Deliberation SAN-2021-019 of October 29, 2021 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Thursday November 04, 2021 Deliberation of the restricted committee n°SAN-2021-019 of 29 October 2021 concerning the Autonomous Paris Transport AuthorityThe National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr. Alexandre LINDEN, President, Mr. Philippe-Pierre CABOURDIN, Vice-President, Mrs. Christine MAUGÜÉ 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. 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 Data Processing and Freedoms; no. 20009228 of May 13, 2020; Having regard to decision no. 2020-101C of June 23, 2020 of the President of the National Commission for Computing and Liberties to instruct the Secretary General to carry out or to have carried out a mission to verify the processing implemented by the Autonomous Paris Transport Authority (RATP); Having regard to the decision of the President of the National Commission for Information Technology and Freedoms appointing a rapporteur to the restricted committee, dated February 12, 2021; Having regard to the report of Mrs. Albane GAILLOT, reporting commissioner, notified to RATP on May 12, 2021; Having regard to the written observations submitted by RATP on June 11, 2021; Having regard to the other documents in the file; e the restricted committee of July 1, 2021:- Mrs Albane GAILLOT, commissioner, heard in her report;In her capacity as representatives of the RATP:- […];- […];- […];The RATP having had the floor lastly;The Restricted Committee adopted the following decision:I. Facts and procedure1. RATP, whose head office is located at 54 quai de la Rapée in Paris (75012), is a public industrial and commercial establishment created by the law of March 21, 1948. RATP is the parent entity of the RATP group, which employed around 65,000 people in 2019. In 2020, its turnover amounted to […] euros and its net profit to […] euros.2. Operations related to the RATP bus network are managed by the BUS department, within the RATP transport and maintenance operations department. The BUS department has approximately 16,000 machinists-receivers (who are the bus drivers), divided into sixteen operational units, each of which covers several bus lines. The social management and innovation department (GIS) is in charge of the group's human resources.3. On May 13, 2020, the National Commission for Computing and Liberties (hereinafter the "CNIL" or the "Commission") received a complaint from the trade union organization CGT-RATP

(referral n° 20009228) relating to an evaluation file for RATP agents, compiled as part of the career advancement procedure for agents in the Bords de Marne bus center. The trade union organization claimed that the file in question contained a certain number of categories of personal data which would give it an illicit, even discriminatory character. This complaint was supplemented by a letter dated June 5, 2020, relating to a similar file concerning the agents of the Quais de Seine bus center.4. On May 18, 2020, RATP notified the Commission of a personal data breach. This notification was supplemented by an additional notification dated June 4, 2020, which developed in particular the description of the breach and the circumstances of its discovery. By these notifications, the RATP reported a violation which would have consisted of the use of a file contrary to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter the " GDPR" or the "Regulations") within the framework of the classification commissions of the agents of the BUS department (joint commissions composed of representatives of the trade unions and the management, aiming to establish which agents benefit from an advancement), resulting in the loss of confidentiality of personal data. This violation allegedly lasted from April 9 to May 11, 2020. RATP further qualified the files in question as contrary to RATP policy and operating rules. The notifications were supplemented by information provided by the RATP by email to the CNIL dated June 11 and August 5, 2020. This information related to the number of bus centers concerned by the violation and, consequently, the number of persons concerned.5. Pursuant to decision no. 2020-101C of June 23, 2020 of the President of the CNIL, a documentary inspection mission was carried out with the RATP, in order to verify compliance by the latter with all of the provisions of the GDPR and of law n° 78-17 of January 6, 1978 as amended relating to data processing, files and freedoms (hereinafter the "law of January 6, 1978 as amended"). More specifically, it was a question of following up on referral no. 20009228 relating to the promotion procedure and the implementation of preparatory files for the classification commissions held in bus centres. This mission was carried out by sending a questionnaire, sent by registered letter of June 26, 2020, to which the RATP replied by letter of July 9, 2020.6. Pursuant to the same decision, a Commission delegation carried out on July 21, 2020 an on-site inspection mission to three bus centres: the Bords de Marne bus centre, that of Aubervilliers and that of Vitry-sur -Seine. These three missions focused on the organization and preparation of the promotion procedure for bus drivers and on the distribution of skills in connection with the management of human resources between RATP headquarters and the bus centres. By email dated July 31, 2020, RATP provided the additional information requested by the delegation during the on-site checks.7. In response to additional requests from the control delegation sent by email on August 11 and September 23, 2020,

