS FTP server, the use of user accounts shared between several employees with regard to the private zone of this same server and the absence of a supervision and reporting of security alerts to the server.57. The rapporteur concludes that, despite prior alerts, DEDALUS BIOLOGY did not implement satisfactory security measures to supervise the MEGABUS FTP server, which not only allowed access to the data concerned by third parties not authorised, but also the disclosure on forums of a file containing the medico-administrative data of nearly 500,000 people.58. In defence, the company notes, with regard to the data breach that took place in February 2021, that the investigations carried out by the company […] concluded that there were intrusions on the DEDALUS BIOLOGY FTP server. However, it specifies that, although the report notes that 90% of the content of the file circulating on the Internet was also available on the FTP server, it should be noted that, on the contrary, […]'s report stated that around 10% of the file circulating on the Internet (approximately 43,000 records) was not on the FTP server and that approximately 50% of the data on the FTP server was not in the file circulating on the Internet. DEDALUS BIOLOGY concludes that "in view of the remaining inconsistencies between the data present on the FTP server and those circulating on the Internet, the combined investigations of Dedalus Biology and […], which ended on March 26, 2021, did not allow at the time of the facts to conclude with certainty that the said intrusions would be at the origin of the cyberattack reported by the press". Lastly, the company refers to the various security measures put in place since then.59. In its last observations in response, the company indicates that it does not intend to contradict the observations made by the rapporteur on the absence of satisfactory security measures governing the MEGABUS FTP server and specifies that it is aware of the defects of the old technology used by its teams, but again highlights the developments that have taken place in terms of security and its major compliance efforts.60. Firstly, the Restricted Committee notes that it appears from the findings made by the CNIL that the company did not have a specific procedure established with regard to data migration operations. In particular, no security measures were provided for the sending of data, which is sensitive within the meaning of Article 9 of the GDPR. The data extraction files were therefore sent "in the clear" (i.e. directly readable, because they were not previously transformed via a hash function), without any encryption or security measures. However, to ensure the security of migration operations for such a large number of sensitive personal

data, specific procedures should be put in place to describe step by step the sequence of tasks to be carried out, the roles and associated responsibilities. Such procedures also make it possible to have a detailed report of the operations for the laboratories or customers whose data have been processed and transmitted. The absence of such procedures puts the personal data concerned at risk of being compromised, yet easily avoidable, which can lead to the exposure of data relating to private life.61. Secondly, the Restricted Committee notes that several successive alerts should have led the company to carry out investigations into its security system. If, with regard to the report made by ANSSI in November 2020, the company indicates that it has undertaken internal investigations to identify the possible source of compromise and has implemented several corrective and preventive actions, it has not carried out due diligence sufficient to identify whether data from other laboratories may have been compromised and whether existing vulnerabilities were the source of the compromise. The Restricted Committee considers that the company did not take the measure of the security problems it was encountering at the time, which ended up culminating in the February 2021 data breach which affected nearly 500,000 people.62. Thirdly, the Restricted Committee notes that several basic security measures were lacking in this case. The Restricted Committee first notes that the personal data stored on the MEGABUS FTP server was not encrypted and was therefore directly readable, whereas it is sensitive data which, by its nature, requires measures specific safety measures.63. In addition, in the context of migrations from DXLAB ONE software to another software, the data, once transferred to the server, was not erased automatically. However, the retention of the data entails a risk of the data leaking or being compromised.64. The Restricted Committee then notes that the public area of the server, in which certain laboratory data was stored for migration purposes, was freely accessible without authentication from the Internet. It was only on November 4, 2020, the date on which the security incident was reported by ANSSI, that "anonymous" access without authentication to the FTP server was cut off and, on February 23, 2021 only, that this server has been permanently taken offline. In addition, the private zone of the server was accessible with user accounts shared between several employees. However, the use of shared accounts poses a disproportionate, yet easily avoidable, risk to the security of the processing and considerably increases the risk of compromise, in particular due to the circulation of the password between several people. In addition, common (or shared) accounts do not allow proper application of the authorization policy, which is nevertheless a fundamental element of the security of information systems, aimed at limiting access to only data for which a user has need.65. Finally, the Restricted Committee stresses that no supervision and security alert escalation procedure was implemented on the FTP server. Connections from suspicious IP

