



## **Délibération SAN-2021-019 du 29 octobre 2021**

### **Commission Nationale de l'Informatique et des Libertés**

Nature de la délibération : Sanction

Date de publication sur Légifrance : Jeudi 04 novembre

Etat juridique : En vigueur

2021

### **Délibération de la formation restreinte n°SAN-2021-019 du 29 octobre 2021 concernant X**

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de Monsieur Alexandre LINDEN, président, Monsieur Philippe-Pierre CABOURDIN, vice-président, Madame Christine MAUGÜÉ et Monsieur Bertrand du MARAIS, membres ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 20 et suivants ;

Vu le décret no 2019-536 du 29 mai 2019 pris pour l'application de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération no 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la saisine no du 13 mai 2020 ;

Vu la décision n° 2020-101C du 23 juin 2020 de la présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements mis en œuvre par X ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 12 février 2021 ;

Vu le rapport de Madame Albane GAILLOT, commissaire rapporteure, notifié à X le 12 mai 2021 ;

Vu les observations écrites versées par X le 11 juin 2021 ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 1er juillet 2021 :

- Madame Albane GAILLOT, commissaire, entendue en son rapport ;

En qualité de représentants de X :

- [...] ;

- [...] ;

- [...] ;

X ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

## I. Faits et procédure

1. X dont le siège social est situé [...], est un établissement public à caractère industriel et commercial. X est l'entité mère du groupe X, qui employait en 2019 environ 65 000 salariés. En 2020, son chiffre d'affaires s'élevait à [...] euros et son résultat net à [...] euros.
2. Les opérations en lien avec le réseau de bus de X sont gérées par le département BUS, au sein de la direction des opérations de transport et de maintenance de l X. Le département BUS compte environ 16 000 machinistes-receveurs (qui sont les conducteurs de bus), répartis en seize unités opérationnelles, qui couvrent chacune plusieurs lignes de bus. La direction gestion et innovation sociales (GIS) est en charge des ressources humaines du groupe.
3. Le 13 mai 2020, la Commission nationale de l'informatique et des libertés (ci-après la " CNIL " ou la " Commission ") a été saisie par l'organisation syndicale CGT-X d'une plainte (saisine n°) portant sur un fichier d'évaluation des agents de X, constitué dans le cadre de la procédure d'avancement de carrière des agents dans le centre de bus X. L'organisation syndicale faisait valoir que le fichier en cause contenait un certain nombre de catégories de données à caractère personnel qui lui confèreraient un caractère illicite, voire discriminatoire. Cette plainte a été complétée par un courrier en date du 5 juin 2020, portant sur un fichier similaire concernant les agents du centre de bus X.
4. Le 18 mai 2020, X a notifié à la Commission une violation de données à caractère personnel. Cette notification a été complétée par une notification complémentaire en date du 4 juin 2020, qui développait notamment la description de la violation et des circonstances de sa découverte. Par ces notifications, X faisait état d'une violation qui aurait consisté en l'utilisation d'un fichier contraire aux dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le " RGPD " ou le " Règlement ") dans le cadre des commissions de classement des agents du département BUS (commissions paritaires composées de représentants des organisations syndicales et de la direction, visant à établir quels agents bénéficient d'un avancement), entraînant la perte de confidentialité de données à caractère personnel. Cette violation aurait duré du 9 avril au 11 mai 2020. X a en outre qualifié les fichiers en cause de contraires à la politique et aux règles de fonctionnement de X. Les notifications ont été complétées par des informations fournies par X par courriels à la CNIL en date des 11 juin et 5 août 2020. Ces informations portaient sur le nombre de centres de bus concernés par la violation et, par conséquent, sur le nombre de personnes concernées.
5. En application de la décision n° 2020-101C du 23 juin 2020 de la présidente de la CNIL, il a été procédé à une mission de contrôle sur pièces auprès de X, afin de vérifier le respect par cette dernière de l'ensemble des dispositions du RGPD et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après la " loi du 6 janvier 1978 modifiée "). Il s'agissait plus particulièrement de donner suite à la saisine n° relative à la procédure d'avancement et à la mise en œuvre de fichiers préparatoires aux commissions de classement tenues dans les centres de bus. Cette mission s'est effectuée par l'envoi d'un questionnaire, adressé par lettre recommandée du 26 juin 2020, auquel X a répondu par courrier du 9 juillet 2020.
6. En application de la même décision, une délégation de la Commission a procédé le 21 juillet 2020 à une mission de contrôle sur place dans trois centres de bus : le centre de bus X, celui d'X et celui de X. Ces trois missions ont porté sur l'organisation et la préparation de la procédure d'avancement des conducteurs de bus et sur la répartition des compétences en lien avec la gestion des ressources humaines entre le siège de X et les centres de bus. Par courriel en date du 31 juillet 2020, X a fourni les éléments complémentaires sollicités par la délégation lors des contrôles sur place.
7. En réponse aux demandes complémentaires de la délégation de contrôle transmises par courriels des 11 août et 23 septembre 2020, X a fourni des éléments complémentaires par courriels des 31 août, 6 octobre et 2 novembre 2020. Ces éléments portaient notamment sur les différents traitements de données à caractère personnel faisant état des journées de grève par agent, sur la politique de durées de conservation des données à caractère personnel traitées par X ainsi que sur l'application X, qui est un outil de visualisation et d'extraction des données à partir de cinq applications informatiques pour le traitement et la gestion des ressources humaines du département BUS (ayant notamment pour finalité " l'exploration de données opérationnelles " et portant sur des données d'exploitation, la qualité de service et les données relatives aux ressources humaines et économiques).
8. Au cours de ces contrôles, X a informé la délégation de la CNIL que des commissions de classement sont tenues annuellement, au niveau de chaque unité opérationnelle. Dans la perspective de ces commissions, la direction des unités opérationnelles formule des propositions concernant les agents qui devraient, selon elle, bénéficier d'un avancement. Ces propositions sont débattues lors des dites commissions. À l'issue de ces commissions, une liste des agents bénéficiant de l'avancement est éditée par la direction du département.
9. S'agissant de l'organisation et de la préparation des commissions de classement, la délégation a été informée que la direction gestion et innovation sociales élabore une liste d'agents dits " proposables " (agents éligibles à l'avancement, en fonction de la date d'ancienneté dans leur grade) et transmet cette liste aux centres de bus. Est ensuite organisée dans chaque unité opérationnelle, en amont des commissions, une réunion préparatoire qui permet aux managers de réaliser