RATP provided additional information by email on August 31, October 6 and November 2, 2020. This information related in particular to the different processing of personal data reporting strike days per agent, on the retention period policy for personal data processed by RATP and on the DORA application, which is a tool for viewing and extracting data from from five computer applications for the processing and management of human resources in the BUS department (in particular for the purpose of "exploring operational data" and relating to operating data, quality of service and data relating to human resources and economic).8. During these checks, RATP informed the CNIL delegation that classification commissions are held annually, at the level of each operational unit. In view of these commissions, the management of the operational units makes proposals concerning the agents who, in their opinion, should benefit from a promotion. These proposals are debated during the said commissions. At the end of these commissions, a list of agents benefiting from the advancement is published by the management of the department.9. With regard to the organization and preparation of classification commissions, the delegation was informed that the social management and innovation department is drawing up a list of so-called "proposable" agents (agents eligible for promotion, depending on the date of seniority in their grade) and sends this list to the bus centres. A preparatory meeting is then organized in each operational unit, prior to the commissions, which allows managers to carry out arbitration and during which a list of agents proposed for promotion is drawn up. Bus center management, human resources managers and line team managers (managers, in charge of a team of bus drivers) take part in this arbitration meeting. With a view to this meeting, a decision support file is created by the personnel assigned to the human resources departments of the operational units, at the request of the bus center management. The RATP indicated that these were files in Excel format listing objective data specific to the profession exercised, such as the number of driving days for example. These data are in principle those listed in the corresponding record of the register kept pursuant to the provisions of Article 30 of the GDPR. The promotion proposals established during the arbitration meeting are sent to the members of the classification commission before the commission is held, but not the preparatory files.10. For the purpose of examining these elements, the President of the Commission, on February 12, 2021, appointed Mrs Albane GAILLOT as rapporteur, on the basis of Article 22 of the law of January 6, 1978 as amended.11. At the end of her investigation, the rapporteur notified the RATP, on May 12, 2021, of a report detailing the breaches of the provisions of the GDPR that she considered constituted in this case. This report proposed that the restricted committee of the Commission impose an administrative fine on the RATP and that this decision be made public but no longer allow the public establishment to be identified by name at the end of a period of two years from its

publication.12. Also attached to the report was a summons to the restricted training session of July 1, 2021, indicating to the RATP that it had one month to submit its written observations in application of the provisions of article 40 of the decree. n° 2019-536 of May 29, 2019.13. RATP responded to the sanction report with written observations dated June 11, 2021.14. On June 22, 2021, the RATP made a request for the session before the restricted formation to be held behind closed doors. By letter dated June 24, 2021, the Chairman of the Restricted Committee rejected this request.15. RATP and the rapporteur presented oral observations during the restricted training session.III. Reasons for decisionA. On the status of RATP data controller and the accountability of the processing in question16. The data controller is defined, under the terms of Article 4, point 7 of the GDPR, as "the natural or legal person, public authority, service or other body which, alone or jointly with others, determines the purposes and means of the processing" .17. The rapporteur considers that the RATP is responsible for the processing in question, within the meaning of Article 4.7 of the GDPR, in particular insofar as it determines the purposes and means of the processing relating to the classification commissions. The rapporteur also notes that the RATP carried out the data breach notifications as data controller. Finally, the rapporteur considers that the shortcomings in question are attributable to her in that they do not relate to an isolated incident but to a practice observed in at least six operational units and in that the RATP did not put in implementation of sufficient means to prevent these breaches.18. In defence, the RATP does not dispute its status as data controller. However, it specifies that while it determines the purposes of the processing linked to the classification commissions, each department determines the methods of organization. The RATP also stresses that this is not a generalized practice. In addition, it claims to have implemented sufficient means to prevent the occurrence of facts such as those which are the subject of this procedure, and highlights several actions carried out, such as the training of agents, the appointment of "GDPR referents/correspondents", the documentation made available.19. Firstly, with regard to the responsibility for the processing, the Restricted Committee considers that the RATP is the entity which determines the purposes and means of the processing relating to the preparation of the classification commissions and, therefore, is responsible for the processing in cause. Indeed, the Restricted Committee notes that the central departments of RATP determine the general rules relating to the holding of classification committees and promotion and, thus, the purposes of the processing relating to the preparation of the classification committees, which are not specific to the various departments that carry them out but are common to RATP. It can be noted in this respect that this processing stems in part from the collective agreements negotiated between the trade unions and the RATP. It also provides its various departments with the means that