addresses were therefore neither detected nor processed. The company's digital forensic report […] also confirms that some suspicious connections have been identified, which confirms that the server was exposed on the Internet and that unauthorized connections to this server took place, without they can be identified thanks to these supervision and alert reporting procedures.66. Finally, the Restricted Committee notes that the breach complained of is not constituted by the data breaches as such, but by the security flaws which are at the origin of the intrusion on the company's servers, noted during the inspections carried out by the CNIL. It emphasizes that this rapporteur's proposal, aimed at penalizing security flaws at the origin of violations, is in line with previous decisions of the restricted committee. Thus, in its deliberation No. SAN 2019-007 of July 18, 2019, the Restricted Committee noted "that basic security measures had not been taken prior to the development of its website [by the sanctioned company], which which made possible the occurrence of the personal data breach ".67. The Restricted Committee stresses, however, that the consequences of these security flaws are not excluded from the scope of its analysis, in that they reveal the materialization of the risk generated by these security flaws. The Restricted Committee thus observes that the existing vulnerabilities have been exploited and that several data breaches have taken place: intrusions on the FTP server, followed by the distribution of a file containing the medical-administrative data of nearly 500,000 people on forums in February 2021. In this regard, the Restricted Committee notes that the intrusions on the FTP server are proven and that they are not contested by the company, these having been established by the investigations carried out by […] for the company account. 68. With regard to the distribution of the file on the forums, if the company indicates that it cannot be concluded with certainty that the intrusions on the FTP server are at the origin of the data breach which resulted in the distribution of this file, the Restricted Committee nevertheless observes that it appears from the elements of the file that around 90% of the data in the file published was present on the FTP server. The file distributed on the forums contains in particular the comments which should not have been extracted by the company DEDALUS BIOLOGY within the framework of the migration of the MEGABUS solution to another solution ("comment P" and "comment D" mentioned above). These different elements tend to show the link between the data appearing in the file accessible on the Internet and those which were on the FTP server.69. Thus, the absence of implementation of security measures protecting the server in question - in particular the absence of encryption, the absence of automatic deletion of data after their migration, the absence of authentication required from the Internet to access to the public area of the server and the use of shared user accounts - has led to said data being made accessible to third parties, despite prior alerts to the breach of personal data having led to the disclosure of a file

containing the medico-administrative data of nearly 500,000 people.70. Therefore, the Restricted Committee considers that DEDALUS BIOLOGY has failed to comply with its obligation resulting from the provisions of Article 32 of the Regulations, which the company does not contest. III. On the penalty and publicity71. Under the terms of III of article 20 of the amended law of January 6, 1978, "When the data controller or its subcontractor does not comply with the obligations resulting from regulation (EU) 2016/679 of April 27, 2016 or the this law, the president of the National Commission for Computing and Liberties may also, if necessary after having sent him the warning provided for in I of this article or, if necessary in addition to a formal notice provided for in II, seize the restricted formation of the commission with a view to the pronouncement, after adversarial procedure, of one or more of the following measures: […] 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 ".72. 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 impose an administrative fine and to decide on the amount of this fine.73 Firstly, on the principle of imposing a fine, the company insists in defense on the absence of violation committed previously, on its significant cooperation with the CNIL, on the remedial measures implemented since the personal data breach and on the major compliance efforts undertaken.74 The Restricted Committee recalls that it must take into account, in order to For the imposition of an administrative fine, the criteria specified in Article 83 of the GDPR, such as the nature and seriousness of the violation, the number of persons affected and the level of damage they have suffered, the fact that the breach was negligent, 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.75 . The Restricted Committee notes, first of all, the numerous security flaws surrounding the MEGABUS FTP server, which was insufficiently protected, which led to a massive personal data breach: a large amount of data concerning 491,840 people was disclosed . 76. The Restricted Committee also insists on the extremely harmful nature of the violation for the persons concerned, insofar as, in addition to civil status data (title, surname, first name), postal, electronic and telephone