un arbitrage et pendant laquelle est élaborée une liste des agents proposés à l'avancement. La direction du centre de bus, les responsables des ressources humaines et les responsables d'équipe de lignes (managers, en charge d'une équipe de conducteurs de bus) participent à cette réunion d'arbitrage. En vue de cette réunion, un fichier d'aide à la décision est créé par les personnels affectés aux services des ressources humaines des unités opérationnelles, à la demande des directions des centres de bus. X a indiqué qu'il s'agissait de fichiers sous format Excel recensant des données objectives propres au métier exercé, telles que le nombre de jours de conduite par exemple. Ces données sont en principe celles listées dans la fiche correspondante du registre tenu en application des dispositions de l'article 30 du RGPD. Les propositions d'avancement établies lors de la réunion d'arbitrage sont transmises aux membres de la commission de classement en amont de la tenue de la commission mais pas les fichiers préparatoires.

10. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 12 février 2021, désigné Madame Albane GAILLOT en qualité de rapporteure, sur le fondement de l'article 22 de la loi du 6 janvier 1978 modifiée.

11. À l'issue de son instruction, la rapporteure a fait notifier à X, le 12 mai 2021, un rapport détaillant les manquements aux dispositions du RGPD qu'elle estimait constitués en l'espèce. Ce rapport proposait à la formation restreinte de la Commission de prononcer à l'encontre de X une amende administrative et que cette décision soit rendue publique mais ne permette plus d'identifier nommément l'établissement public à l'expiration d'un délai de deux ans à compter de sa publication.

12. Était également jointe au rapport une convocation à la séance de la formation restreinte du 1er juillet 2021 indiquant à X qu'elle disposait d'un délai d'un mois pour communiquer ses observations écrites en application des dispositions de l'article 40 du décret n° 2019-536 du 29 mai 2019.

13. X a répondu au rapport de sanction par des observations écrites en date du 11 juin 2021.

14. Le 22 juin 2021, X a formulé une demande pour que la séance devant la formation restreinte se tienne à huis clos. Par courrier du 24 juin 2021, le président de la formation restreinte a rejeté cette demande.

15. X et la rapporteure ont présenté des observations orales lors de la séance de la formation restreinte.

### III. Motifs de la décision

#### A. Sur la qualité de responsable de traitement de X et l'imputabilité des traitements en cause

16. Le responsable de traitement est défini, aux termes de l'article 4, point 7 du RGPD, comme " la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ".

17. La rapporteure estime que X est responsable des traitements en cause, au sens de l'article 4.7 du RGPD, notamment dans la mesure où elle détermine les finalités et les moyens des traitements relatifs aux commissions de classement. La rapporteure relève également que X a procédé aux notifications de violation de données en tant que responsable de traitement. Enfin, la rapporteure estime que les manquements en cause lui sont imputables en ce qu'ils ne relèvent pas d'un incident isolé mais d'une pratique constatée dans au moins six unités opérationnelles et en ce que X n'a pas mis en œuvre de moyens suffisants pour prévenir ces manquements.

18. En défense, X ne conteste pas sa qualité de responsable de traitement. Elle précise cependant que si elle détermine les finalités des traitements liés aux commissions de classement, chaque département en détermine les modalités d'organisation. X souligne également qu'il ne s'agit pas d'une pratique généralisée. En outre, elle se prévaut d'avoir mis en œuvre des moyens suffisants pour prévenir la survenance de faits tels que ceux qui font l'objet de la présente procédure, et met en avant plusieurs actions réalisées, telles que la formation des agents, la désignation de " référents/correspondants RGPD ", la documentation mise à disposition.

19. En premier lieu, s'agissant de la responsabilité du traitement, la formation restreinte estime que X est l'entité qui détermine les finalités et les moyens des traitements relatifs à la préparation des commissions de classement et, partant, est responsable des traitements en cause. En effet, la formation restreinte relève que les services centraux de X déterminent les règles générales relatives à la tenue des commissions de classement et à l'avancement et, ainsi, les finalités des traitements relatifs à la préparation des commissions de classement, qui ne sont pas propres aux différents départements qui les réalisent mais sont communes à X. Il peut être relevé à cet égard que ces traitements découlent en partie des accords collectifs négociés entre les organisations syndicales et X. Celle-ci met également à la disposition de ses différents départements les moyens qui leur permettent de réaliser les traitements relatifs aux commissions de classement, tels que l'application X. La formation restreinte souligne également que X a procédé à la notification de la violation de données en son propre nom, sans attribuer la responsabilité des traitements mis en cause dans cette notification à une autre entité et qu'elle a indiqué dans cette notification avoir agi pour mettre fin à la violation. En outre, elle note que le délégué à la protection des données de X, attaché aux services de la direction générale de X, a répondu aux

demandes des services de la CNIL, en tant que représentant de l'établissement public et non des différents départements en particulier.

20. En second lieu, la formation restreinte considère que les manquements, dont l'existence est examinée dans le cadre de la présente procédure, sont imputables à X. À cet égard, elle observe, certes, que X fait valoir que les agissements relevés ne sont pas conformes à ses règles de fonctionnement. Cependant, tout d'abord, la formation restreinte note que les fichiers en cause ne relèvent pas d'un incident isolé dans un centre de bus. Au contraire, la délégation de contrôle a pu constater que cette pratique était établie non seulement dans le centre de bus des X, visé par une plainte, mais également dans les centres de bus d'X et de X, qui n'avaient pas fait l'objet d'un signalement avant leur contrôle par la délégation.