allow them to carry out processing relating to classification commissions, such as the DORA application. The Restricted Committee also points out that the RATP notified the data breach in its own name, without attributing responsibility for the processing in question in this notification to another entity and that it indicated in this notification that it had acted to end the violation. In addition, it notes that the RATP data protection officer, attached to the services of the general management of the RATP, responded to the requests of the CNIL services, as a representative of the public establishment and not of the different departments in particular.20. Secondly, the Restricted Committee considers that the breaches, the existence of which is being examined in the context of this procedure, are attributable to RATP. In that regard, it observes, admittedly, that the RATP claims that the actions noted do not comply with its operating rules. However, first of all, the Restricted Committee notes that the files in question do not relate to an isolated incident in a bus center. On the contrary, the inspection delegation was able to observe that this practice was established not only in the Bords de Marne bus center, the subject of a complaint, but also in the bus centers of Aubervilliers and Vitry-sur-Seine, which had not been the subject of a report before their control by the delegation.21. Next, the Restricted Committee considers that it is up to the data controller to ensure the implementation of data protection regulations within its departments, in particular by setting up adequate procedures and training Staff. In the present case, RATP is criticized for not having implemented sufficient means to prevent such breaches of the protection of the personal data of its agents in the context of processing relating to classification commissions.B. On the breach relating to the obligation to ensure the adequacy, relevance and non-excessive nature of the personal data processed pursuant to Articles 5.1.c and 5.2 of the GDPR22. Article 5, paragraph 1, c) of the GDPR provides that personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimization)".23. Article 5, paragraph 2, of the GDPR provides: "The controller is responsible for compliance with paragraph 1 and is able to demonstrate that it is complied with (responsibility)" .24. The rapporteur notes that, in the context of the investigation, the CNIL's delegation of control noted that the register sheet relating to the preparation of the classification commissions, established in May 2018, provides for the categories of personal data which are considered necessary for the processing and which may therefore appear in the preparatory files for commissions according to the RATP. These categories of data are as follows: "the surname, first name of the agent, name of the team leader", "the employee number, date of hiring, date of qualification", "the former level with date, the level offered, any bonuses", "the date of the appraisal and progress interviews, progress plans where applicable", "professional evaluation criteria", "presence at work", "unavailability (without distinction between the reasons)",

"accidentology", "any customer complaints, information reports, penalties". The human resources manager of the BUS department also reminded all the human resources management staff of the bus centers, in an email sent on May 5, 2020, that the categories of personal data that may be contained in these files preparations were exhaustively listed in the corresponding register sheet and that the files could not contain other data.25. The rapporteur also notes that it has been observed that the practice of preparing classification commissions in the bus centers inspected consisted in integrating into the preparatory files, in addition to the number of days of absence during the years assessed, data relating to the reasons for the unavailability of agents, including, in particular, the number of strike days per agent during the period assessed (ie three years).26. In the light of these findings, the rapporteur considers that the purpose of the processing constituted by the preparation of the classification committees is the evaluation of staff with a view to taking decisions relating to their promotion and that the processing for this purpose of data relating to the number of strike days per employee appears excessive, in that they do not constitute adequate, relevant and necessary data for the achievement of this purpose.27. In addition, the rapporteur notes that the RATP informed the delegation that, in order to put an end to the data breach notified to the CNIL on May 18, 2020 and before the delegation's checks, it had brought all the preparatory files into compliance. drawn up for the classification commissions for the years 2019 and 2020 in each of the bus centers with the corresponding form in the register of processing activities of the BUS department. The rapporteur notes that the findings do not confirm this assertion insofar as the breach continued on the date of the on-site checks in at least two bus centers (Bords de Marne and Vitry-sur-Seine).28. In defence, the RATP does not dispute the constitution of files containing data relating to the number of days on strike by agents but stresses that this practice is contrary to its internal rules, that it concerns only a few operational units and that the duration of such a practice cannot be established. As for the persistence of the breach to date of the on-site checks, the RATP maintains that it is a technical error due to the poor mastery of the Excel tool and provides declarations from the directors of the operational units concerned attesting that they were unaware of the existence of these tabs, which therefore could not, a fortiori, be used.29. Firstly, with regard to the relevance of the processing of data relating to the number of days on strike, the Restricted Committee notes first of all that the RATP argued, in particular during the checks, that the rules on career development and advancement were determined by collective agreements negotiated with the trade unions. These agreements do not provide for automatic advancement but take into account the evaluation of individual performance. The RATP has specified the categories of data that may appear in the preparatory files for the classification commissions and,

among these, are the data relating to "presence at work" and "unavailability (without distinction between the reasons)". The Restricted Committee notes that these criteria are reflected in particular, in the preparatory files in question, by columns relating to the number of working days, the "driving" time, the number of days of rest and the number of days of absence. . As regards this last column, the applicable rules do not require it to contain the reason for the absences.30. The restricted training thus points out that the number of days of absence, in the same way as, for example, the number of days of work and the number of days of rest, is a data which can be taken into consideration within the framework of the agreements collectives.31. It notes that the collective agreements provide that certain absences, such as absence linked to maternity leave, must appear separately so that this data is not taken into account unfavorably in the evaluation of the performance of the agent. concerned. On the other hand, apart from