contact details , very sensitive data was leaked. The file subject to the personal data breach contains information relating to HIV infection, cancers or genetic diseases, pregnancy, drug treatments followed by patients or even genetic data. The data concerned by the breach are health data, which are special categories of data within the meaning of Article 9 of the GDPR (so-called "sensitive" data). Given the nature of the data concerned, the Restricted Committee considers that the company should have exercised particular vigilance with regard to securing such data, to prevent it from being reused by unauthorized third parties, thus prejudice to the persons affected by the data breach. However, the negligence committed in terms of security has been multiple and particularly serious, while the company deals with sensitive data and it had already been alerted to the potential existence of risks, some of which have materialized. The Restricted Committee considers that the breach that led to the data breach is particularly serious.77. It also points out that, given the nature of this personal data, the persons affected by the breach are prime targets for personalized phishing (sending false messages or false documents to recover personal information or money): potential hackers now have their social security number, the name of their prescribing doctor, the date of their examination, the name of the laboratory or, in some cases, information medical. The nature of the personal data compiled also underlies risks of identity theft, fake prescriptions (which may use the names of doctors), fake distress messages repeating the health problems mentioned.78. Finally, the Restricted Committee notes that the company did not take any specific measures to stop the dissemination of the file once it became aware of it. It was the president of the CNIL, and not the company DEDALUS BIOLOGY, who issued a summary summons to ensure the effective blocking of the disputed file.79. If the Restricted Committee notes that the company cooperated throughout the procedure with the services of the CNIL, it considers that the security flaws, which allowed the realization of the data breach, including both the intrusions on the FTP server and the distribution of the file online, result from a negligence of the basic information system security rules which led to the personal data processed by the company being made accessible to unauthorized third parties.80. The Restricted Committee also notes that the fact that DEDALUS BIOLOGY processed personal data beyond the instructions given by the data controllers and therefore committed a breach of Article 29 of the GDPR contributed to aggravating the violation, since comments which should not have been extracted subsequently ended up in the file distributed online and accessible on the forums.81. Finally, the Restricted Committee recalls that the various documents governing the contractual relations between DEDALUS BIOLOGY and the laboratories do not include the information required by Article 28 of the GDPR, which is also not likely to ensure effective protection of the personal data processed through contractual guarantees. 82.

Consequently, the Restricted Committee considers that an administrative fine should be imposed with regard to the breaches of Articles 28, paragraph 3, 29 and 32 of the GDPR.83. Secondly, as regards the amount of the fine, the company points out that […]. The company insists on the fact that the financial situation of the company must be taken into account, so that the imposed fine is adapted to the contributory capacities of the data controller.84. The Restricted Committee recalls that paragraph 3 of Article 83 of the Rules provides that in the event of multiple violations, as is the case here, the total amount of the fine cannot exceed the amount fixed for the most serious violation. Insofar as the company is accused of a breach of Articles 28, 29 and 32 of the GDPR, the maximum amount of the fine that can be withheld is 10 million euros or 2% of annual turnover. worldwide, whichever is higher.85. The Restricted Committee also recalls that administrative fines must be dissuasive but proportionate. It considers in particular that the activity of the company and its financial situation must be taken into account for the determination of the sanction and in particular, in the event of an administrative fine, of its amount. It notes in this respect that the company reports a turnover of 18.8 million euros in 2019 and 16.3 million euros in 2020, for a net result amounting to 2,226,949 euros in 2019 and 1,437,017 euros in 2020.86. In view of these elements, the Restricted Committee considers that the imposition of a fine of 1,500,000 euros appears justified.87. Thirdly, with regard to the publicity of the sanction, the company indicates that the cyberattack which involved it was the subject of very significant publicity, since several press articles were published and then relayed both in the printed press and television, in France and abroad. The incident was also the subject of several communications from the CNIL. It adds that this media coverage will have particularly harmful effects for it, not only in the context of its activity, but also on its turnover.88. Given the seriousness of the breaches committed, particularly the breaches relating to safety, of the number of persons concerned and the consequences for them, the Restricted Committee considers that the publicity of the decision is justified. FOR THESE REASONS The Restricted Committee of the CNIL, after deliberation, decides to: DEDALUS BIOLOGY an administrative fine in the amount of 1,500,000 (one million five hundred thousand) euros; - make public, on the CNIL website and on the Légifrance website, its deliberation, which will no longer identify by name the company at the end of a period of two years from its publication. Chairman Alexandre LINDEN This decision may be appealed to the Council of State within two months from its notification.