21. Ensuite, la formation restreinte considère qu'il appartient au responsable de traitement de s'assurer de la mise en œuvre de la réglementation relative à la protection des données au sein de ses services, notamment par la mise en place de procédures adéquates et la formation du personnel. En l'espèce, il est reproché à X de ne pas avoir mis en œuvre de moyens suffisants pour prévenir de telles atteintes à la protection des données à caractère personnel de ses agents dans le cadre des traitements relatifs aux commissions de classement.

B. Sur le manquement relatif à l'obligation de veiller à l'adéquation, à la pertinence et au caractère non excessif des données à caractère personnel traitées en application des articles 5.1.c et 5.2 du RGPD

22. L'article 5, paragraphe 1, c) du RGPD prévoit que les données à caractère personnel doivent être " adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ".

23. L'article 5, paragraphe 2, du RGPD dispose : " Le responsable de traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité) ".

24. La rapporteure relève que, dans le cadre de l'instruction, la délégation de contrôle de la CNIL a constaté que la fiche de registre relative à la préparation des commissions de classement, établie en mai 2018, prévoit les catégories de données à caractère personnel qui sont considérées comme nécessaires au traitement et qui peuvent donc figurer dans les fichiers préparatoires aux commissions selon X. Ces catégories de données sont les suivantes : " les nom, prénom de l'agent, nom du responsable d'équipe ", " les matricule, date d'embauche, date de qualification ", " l'ancien niveau avec date, le niveau proposé, les gratifications éventuelles ", " la date des entretiens d'appréciation et de progrès, le cas échéant des plans de progrès ", " les critères professionnels d'évaluation ", " la présence au travail ", " les indisponibilités (sans distinction entre les motifs) ", " l'accidentologie ", " les éventuels plaintes clients, rapports d'information, sanctions ". Le responsable des ressources humaines du département BUS a en outre rappelé à l'ensemble du personnel gestionnaire des ressources humaines des centres de bus, dans un courriel adressé le 5 mai 2020, que les catégories de données à caractère personnel pouvant être contenues dans ces fichiers préparatoires étaient limitativement énumérées dans la fiche du registre correspondante et que les fichiers ne pouvaient contenir d'autres données.

25. La rapporteure note également qu'il a été constaté que la pratique de la préparation des commissions de classement dans les centres de bus contrôlés consistait à intégrer aux fichiers préparatoires, en sus du nombre de jours d'absence au cours des années évaluées, des données relatives aux motifs d'indisponibilité des agents, dont, notamment, le nombre de jours de grève par agent au cours de la période évaluée (soit trois ans).

26. Au regard de ces constatations, la rapporteure considère que la finalité du traitement que constitue la préparation des commissions de classement est l'évaluation des agents en vue de la prise de décisions relatives à leur avancement et que le traitement à cette fin de données relatives au nombre de jours de grève par agent apparaît excessif, en ce qu'elles ne constituent pas des données adéquates, pertinentes et nécessaires à l'atteinte de cette finalité.

27. En outre, la rapporteure relève que X a informé la délégation avoir procédé, pour mettre fin à la violation de données notifiée à la CNIL le 18 mai 2020 et avant les contrôles de la délégation, à la mise en conformité de tous les fichiers préparatoires établis en vue des commissions de classement des années 2019 et 2020 dans chacun des centres de bus avec la fiche correspondante du registre des activités de traitement du département BUS. La rapporteure note que les constatations ne confirment pas cette affirmation dans la mesure où le manquement perdurait à la date des contrôles sur place dans au moins deux centres de bus (X et X).

28. En défense, X ne conteste pas la constitution de fichiers contenant des données relatives au nombre de jours de grève des agents mais souligne que cette pratique est contraire à ses règles internes, que cela ne concerne que quelques unités opérationnelles et que la durée d'une telle pratique ne peut être établie. Quant à la persistance du manquement au jour des contrôles sur place, X soutient qu'il s'agit d'une erreur technique due à la mauvaise maîtrise de l'outil Excel et fournit des déclarations des directeurs des unités opérationnelles concernées attestant qu'ils ignoraient l'existence de ces onglets, qui ne pouvaient donc, a fortiori, être utilisés.

29. En premier lieu, s'agissant de la pertinence du traitement d'une donnée relative au nombre de jours de grève, la formation restreinte relève d'abord que X a fait valoir, notamment au cours des contrôles, que les règles en matière de déroulement de carrière et d'avancement étaient fixées par des accords collectifs négociés avec les organisations syndicales. Ces accords ne prévoient pas d'avancement automatique mais la prise en compte de l'évaluation des performances individuelles. X a précisé les catégories de données pouvant figurer dans les fichiers préparatoires aux commissions de classement et, parmi celles-ci, se trouvent les données relatives à la " présence au travail " et aux " indisponibilités (sans distinction entre les motifs) ". La formation restreinte relève que ces critères sont notamment traduits, dans les fichiers préparatoires en cause, par des colonnes relatives au nombre de jours de travail, au temps de " roulage ", au nombre de jours de repos et au nombre de jours d'absence. S'agissant de cette dernière colonne, il n'est pas prévu par les règles applicables qu'elle contienne le motif des absences.

30. La formation restreinte relève ainsi que le nombre de jours d'absence, au même titre que, par exemple, le nombre de jours de travail et le nombre de jours de repos, est une donnée qui peut être prise en considération dans le cadre des accords collectifs.

31. Elle relève que les accords collectifs prévoient que certaines absences, telles que l'absence liée à un congé de maternité, doivent apparaître de manière distincte afin que cette donnée ne soit pas prise en compte défavorablement dans l'évaluation de la performance de l'agent concerné. En revanche, en dehors de ces exceptions définies dans les accords, il ne ressort pas de cet ensemble de règles que les motifs d'absence des agents puissent être pris en compte pour leur évaluation.