these exceptions defined in the agreements, it does not follow from this set of rules that the reasons for the absence of staff can be taken into account for their assessment.32. Consequently, if the Restricted Committee does not question the relevance of the treatment of the number of days of absence with regard to the rules set, in particular by the collective agreements, it considers that it is not relevant, with a view to the evaluation of agents, to treat data relating to the number of days on strike as a separate category from the total number of days of absence. Indeed, knowledge of the reason for the absence is not necessary. The Restricted Committee also notes that the dedicated record of the processing register specifies that, among the categories of data provided for as being able to appear in these files, only "unavailability (without distinction between the reasons)" appears. Therefore, it appears excessive and contrary to the principle of minimization to individualize the category of the number of days on strike among the absences recorded and to process this data for these purposes.33. The RATP did not deny the illicit nature of the files produced in certain bus centers in the context of the preparation of the classification commissions and argued that such a practice was contrary to its general policy.34. The Restricted Committee considers that, insofar as the files in question constitute decision support files, they can only be composed of the personal data necessary for taking decisions relating to the evaluation, which have been previously determined.35. Finally, the Restricted Committee underlines the specificity of the data relating to the exercise of the right to strike by an agent and notes that the processing of this personal data is not neutral. Indeed, the processing of this particular category of data by an employer must be limited to certain legitimate purposes and must fit within the legal framework resulting in particular from Article L. 1324-7 of the Transport Code and the article R. 3243-4 of the labor code.36. Secondly, with regard to the number of people affected by this processing, the Restricted Committee notes that the RATP reported, through the data

breach notifications as well as the subsequent emails sent to the CNIL on June 11 and August 5, 2020 , the existence of files containing data relating to strike days in four operational units (Bords de Marne, Quai de Seine, Paris Sud-Ouest and Rives-Nord). CNIL checks in two other operational units, selected at random, also revealed the existence of these progress files. Six operational units out of the existing sixteen are therefore concerned, the others not having been subject to checks. The Restricted Committee therefore notes that these are not isolated facts.37. Thirdly, with regard to the persistence of the practice in question, the Restricted Committee notes that the RATP argued during the inspection that, following its discovery of the file at the Bords de Marne bus center, it had carried out, on May 11 and 12, 2020, an analysis of all the preparatory files established for the classification commissions for the years 2019 and 2020 in each of the bus centers and brought all of these files into conformity with the corresponding sheet of the register of processing activities of the BUS department. The Restricted Committee stresses that it was nevertheless found, during checks in the bus centers of the Bords de Marne and Vitry-sur-Seine, that the files relating to the year 2020, presented by the RATP as purged of any data not necessary, contained tabs containing details of staff unavailability and, in particular, data relating to strike days.38. In this respect, if, to justify that this failure continued, the RATP argued that it was a technical error and provided statements from the directors of the operational units concerned attesting that they were unaware of the existence of these "hidden" tabs, which therefore could not be used, the Restricted Committee considers that the RATP cannot rely on its repeated poor command of the Excel tool to justify the presence of certain data in the files in question. Furthermore, even in the event that the directors of the operational units concerned were unaware of the presence of the tabs in question in the files concerned, that does not call into question the materiality of the breach found.39. Finally, the Restricted Committee recalls that the obligation to process only adequate, relevant and necessary data implies not only that of defining the data which must be processed but also of putting in place the measures, in particular organizational measures, relevant to ensure that only those data necessary for the purposes are actually processed. However, the Restricted Committee observes that that was not the case in the present case, as evidenced by the occurrence of the facts in question.40. Indeed, it is clear that, although contrary to the general policy of the RATP, the practice in question does not constitute an isolated act, which would have concerned only a small group of agents. On the contrary, first of all, this practice results in particular from the lack of rigor in the supervision of the organization of promotion procedures as well as the tools made available to the various departments in this context. In particular, the configuration of the DORA tool, which only allows the extraction of all the data relating to an agent or even to all the agents of

a bus center, without possible to sort between the categories of data to be selected for extraction, was likely to contribute to the creation of classification commission files containing data that were inadequate for the purpose pursued. In addition, the Restricted Committee notes that certain organizational measures, such as the one mentioned by RATP during the procedure in order to prevent such practices from recurring - consisting in the creation of a common Excel tool which must be used to data extractions in DORA (and other relevant applications) carried out for the constitution of preparatory files, in order to freeze what a preparatory table may contain in terms of data - now make it possible to prevent the emergence of such practices, and could have been usefully implemented before the present proceedings were initiated.41. In view of all of the foregoing, the Restricted Committee considers that it was the responsibility of the RATP, as data controller, to ensure that only the categories of personal data necessary