32. Par conséquent, si la formation restreinte ne remet pas en cause la pertinence du traitement du nombre de jours d'absence au regard des règles fixées, notamment par les accords collectifs, elle estime qu'il n'est pas pertinent, en vue de l'évaluation des agents, de traiter des données relatives au nombre de jours de grève en tant que catégorie distincte du nombre total de jours d'absence. En effet, la connaissance du motif de l'absence n'est pas nécessaire. La formation restreinte relève d'ailleurs que la fiche dédiée du registre des traitements précise que, parmi les catégories de données prévues comme pouvant figurer dans ces fichiers, figurent seulement les " indisponibilités (sans distinction entre les motifs) ". Dès lors, il apparaît excessif et contraire au principe de minimisation d'individualiser la catégorie du nombre de jours de grève parmi les absences recensées et de traiter ainsi ces données pour ces finalités.

33. X n'a pas nié le caractère illicite des fichiers réalisés dans certains centres de bus dans le cadre de la préparation des commissions de classement et a fait valoir qu'une telle pratique était contraire à sa politique générale.

34. La formation restreinte considère que, dans la mesure où les fichiers en cause constituent des fichiers d'aide à la décision, ils ne peuvent être composés que des données à caractère personnel nécessaires à la prise de décisions relatives à l'évaluation, qui ont été déterminées préalablement.

35. La formation restreinte souligne enfin la spécificité des données relatives à l'exercice du droit de grève par un agent et relève que le traitement de ces données à caractère personnel n'est pas neutre. En effet, le traitement de cette catégorie particulière de données par un employeur doit être limité à certaines finalités légitimes et doit s'insérer dans le cadre légal qui résulte notamment de l'article L. 1324-7 du code des transports et de l'article R. 3243-4 du code du travail.

36. En deuxième lieu, en ce qui concerne le nombre de personnes concernées par ces traitements, la formation restreinte relève que X a rapporté, par les notifications de violation de données ainsi que les courriels subséquents adressés à la CNIL les 11 juin et 5 août 2020, l'existence de fichiers contenant des données relatives aux jours de grève dans quatre unités opérationnelles (X, X, X et X). Les contrôles de la CNIL dans deux autres unités opérationnelles, sélectionnées au hasard, ont également permis de constater l'existence de ces fichiers d'avancement. Six unités opérationnelles sur les seize existantes sont donc concernées, les autres n'ayant pas fait l'objet de contrôles. La formation restreinte relève dès lors qu'il ne s'agit pas de faits isolés.

37. En troisième lieu, s'agissant de la persistance de la pratique en cause, la formation restreinte relève que X a fait valoir lors du contrôle que, à la suite de sa découverte du fichier au centre de bus des X, elle avait procédé, les 11 et 12 mai 2020, à une analyse de tous les fichiers préparatoires établis en vue des commissions de classement des années 2019 et 2020 dans chacun des centres de bus et mis en conformité l'ensemble de ces fichiers avec la fiche correspondante du registre des activités de traitement du département BUS. La formation restreinte souligne qu'il a pourtant été constaté, lors des contrôles dans les centres de bus des X et de X, que les fichiers relatifs à l'année 2020, présentés par X comme purgés de toute donnée non nécessaire, contenaient des onglets dans lesquels se trouvaient le détail des indisponibilités des agents et notamment des données relatives aux jours de grève.

38. À cet égard, si, pour justifier que ce manquement ait perduré, X a fait valoir qu'il s'agissait d'une erreur technique et a fourni des déclarations des directeurs des unités opérationnelles concernées attestant qu'ils ignoraient l'existence de ces onglets " masqués ", qui ne pouvaient donc être utilisés, la formation restreinte estime que X ne saurait se prévaloir de sa mauvaise maîtrise répétée de l'outil Excel pour justifier la présence de certaines données dans les fichiers en cause. En

outre, même dans l'hypothèse où les directeurs des unités opérationnelles concernées auraient ignoré la présence des onglets en cause dans les fichiers concernés, cela ne remet pas en cause la matérialité du manquement constaté.

39. En dernier lieu, la formation restreinte rappelle que l'obligation de ne traiter que des données adéquates, pertinentes et nécessaires implique non seulement celle de définir les données qui doivent être traitées mais aussi de mettre en place les mesures, notamment organisationnelles, pertinentes pour veiller à ce que seules ces données nécessaires aux finalités soient effectivement traitées. Or, la formation restreinte observe que tel n'a pas été le cas en l'espèce, comme en atteste la survenance des faits en cause.

40. En effet, force est de constater que, bien que contraire à la politique générale de X, la pratique en cause ne constitue pas un acte isolé, qui n'aurait concerné qu'un petit groupe d'agents. Au contraire, tout d'abord, cette pratique résulte notamment du manque de rigueur dans la supervision de l'organisation des procédures d'avancement ainsi que des outils mis à disposition des différents départements dans ce cadre. À cet égard, en particulier, la configuration de l'outil X, qui permet seulement l'extraction de l'ensemble des données relatives à un agent ou même à l'ensemble des agents d'un centre de bus, sans qu'il soit possible de faire un tri entre les catégories de données à sélectionner pour les extraire, était susceptible de contribuer à la constitution de fichiers de commissions de classement contenant des données inadéquates au regard de la finalité poursuivie. En outre, la formation restreinte relève que certaines mesures organisationnelles, telles que celle évoquée par X au cours de la procédure afin d'éviter que de telles pratiques se reproduisent - consistant en la création d'un outil commun Excel qui doit être utilisé pour les extractions de données dans X (et les autres applications pertinentes) réalisées pour la constitution des fichiers préparatoires, afin de figer ce qu'un tableau préparatoire peut contenir en termes de données - permettent à présent d'empêcher l'émergence de telles pratiques, et auraient pu être utilement mises en œuvre avant l'engagement de la présente procédure.

41. Au vu de l'ensemble de ce qui précède, la formation restreinte considère qu'il incombait à X, en tant que responsable de traitement, de s'assurer que ne soient utilisées que des catégories de données à caractère personnel nécessaires à la prise de décisions relatives à l'évaluation pour constituer les fichiers en cause, conformément aux articles 5.1.c et 5.2 du RGPD. Partant, la X a manqué à ses obligations en incluant dans ces fichiers des données relatives au nombre de jours de grève par agent au cours de la période évaluée et en s'abstenant de s'assurer que la purge décidée à la suite de la découverte des fichiers en cause soit effectivement mise en œuvre.

42. La formation restreinte considère par conséquent que ces faits constituent un manquement aux articles 5, paragraphe 1, e), et 5, paragraphe 2, du RGPD.

C. Sur le manquement à l'obligation de définir et de respecter une durée de conservation des données à caractère personnel proportionnée à la finalité du traitement en application de l'article 5.1.e du RGPD

43. Aux termes de l'article 5.1.e du Règlement, les données à caractère personnel doivent être " conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) ".

1. S'agissant des durées de conservation des données accessibles dans l'application X

44. La rapporteure relève que la délégation a été informée que l'application X est un outil permettant de visualiser et d'extraire des données à partir de cinq applications informatiques, qui sont mises en œuvre pour le traitement et la gestion des ressources humaines du département BUS. X a indiqué que cette application a notamment pour finalité " l'exploration de données opérationnelles " (données d'exploitation, qualité de service, données relatives aux ressources humaines et économiques). En tant qu'outil de visualisation, elle ne permet pas aux utilisateurs de modifier les données dans les systèmes d'information pouvant être explorés, mais leur permet de les extraire vers des fichiers Excel.

45. La rapporteure relève également que la délégation a été informée que les données à caractère personnel contenues dans X sont conservées, en base active, pendant la durée de l'emploi de l'agent au département BUS, allongée de six ans. La rapporteure souligne que X n'a pas été en mesure de justifier cette durée de conservation des données au regard des finalités pour lesquelles elles sont traitées et considère que cette durée de conservation en base active des données dans l'outil X est ainsi excessive.

46. En défense, X fait valoir que la durée de conservation qui avait été indiquée à la délégation de contrôle, à savoir la durée de l'emploi de l'agent au département BUS, allongée de six ans, était erronée et que cette durée correspondait à la durée de conservation des données en base archive et non en base active. Dans ses écritures, X explique que la durée de conservation en base active était en fait de six ans à la date des contrôles effectués par la CNIL. Elle précise en outre que

cette durée a été considérée comme excessive au cours de travaux internes et qu'elle a été réduite à deux ans, plus l'année en cours, après les contrôles effectués par la délégation.

47. La formation restreinte prend tout d'abord acte des précisions apportées par X au cours de la procédure et notamment du fait que les données étaient conservées en base active dans X pendant six ans et non pendant la durée de l'emploi allongée de six ans.

48. La formation restreinte rappelle que la durée de conservation des données à caractère personnel doit être déterminée en fonction de la finalité poursuivie par le traitement. Lorsque cette finalité est atteinte, les données doivent en principe être supprimées, anonymisées ou faire l'objet d'un archivage intermédiaire lorsque leur conservation est nécessaire pour le respect d'obligations légales ou à des fins précontentieuses ou contentieuses.

49. En l'espèce, l'application X est un outil de visualisation de données aux fins de gestion des ressources humaines du département BUS, ayant pour finalité " l'exploration de données opérationnelles ". Elle doit permettre, entre autres, un suivi d'activité des agents. La formation restreinte relève que cette finalité, telle qu'identifiée par X, est très large et peu précise, et qu'elle ne permet pas de comprendre précisément les besoins opérationnels qui en découlent. En outre, aucun élément du dossier ne permet de déterminer quelles finalités justifieraient que les agents habilités à accéder à X puissent, en vue de les atteindre, visualiser l'ensemble de ces données relatives aux ressources humaines sur une période de six ans. Par exemple, figurent parmi ces informations les données relatives au nombre de jours de grève par agent, qui servent notamment à calculer l'assiette de la paie ainsi que des cotisations et contributions sociales. X n'établit pas pourquoi ces informations auraient vocation à être conservées dans l'application X, dès lors que le bulletin de paie est établi, pendant une durée de six ans, alors qu'une durée bien inférieure en base active serait suffisante pour l'établissement de la paie. D'autres finalités, comme la visualisation d'informations pour le suivi d'activité des agents, peuvent justifier une durée supérieure mais la nécessité de remonter sur les six années précédentes n'est pas établie.

50. La formation restreinte relève en outre que, loin d'être en mesure de justifier la durée de conservation de l'ensemble des données dans l'application X au regard des finalités de cet outil, X a au contraire fait valoir que la durée de conservation en base active de l'application X, à la date des contrôles, avait été considérée comme excessive au regard des finalités d'exploration de cette application. Cette durée a, au cours de la procédure, été réduite à deux ans plus l'année en cours, pour permettre aux managers de réaliser un suivi d'activité des agents sur une période réduite mais suffisamment significative pour voir les évolutions.

51. Par conséquent, la formation restreinte estime que la conservation des données à caractère personnel en cause pendant six ans en base active, sans qu'une approche différenciée et adaptée de conservation des données au regard des finalités précises pour lesquelles elles sont traitées soit mise en œuvre, ne permettait pas de respecter le principe de la limitation de la durée de conservation des données.

52. Au regard de l'ensemble de ces éléments, la formation restreinte considère que le manquement à l'article 5, paragraphe 1, e), du RGPD est caractérisé.

## 2. S'agissant de la durée de conservation des fichiers de préparation des commissions de classement

53. La rapporteure note que la délégation a été informée que la durée de conservation prévue des fichiers de préparation des commissions de classement était de dix-huit mois, à partir de la tenue de la commission de classement pour laquelle ils sont établis. Cette durée est prévue sur la fiche de registre correspondante, en fonction de la finalité de ce traitement (aide à la prise de décision en vue de l'évaluation des agents). Toutefois, la délégation a constaté que, dans les centres de bus d'X et de X, des fichiers de préparation des commissions de classement de 2017 étaient présents sur les serveurs.