to take decisions relating to the evaluation to constitute the files in question, in accordance with articles 5.1.c and 5.2 of the GDPR. Consequently, the RATP failed in its obligations by including in these files data relating to the number of strike days per agent during the period assessed and by failing to ensure that the purge decided upon following the discovery of the files in question is actually implemented.42. The Restricted Committee therefore considers that these facts constitute a breach of Articles 5, paragraph 1, e), and 5, paragraph 2, of the GDPR.C. On the breach of the obligation to define and respect a retention period for personal data proportionate to the purpose of the processing pursuant to Article 5.1.e of the GDPR43. Under the terms of Article 5.1.e of the Regulation, personal data must be “kept in a form allowing the identification of the persons concerned for a period not exceeding that necessary with regard to the purposes for which they are processed; personal data may be stored for longer periods insofar as they will be processed exclusively for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89 , paragraph 1, provided that the appropriate technical and organizational measures required by this Regulation are implemented in order to guarantee the rights and freedoms of the data subject (restriction of storage)" .1. With regard to the retention periods of the data accessible in the DORA44 application. The rapporteur notes that the delegation was informed that the DORA application is a tool for viewing and extracting data from five IT applications, which are implemented for the processing and management of human resources in the BUS department . RATP has indicated that this application is intended in particular to "explore operational data" (operating data, quality of service, data relating to human and economic resources). As a visualization tool, it does not allow users to modify data in drillable information systems, but allows them to extract it to Excel files.45. The rapporteur also notes that the delegation was informed that the personal data contained in DORA are kept, on an active basis,

for the duration of the agent's employment in the BUS department, extended by six years. The rapporteur stresses that the RATP has not been able to justify this retention period of the data with regard to the purposes for which they are processed and considers that this retention period in the active database of the data in the DORA tool is therefore excessive. .46. In defence, the RATP argues that the retention period which had been indicated to the delegation of control, namely the duration of the agent's employment in the BUS department, extended by six years, was incorrect and that this duration corresponded the retention period of the data in the archive database and not in the active database. In its written submissions, the RATP explains that the retention period in the active database was in fact six years on the date of the checks carried out by the CNIL. It further states that this duration was considered excessive during internal work and that it was reduced to two years, plus the current year, after the checks carried out by the delegation.47. The Restricted Committee first takes note of the clarifications provided by the RATP during the procedure and in particular the fact that the data was kept in an active database in DORA for six years and not for the length of the employment extended by six years. .48. The Restricted Committee recalls that the retention period for personal data must be determined according to the purpose pursued by the processing. When this purpose is achieved, the data must in principle be deleted, anonymized or subject to intermediate archiving when their retention is necessary for compliance with legal obligations or for pre-litigation or litigation purposes.49. In this case, the DORA application is a data visualization tool for the purposes of human resources management in the BUS department, with the purpose of "exploring operational data". It must allow, among other things, monitoring of agent activity. The Restricted Committee notes that this purpose, as identified by the RATP, is very broad and imprecise, and that it does not allow a precise understanding of the resulting operational needs. In addition, nothing in the file makes it possible to determine what purposes would justify the agents authorized to access DORA being able, in order to achieve them, to view all of these data relating to human resources over a period of six years. For example, this information includes data relating to the number of days on strike per agent, which is used in particular to calculate the payroll and social security contributions. The RATP does not establish why this information should be kept in the DORA application, once the payslip is established, for a period of six years, whereas a much shorter period on an active basis would be sufficient to payroll establishment. Other purposes, such as viewing information for monitoring agent activity, may justify a longer duration, but the need to go back over the previous six years has not been established.50. The Restricted Committee also notes that, far from being able to justify the retention period of all the data in the DORA application with regard to the purposes of this tool, the RATP has on the contrary argued that the duration of

retention of the DORA application in an active database, at the date of the checks, had been considered excessive with regard to the exploration purposes of this application. This duration was, during the procedure, reduced to two years plus the current year, to allow managers to monitor the activity of agents over a short but sufficiently significant period to see the changes.51. Consequently, the Restricted Committee considers that the retention of the personal data in question for six years on an active basis, without a differentiated and adapted approach to data retention with regard to the specific purposes for which they are processed being implemented. , did not make it possible to comply with the principle of limiting the duration of data retention.52. In view of all of these elements, the Restricted Committee considers that the breach of Article 5, paragraph 1, e) of the GDPR is clear.2. With regard to the retention period of the preparation files of the classification commissions53. The rapporteur notes that the delegation has been informed that the planned retention period for the classification commission preparation files is eighteen months, starting from the holding of the classification commission for which they are drawn up. This duration is provided for on the corresponding register sheet, depending on the purpose of this processing (decision-making support for the evaluation of agents). However, the delegation noted that, in the bus centers of Aubervilliers and Vitry-sur-Seine, preparation files for the 2017 classification commissions were present on the servers.54. In view of these findings, the rapporteur criticizes the RATP for keeping the files in question for a period that exceeds that necessary for the purpose of the processing and for not effectively implementing its retention period policy. 