54. Au regard de ces constatations, la rapporteure fait grief à la X de conserver les fichiers en cause pour une durée qui excède celle nécessaire au regard de la finalité du traitement et de ne pas mettre en œuvre de manière effective sa politique de durée de conservation.

55. En défense, X souligne le caractère isolé des faits.

56. La formation restreinte relève que les fichiers de préparation des commissions sont établis comme support de prise de décision de réunions préparatoires aux commissions de classement annuelles, en vue de l'évaluation des agents, et ne peuvent par conséquent être conservés que pour la durée nécessaire à la réalisation de cette finalité. La formation restreinte observe que la X a fixé leur durée de conservation à dix-huit mois après la commission de classement pour laquelle ces fichiers sont réalisés, ayant estimé qu'il s'agissait de la durée nécessaire à la finalité du traitement.

57. Or, la formation restreinte relève que la délégation de la CNIL a constaté la conservation, dans les centres de bus d'X et de X, des fichiers de préparation des commissions de classement datant de 2017, ce qui correspond à une durée de plus de trois ans après la tenue de la commission de classement concernée. La formation restreinte considère que cette conservation est excessive dans la mesure où elle dépasse la durée nécessaire à l'atteinte de la finalité poursuivie, qui est,

selon X, de dix-huit mois après la commission de classement pour laquelle ces fichiers sont réalisés. La durée de conservation prévue des fichiers de préparation des commissions de classement n'est ainsi pas mise en œuvre de manière effective puisque seuls des fichiers relatifs aux commissions de classement 2019 et 2020 auraient dû pouvoir figurer sur les serveurs à la date des contrôles. Or, l'effectivité de la mise en œuvre d'une politique de durée de conservation des données est le pendant nécessaire de sa définition et permet d'assurer que les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Cela permet par ailleurs, notamment, de réduire les risques d'usage non autorisé des données en cause, par un salarié ou par un tiers.

58. Par conséquent, la formation restreinte considère que X a méconnu ses obligations au regard de l'article 5, paragraphe 1, e), du RGPD.

D. Sur le manquement relatif à l'obligation d'assurer la sécurité des données à caractère personnel en application de l'article 32 du RGPD

1. Sur les habilitations d'accès et d'extraction des données dans X

59. L'article 32 du Règlement dispose :

" 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

[...] b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;[...] "

60. La rapporteure relève que la délégation a été informée que l'outil X permet à l'ensemble des agents habilités, quelles que soient leurs missions, d'effectuer les mêmes actions et, ainsi, non seulement de visualiser les données à caractère personnel stockées dans l'outil mais également d'extraire l'ensemble de ces données. La rapporteure estime en conséquence que la politique d'habilitation de X ne permet pas de limiter l'accès des utilisateurs aux seules données dont ils ont effectivement besoin dans le cadre de leurs fonctions, étant rappelé que l'outil X contient un volume important de données, notamment en lien avec la gestion des ressources humaines, et relatives à l'ensemble des agents des départements BUS et MRB (matériel roulant bus).

61. En défense, X soutient que le système ne peut être cloisonné et que tous les agents habilités ont besoin d'avoir accès à l'ensemble des données dans le cadre de leurs fonctions. Elle fait également valoir que l'accès transversal entre les unités opérationnelles correspond à une nécessité opérationnelle et organisationnelle et précise à cet égard que les directeurs d'unité opérationnelle ont besoin d'avoir accès aux données de toutes les unités opérationnelles en vue d'assurer la continuité du service. X soutient également être en train de mettre en œuvre un plan d'action visant à cloisonner l'accès des profils " management d'unité opérationnelle " et " assistant RH " aux seules données de l'unité opérationnelle à laquelle ils sont rattachés.

62. La formation restreinte rappelle à cet égard qu'en application de l'article 32 du RGPD, le responsable de traitement doit mettre en place des mesures appropriées pour assurer la confidentialité des données et éviter que les données soient traitées de façon illicite par le fait de personnes qui n'ont pas besoin d'en connaître. La prévention des mésusages et des violations de données peut être en partie assurée par des mesures organisationnelles, notamment en informant les utilisateurs du système d'information sur les données qu'ils sont autorisés à traiter pour leurs missions, en contrôlant l'usage qui en est fait, notamment aux moyens de journaux de connexion, et en sanctionnant disciplinairement le non-respect des règles applicables. En complément de ces mesures, la gestion des habilitations à consulter ou à utiliser un système d'information doit tendre à limiter les accès aux seules données à caractère personnel dont un utilisateur a besoin pour l'accomplissement de ses missions, notamment en définissant des profils d'habilitation dans les systèmes en séparant les tâches et les domaines de responsabilité. Il appartient donc au responsable de traitement de mettre en place, en fonction de la plus ou moins grande diversité des missions des utilisateurs, une politique de gestion des habilitations qui soit appropriée à l'importance et à la sensibilité des données traitées, ainsi qu'aux risques auxquels les personnes concernées sont exposées, en fonction des moyens dont il peut disposer.

63. À titre illustratif, la formation restreinte relève que le Guide pour l'élaboration d'une politique de sécurité de système d'information de l'Agence nationale de sécurité des systèmes d'information (publié en 2004) précise à cet égard que la définition des habilitations doit respecter le principe du besoin d'en connaître : tout acteur aura exclusivement accès aux informations dont il a besoin dans l'accomplissement de sa tâche.



64. En l'espèce, la formation restreinte relève, en premier lieu, que tous les utilisateurs de X habilités à accéder à la partie " pointage " de l'outil ont accès aux données relatives à l'ensemble des agents des départements BUS et MRB. D'une part, tous les agents habilités accèdent donc à l'ensemble des catégories de données (l'ensemble des données relatives aux ressources humaines et ainsi, notamment, des données relatives aux jours de grève ou aux arrêts-maladies) sans distinction des fonctions ou des missions des agents. D'autre part, ces agents accèdent aux données relatives aux agents de leur unité opérationnelle mais également de toutes les autres unités opérationnelles (soit plus de 16 000 personnes), sans que la nécessité de cet accès pour l'ensemble des agents ait été établie par X. Au contraire, celle-ci a expliqué dans ses observations écrites être en train de mettre en œuvre un plan d'action visant à cloisonner l'accès de certains profils aux seules données de l'unité opérationnelle à laquelle ils sont rattachés et, ainsi, à définir une politique d'habilitation plus stricte.