55. In defence, the RATP emphasizes the isolated nature of the facts.56. The Restricted Committee notes that the commission preparation files are drawn up as a support for decision-making for preparatory meetings for the annual classification commissions, with a view to evaluating agents, and can therefore only be kept for the time necessary to the achievement of this purpose. The Restricted Committee observes that the RATP has set their retention period at eighteen months after the classification commission for which these files are produced, having considered that this was the period necessary for the purpose of the processing.57. However, the Restricted Committee notes that the CNIL delegation noted the retention, in the bus centers of Aubervilliers and Vitry-sur-Seine, of the preparation files for the classification commissions dating from 2017, which corresponds to a duration of more than three years after the meeting of the classification commission concerned. The Restricted Committee considers that this retention is excessive insofar as it exceeds the duration necessary to achieve the purpose pursued, which is, according to the RATP, eighteen months after the classification commission for which these files are made. . The planned retention period for the classification commission preparation files is therefore not effectively implemented since only files relating to the 2019

and 2020 classification commissions should have been able to appear on the servers on the date of the checks. However, the effectiveness of the implementation of a data retention period policy is the necessary counterpart of its definition and makes it possible to ensure that the data is kept in a form allowing the identification of the persons concerned for a period of time. not exceeding that necessary with regard to the purposes for which they are processed. This also makes it possible, in particular, to reduce the risk of unauthorized use of the data in question, by an employee or by a third party.58. Consequently, the Restricted Committee considers that the RATP has breached its obligations under Article 5, paragraph 1, e), of the GDPR.D. On the breach of the obligation to ensure the security of personal data pursuant to Article 32 of the GDPR1. On authorizations for access and extraction of data in DORA59. Article 32 of the Regulation provides: "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, 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;[…]".60. The rapporteur notes that the delegation was informed that the DORA tool enables all authorized agents, whatever their assignments, to carry out the same actions and, thus, not only to view the personal data stored in the tool but also to extract all of this data. The rapporteur therefore considers that DORA's authorization policy does not make it possible to limit users' access to only the data they actually need in the context of their duties, it being recalled that the DORA tool contains a large volume of data, particularly in connection with human resources management, and relating to all staff in the BUS and MRB (bus rolling stock) departments.61. In defence, the RATP maintains that the system cannot be partitioned and that all authorized agents need to have access to all the data as part of their duties. It also argues that transversal access between business units corresponds to an operational and organizational need and specifies in this respect that business unit directors need to have access to data from all business units in order to ensure continuity of service. RATP also maintains that it is in the process of implementing an action plan aimed at partitioning the access of the "operational unit management" and "HR assistant" profiles to the data of the operational unit to which they are attached. 62. The Restricted Committee recalls in this regard that pursuant to Article 32 of the GDPR, the data controller must put in place appropriate measures to ensure the confidentiality of the data and to prevent the data from being processed unlawfully by the fact of people who don't need to know. The prevention of misuse and data breaches can be partly ensured by

organizational measures, in particular by informing the users of the information system of the data that they are authorized to process for their missions, by controlling the use that is done, in particular by means of connection logs, and by disciplinary sanctions for non-compliance with the applicable rules. In addition to these measures, the management of authorizations to consult or use an information system must tend to limit access to only the personal data that a user needs for the accomplishment of his missions, in particular by defining profiles empowerment in systems by separating tasks and areas of responsibility. It is therefore up to the data controller to put in place, depending on the greater or lesser diversity of users' missions, an authorization management policy that is appropriate to the importance and sensitivity of the data processed, as well as the risks to which the persons concerned are exposed, according to the means at his disposal.63. By way of illustration, the Restricted Committee notes that the Guide for the development of an information system security policy of the National Agency for the Security of Information Systems (published in 2004) specifies in this respect that the definition authorizations must respect the principle of the need to know: all actors will have exclusive access to the information they need in the performance of their task.64. In the present case, the Restricted Committee notes, firstly, that all DORA users authorized to access the "check-in" part of the tool have access to data relating to all agents of the BUS and MRB departments. On the one hand, all authorized agents therefore have access to all categories of data (all data relating to human resources and thus, in particular, data relating to strike days or sick leave) without distinguishing functions or missions of agents. On the other hand, these agents access the data relating to the agents of their operational unit but also of all the other operational units (i.e. more than 16,000 people), without the need for this access for all the agents having been established. by the RATP. On the contrary, the latter explained in its written observations that it was in the process of implementing an action plan aimed at partitioning the access of certain profiles solely to the data of the operational unit to which they are attached and, thus, to define a stricter clearance policy.65. Secondly, the Restricted Committee considers that the configuration of the tool does not ensure the confidentiality of the data within the meaning of Article 32 of the GDPR insofar as all the authorized agents can extract all the data contained in the tool. Indeed, the delegation found that the security clearance policy did not make it possible to distinguish, according to the functions of the authorized agents, whether the ability to extract personal data was necessary with regard to their functions.66. Consequently, the Restricted Committee considers that the authorization policy of the DORA tool does not make it possible to guarantee that the authorized persons have access only to the data strictly necessary for their functions. She believes that the authorization policy should be more refined and allow the creation of more

different profiles, relating to the functions of the agents or the bus centers to which they are assigned, as the RATP now plans to put in place, a fortiori given the volume of data and the sensitivity of certain data accessible in the tool.67. In view of all of these elements, the Restricted Committee considers that the level of confidentiality of the personal data contained in this tool does not comply with the requirements of Article 32 of the GDPR.2. On access authorizations to the preparation files of the classification commissions68. The rapporteur stresses that the delegation noted that, at the Aubervilliers bus centre, the files for preparing the classification commissions were accessible on a server to all participants in the arbitration meetings for which they were drawn up. Thus, these preparatory files were accessible not only to center management and the human resources department, who could in any event view the data contained in these files on DORA, but also to all line team managers , who are not authorized to consult this data in DORA. The thirteen line team managers therefore had access to the personal data of all the bus drivers who could be offered for promotion to the bus center (about 800 bus drivers are assigned to this bus center, of which only a part is "proposable" each year).69. The rapporteur considers that the fact that the preparatory files for the classification commissions are accessible on a server to all line team managers does not make it possible to guarantee the confidentiality of the data insofar as these files contain a great deal of data to personal character of agents, and in particular of agents who are not under their responsibility.70. In defence, the RATP maintains that all the authorized managers need, within the framework of the preparatory meeting, to have visibility on the data relating to all the bus drivers who can be proposed from the same operational unit, to to be able to arbitrate. It specifies that the provision of these files to all managers is necessary in order to ensure the collegiality of decisions during the arbitration meetings in question.71. With regard to the provisions of Article 32 of the GDPR mentioned above, the Restricted Committee considers that the confidentiality of the data contained in the preparatory files for the classification commissions at issue in this case is not guaranteed when the files are made available to all line team managers, without distinguishing between agents under their responsibility or not. Indeed, it notes first of all that if it is legitimate for the line team managers to have access to the personal data of the agents under their responsibility upstream of the commissions, in order to decide on their possible Further, it does not appear proportionate for the personal data of all bus center bus drivers to be available to them on a server.72. The Restricted Committee then notes that the practice called into question by the rapporteur differs from that observed in the other bus centers inspected, where these files are not made available to line team managers before the arbitration meeting, but only projected at these meetings. It notes that this practice does not call into question the collegiality of decisions and, thus, satisfies the purpose of the processing, while

ensuring a higher degree of confidentiality of the data. In this regard, the Restricted Committee considers that the risks associated with the loss of confidentiality of data, such as the reuse of the latter, are much lower when the data in question is only projected, for the duration of a meeting, and not available on a server.73. Consequently, the Restricted Committee considers that the practice observed in the other bus centers inspected allows it to be considered that the risk associated with the fact that the files in question are accessible on a server to all line team managers is not proportionate to the purpose sought, that is to say the need for the participants in the arbitration meetings to have knowledge of these data from time to time in order to participate in the arbitrations.74. In view of all of these elements, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 32 of the GDPR.IV. On corrective measures and their publicity75. Under the terms of III of article 20 of the modified law of January 6, 1978: "When the data controller or its subcontractor does not comply with the obligations resulting from regulation (EU) 2016/679 of April 27, 2016 or from the this law, the president of the National Commission for Computing and Liberties may also, if necessary after having sent him the warning provided for in I of this article or, if necessary in addition to a formal notice provided for in II, seize the restricted formation of the commission with a view to the pronouncement, after adversarial procedure, of one or more of the following measures: […] 7° With the exception of cases where the processing is implemented by the State, an administrative fine not to exceed 10 million euros or, in the case of a company, 2% of the total worldwide annual turnover of the previous financial year, whichever is higher. mentioned in 5 and 6 of article 83 of regulation (EU) 2016/6 79 of April 27, 2016, these ceilings are increased to €20 million and 4% of said revenue respectively. The restricted committee takes into account, in determining the amount of the fine, the criteria specified in the same article 83". 