65. En second lieu, la formation restreinte estime que la configuration de l'outil ne permet pas d'assurer la confidentialité des données au sens de l'article 32 du RGPD dans la mesure où tous les agents habilités peuvent extraire l'ensemble des données contenues dans l'outil. En effet, la délégation a constaté que la politique d'habilitation ne permettait pas de distinguer, selon les fonctions des agents habilités, si la capacité à extraire des données à caractère personnel était nécessaire au regard de leurs fonctions.

66. Par conséquent, la formation restreinte considère que la politique d'habilitation de l'outil X ne permet pas de garantir que les personnes habilitées ont accès aux seules données strictement nécessaires à leurs fonctions. Elle estime que la politique d'habilitation devrait être plus fine et permettre la création de davantage de profils différents, relatifs aux fonctions des agents ou aux centres de bus auxquels ils sont affectés, ainsi que X prévoit à présent de le mettre en place, a fortiori compte tenu du volume de données et de la sensibilité de certaines données accessibles dans l'outil.

67. Au regard de l'ensemble de ces éléments, la formation restreinte considère que le niveau de confidentialité des données à caractère personnel contenues dans cet outil n'est pas conforme aux exigences de l'article 32 du RGPD.

## 2. Sur les habilitations d'accès aux fichiers de préparation des commissions de classement

68. La rapporteure souligne que la délégation a constaté que, au centre de bus d'X, les fichiers de préparation des commissions de classement étaient accessibles sur un serveur à tous les participants aux réunions d'arbitrage pour lesquelles ils étaient établis. Ainsi, ces fichiers préparatoires étaient accessibles, non seulement à la direction du centre et au service des ressources humaines, qui pouvaient en tout état de cause visualiser les données contenues dans ces fichiers sur X, mais également à tous les responsables d'équipe de ligne, qui ne sont pas habilités à consulter ces données dans X. Les treize responsables d'équipe de ligne avaient donc accès aux données à caractère personnel de tous les conducteurs de bus proposés à l'avancement du centre de bus (environ 800 conducteurs de bus sont affectés à ce centre de bus, dont une partie seulement est " proposable " chaque année).

69. La rapporteure considère que le fait que les fichiers préparatoires aux commissions de classement soient accessibles sur un serveur à l'ensemble des responsables d'équipes de ligne ne permet pas de garantir la confidentialité des données dans la mesure où ces fichiers contiennent de nombreuses données à caractère personnel d'agents, et notamment d'agents qui ne sont pas sous leur responsabilité.

70. En défense, X soutient que l'ensemble des managers habilités ont besoin, dans le cadre de la réunion préparatoire, d'avoir une visibilité sur les données relatives à l'ensemble des conducteurs de bus proposés d'une même unité opérationnelle, pour pouvoir procéder aux arbitrages. Elle précise que la mise à disposition de ces fichiers à l'ensemble des managers est nécessaire afin d'assurer la collégialité des décisions lors des réunions d'arbitrage en cause.

71. Au regard des dispositions de l'article 32 du RGPD précitées, la formation restreinte considère que la confidentialité des données contenues dans les fichiers préparatoires aux commissions de classement en cause en l'espèce n'est pas garantie lorsque les fichiers sont mis à disposition de l'ensemble des responsables d'équipe de ligne, sans distinction selon qu'ils s'agissent d'agents sous leur responsabilité ou non. En effet, elle relève tout d'abord que s'il est légitime pour les responsables d'équipe de ligne d'avoir accès aux données à caractère personnel des agents sous leur responsabilité en amont des commissions, en vue de se prononcer sur leur éventuel avancement, il n'apparaît pas proportionné que les données à caractère personnel de l'ensemble des conducteurs de bus du centre de bus soient à leur disposition sur un serveur.

72. La formation restreinte note ensuite que la pratique mise en cause par la rapporteure diffère de celle constatée dans les autres centres de bus contrôlés, où ces fichiers ne sont pas mis à la disposition des responsables d'équipe de ligne avant la réunion d'arbitrage, mais seulement projetés lors de ces réunions. Elle relève que cette pratique ne remet pas en cause la collégialité des décisions et, ainsi, satisfait la finalité du traitement, tout en assurant un plus haut degré de confidentialité des données. À cet égard, la formation restreinte considère que les risques associés à la perte de confidentialité des données, tels que la réutilisation de celles-ci, sont nettement moindres lorsque les données en cause sont seulement projetées, le temps d'une réunion, et non à disposition sur un serveur.

73. Par conséquent, la formation restreinte considère que la pratique constatée dans les autres centres de bus contrôlés permet de considérer que le risque associé au fait que les fichiers en cause soient accessibles sur un serveur à tous les responsables d'équipe de ligne n'est pas proportionné à la finalité recherchée, c'est-à-dire la nécessité, pour les participants aux réunions d'arbitrage, d'avoir ponctuellement connaissance de ces données afin de participer aux arbitrages.

74. Au regard de l'ensemble de ces éléments, la formation restreinte considère que les faits précités sont constitutifs d'un manquement à l'article 32 du RGPD.

#### IV. Sur les mesures correctrices et leur publicité

75. Aux termes du III de l'article 20 de la loi du 6 janvier 1978 modifiée :

" Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : [...]

7° À l'exception des cas où le traitement est mis en œuvre par l'État, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du 27 avril 2016, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83 "

76. L'article 83 du RGPD prévoit que " Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives ", avant de préciser les éléments devant être pris en compte pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de cette amende.