76. 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 to decide whether to impose an administrative fine and to decide on the amount of this fine.77 Firstly, on the principle of imposing an administrative fine, the RATP maintains that such a measure is not necessary. account must be taken of the circumstances of the case and in particular of the measures which it adopted during the procedure. It also maintains that the majority of the decisions rendered against public establishments were not sa financial ctions when "the breaches seemed to relate to similar facts" .78. 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.79. The Restricted Committee considers first of all that the RATP has shown serious failures in terms of the protection of personal data since breaches are made up of fundamental and elementary principles of the GDPR, which are the principles of data minimization, responsibility, limitation of the duration of data retention and security.80. The Restricted Committee notes that by breaching the principle of minimizing personal data, the RATP has demonstrated certain negligence, relating to a fundamental principle of the GDPR. Indeed, data relating to the exercise of the right to strike by an agent has been made accessible to people who did not have to know about it. The Restricted Committee notes that while, in the context of certain other processing activities, the data controller could process this data, the situation is different in the context of the evaluation of agents, for which the number of strike days per agent was not relevant data. In addition, the use of this particular data, in the context of decision-making relating to the agent's career, may be unfavorable to him.81. Next, the Restricted Committee notes that, even after being informed of the violation and after carrying out a "social alert" procedure in consultation with the trade unions, the RATP did not take all the necessary measures to ensure the conformity of all the bus centers since the persistence of the breach of article 5.1.c) of the GDPR was noted during the checks, although the RATP affirmed to the CNIL that it had brought all the files into conformity in all bus centers.82. In addition, with regard to the breach relating to the retention period of the data, the Restricted Committee notes that the RATP stated, during the inspection, that it considered that the retention period set was excessive, without however having implemented effective manner of the measures allowing the compliance of its data retention period policy.83. The Restricted Committee also notes that several shortcomings observed concerned a large number of people, namely approximately 16,000 agents of the BUS department, which led a trade union organization to seize the CNIL.84. Finally, the Restricted Committee notes that the compliance measures adopted during the procedure do not cover all the breaches and do not, in any event, exonerate RATP from its liability for the past.85. Consequently, the Restricted Committee considers that an administrative fine should be imposed with regard to the breaches of Articles 5-1-c), 5-1-e), 5-2 and 32 of the GDPR.86. Secondly, with regard to the amount of the fine, RATP highlights the measures taken to remedy all of the allegations referred to in the report and its commitment to pursue all of these measures. She also maintains that her financial situation, mainly due to the health crisis, must be taken into consideration. Finally, she argues that the amount proposed by the rapporteur would be disproportionate with regard to the previous decisions of the CNIL.87. 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 RATP is alleged to have breached Articles 5-1-c), 5-1-e), 5-2 and 32 of the Regulations, the maximum amount of the fine that may be withheld is EUR 20 million or 4% of worldwide annual turnover, whichever is greater.88. The Restricted Committee also recalls that administrative fines must be dissuasive but proportionate. It considers in particular that the activity of the organization 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 RATP reports a turnover in 2020 of around […] euros for a net result of […] euros, whereas the net result amounted to […] euros in 2019.89. Therefore, in view of the economic context caused by the Covid-19 health crisis, its consequences on the financial situation of RATP, its compliance efforts and the relevant criteria of Article 83, paragraph 2, of the GDPR mentioned above, the Restricted Committee considers that the imposition of an administrative fine of 400,000 euros appears justified.90. Thirdly, with regard to the publicity of the sanction, the RATP maintains that such a measure would cause it a disproportionate harm and argues in particular that it would harm its strategy of reminding users and that it would be harmful for the relations maintained by the RATP with its agents.91.In view of the plurality of breaches noted, their persistence, their seriousness and the number of people concerned, the Restricted Committee considers that the publication of this decision is justified.PAR THESE REASONSThe Restricted Committee of the CNIL, after having deliberated, decides to:- pronounce against the Régie Autonome des Transports Parisiens an administrative fine in the amount of 400,000 (four hundred thousand) euros with regard to the breaches Articles 5-1-c), 5-1-c), 5-1-e), 5-2 and 32 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 relating to the protection personal data and free c circulation of this data; - make public, on the CNIL website and on the Légifrance website, its deliberation, which will no longer identify the Régie Autonome des Transports Parisiens by name at the end of a period of one year from from its publication. President Alexandre LINDEN This decision may be appealed to the Council of State within two months of its notification.