77. En premier lieu, sur le principe du prononcé d'une amende administrative, X soutient qu'une telle mesure n'est pas nécessaire. Elle considère notamment qu'il doit être tenu compte des circonstances de l'espèce et en particulier des mesures qu'elle a adoptées au cours de la procédure. Elle soutient également que la majorité des décisions rendues à l'encontre d'établissements publics n'étaient pas des sanctions financières alors que " les manquements semblaient concerner des faits semblables "

78. La formation restreinte rappelle qu'elle doit tenir compte, pour le prononcé d'une amende administrative, des critères précisés à l'article 83 du RGPD, tels que la nature, la gravité et la durée de la violation, les mesures prises par le responsable du traitement pour atténuer le dommage subi par les personnes concernées, le degré de coopération avec l'autorité de contrôle et les catégories de données à caractère personnel concernées par la violation.

79. La formation restreinte considère d'abord que X a fait preuve de défaillances graves en matière de protection des données à caractère personnel puisque des manquements sont constitués à des principes fondamentaux et élémentaires du RGPD que sont les principes de minimisation des données, de responsabilité, de limitation de la durée de conservation des données et de sécurité.

80. La formation restreinte relève que par le manquement au principe de minimisation des données à caractère personnel, X a fait preuve d'une négligence certaine, portant sur un principe fondamental du RGPD. En effet, des données relatives à l'exercice du droit de grève par un agent ont été rendues accessibles à des personnes qui n'avaient pas à en connaître. La formation restreinte relève que si, dans le cadre de certaines autres activités de traitement, le responsable de traitement pouvait traiter ces données, il en est autrement dans le cadre de l'évaluation des agents, pour laquelle le nombre de jours de grève par agent ne constituait pas une donnée pertinente. En outre, l'utilisation de ces données particulières, dans un contexte de prises de décisions relatives à la carrière de l'agent, peut lui être défavorable.

81. Ensuite, la formation restreinte relève que, même après avoir été informée de la violation et après avoir mené en concertation avec les organisations syndicales une procédure d'" alerte sociale ", X n'a pas pris toutes les mesures nécessaires pour assurer la mise en conformité de tous les centres de bus puisque la persistance du manquement à l'article 5.1.c) du RGPD a été constatée lors des contrôles, bien que X ait affirmé à la CNIL avoir mis en conformité l'ensemble des fichiers dans tous les centres de bus.

82. En outre, s'agissant du manquement relatif à la durée de conservation des données, la formation restreinte relève que X a déclaré, au cours du contrôle, considérer que la durée de conservation fixée était excessive, sans pour autant avoir mis

en œuvre de manière effective des mesures permettant la mise en conformité de sa politique de durée de conservation des données.

83. La formation restreinte relève également que plusieurs manquements constatés ont concerné un nombre important de personnes, à savoir environ 16 000 agents du département BUS, ce qui a conduit une organisation syndicale à saisir la CNIL.

84. Enfin, la formation restreinte relève que les mesures de mise en conformité adoptées au cours de la procédure ne concernent pas tous les manquements et n'exonèrent pas, en tout état de cause, X de sa responsabilité pour le passé.

85. En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative au regard des manquements aux articles 5-1-c), 5-1-e), 5-2 et 32 du RGPD.

86. En deuxième lieu, s'agissant du montant de l'amende, X met en avant les mesures prises pour remédier à l'ensemble des faits reprochés visés dans le rapport et son engagement à poursuivre l'ensemble de ces mesures. Elle soutient également que sa situation financière, principalement en raison de la crise sanitaire, doit être prise en considération. Enfin, elle fait valoir que le montant proposé par la rapporteure serait disproportionné au regard des précédentes décisions de la CNIL.

87. La formation restreinte rappelle que le paragraphe 3 de l'article 83 du Règlement prévoit qu'en cas de violations multiples, comme c'est le cas en l'espèce, le montant total de l'amende ne peut excéder le montant fixé pour la violation la plus grave. Dans la mesure où il est reproché à X un manquement aux articles 5-1-c), 5-1-e), 5-2 et 32 du Règlement, le montant maximum de l'amende pouvant être retenu s'élève à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

88. La formation restreinte rappelle également que les amendes administratives doivent être dissuasives mais proportionnées. Elle considère en particulier que l'activité de l'organisme et sa situation financière doivent être prises en compte pour la détermination de la sanction et notamment, en cas d'amende administrative, de son montant. Elle relève à ce titre que X fait état d'un chiffre d'affaires en 2020 s'établissant à environ [...] euros pour un résultat net de [...] euros alors que le résultat net s'élevait à [...] euros en 2019.

89. Dès lors, au regard du contexte économique causé par la crise sanitaire de la Covid-19, de ses conséquences sur la situation financière de X, de ses efforts de mise en conformité et des critères pertinents de l'article 83, paragraphe 2, du RGPD évoqués ci-avant, la formation restreinte considère que le prononcé d'une amende administrative de 400 000 euros apparaît justifié.

90. En troisième lieu, s'agissant de la publicité de la sanction, X soutient qu'une telle mesure lui causerait une atteinte disproportionnée et fait notamment valoir qu'elle nuirait à sa stratégie de relance auprès des usagers et qu'elle serait néfaste pour les relations entretenues par X avec ses agents.

91. Au regard de la pluralité des manquements relevés, de leur persistance, de leur gravité et du nombre de personnes concernées, la formation restreinte considère que la publicité de la présente décision se justifie.

#### PAR CES MOTIFS

La formation restreinte de la CNIL, après en avoir délibéré, décide de :

- prononcer à l'encontre de X une amende administrative d'un montant de 400 000 (quatre cent mille) euros au regard des manquements constitués aux articles 5-1-c), 5-1-c), 5-1-e), 5-2 et 32 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données ;

- rendre publique, sur le site de la CNIL et sur le site de Légifrance, sa délibération, qui n'identifiera plus nommément la X à l'expiration d'un délai d'un an à compter de sa publication.

Le président

Alexandre LINDEN

Cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'État dans un délai de deux mois à compter de sa notification.