Délibération SAN-2025-015 du 22 décembre 2025

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Etat juridique : En vigueur

Date de publication sur Légifrance : Mercredi 24 décembre 2025

Délibération de la formation restreinte n° SAN – 2025-015 du 22 décembre 2025 prononçant une sanction pécuniaire à l'encontre de la société NEXPUBLICA FRANCE

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Philippe-Pierre CABOURDIN, président, M. Vincent LESCLOUS, vice-président, Mmes Laurence FRANCESCHINI et Isabelle LATOURNARIE-WILLEMS et M. Didier KLING, membres,

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

Vu la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 20 et suivants ;

Vu le décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2025-1154 QPC du 8 août 2025 du Conseil constitutionnel ;

Vu la décision n° 2023-063C du 20 mars 2023 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 ;

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 du 13 mai 2025 ;

Vu le rapport de M. Fabien TARISSAN, commissaire rapporteur, du 16 juin 2025, signifié à la société NEXPUBLICA FRANCE le 17 juin 2025 ;

Vu les observations écrites de la société NEXPUBLICA FRANCE reçues le 29 juillet 2025 ;

Vu la réponse du rapporteur notifiée à la société NEXPUBLICA FRANCE le 29 août 2025 ;

Vu les observations écrites de la société NEXPUBLICA FRANCE reçues le 10 octobre 2025 ;

Vu la clôture de l'instruction notifiée à la société NEXPUBLICA FRANCE le 29 octobre 2025 ;

Vu les observations orales formulées lors de la séance de la formation restreinte du 27 novembre 2025 ;

Vu les autres pièces du dossier,

Étaient présents, lors de la séance de la formation restreinte :

- M. Fabien TARISSAN, commissaire, entendu en son rapport ;

En qualité de représentants de la société NEXPUBLICA FRANCE :

- (…)

La société NEXPUBLICA FRANCE ayant été informée de son droit de garder le silence sur les faits qui lui étaient reprochés et ayant eu la parole en dernier ;

Après en avoir délibéré, a adopté la décision suivante :

I. Faits et procédure

1. La société NEXPUBLICA FRANCE (ci-après, " la société ") est une société par actions simplifiée sise au 4-10, rue Mozart à Clichy (92110). En 2024, elle employait environ 1 000 personnes, son chiffre d'affaires était de (…) et son résultat net de (…) d'euros.

2. Depuis le 21 janvier 2025, la société n'est plus une filiale du groupe INETUM. Anciennement " INETUM SOFTWARE FRANCE ", la société a également changé de dénomination sociale par publication au bulletin officiel des annonces civiles et commerciales du 28 mars 2025, pour devenir " NEXPUBLICA FRANCE ". Les sociétés INETUM et NEXPUBLICA FRANCE sont désormais des entités juridiques séparées, poursuivant des activités économiques distinctes et n'entretenant pas de lien capitalistique.

3. La société NEXPUBLICA FRANCE poursuit les activités de conseil en systèmes et logiciels informatiques d'INETUM SOWFTWARE FRANCE. Elle développe et commercialise à ce titre un progiciel dénommé " Public CRM " (ci-après, " PCRM "), qui est un outil de gestion de la relation avec les usagers dans le domaine de l'action sociale. La première version de cet outil de gestion a été mise en production à la MDPH du département du Nord, le 24 décembre 2019.

4. Le groupement d'intérêt public (GIP) Maison Départementale pour les Personnes Handicapées (ci-après, " MDPH ") du département du Nord utilise le PCRM pour assurer son rôle de guichet unique d'information auprès des personnes en situation de handicap et de leurs familles, ainsi que l'instruction administrative et médico-sociale de toute demande de compensation du handicap. La MDPH traite par exemple les demandes de cartes de priorité, d'invalidité, de stationnement et d'allocations d'éducation pour les enfants en situation de handicap ; elle apporte un appui pour la scolarisation ou l'insertion professionnelle pour les publics relevant de ses missions ; elle oriente les personnes vers des établissements ou services médico-sociaux, ou encore traite la demande de prestation de compensation du handicap.

5. La société NEXPUBLICA FRANCE édite et héberge ainsi le PCRM qui permet à la MDPH du département du Nord d'assurer le suivi des demandes dont elle a la charge, ainsi qu'aux usagers de suivre l'avancée de leur dossier via la plateforme en ligne " portail-autonomie-usager.lenord.fr " du PCRM.

6. La société NEXPUBLICA FRANCE sous-traite l'hébergement ainsi que les habilitations des utilisateurs dans son système d'information à la société (…) qui appartient (…), certifié " hébergeur de données de santé " au sens de l'article L. 1111-8 du code de la santé publique.

7. En mai 2023, environ (…) comptes utilisateurs avaient été créés pour la MDPH du département du Nord, depuis la mise en production du progiciel (24 décembre 2019). Le baromètre établi par la Caisse nationale de solidarité pour l'autonomie indique que la MPHD du département du Nord a rendu (…) décisions et avis en 2022 et que, la même année, (…) personnes avaient au moins un droit ouvert auprès de la MDPH.

8. Les 2 et 10 novembre 2022, des usagers du portail de la MDPH ont signalé avoir accès à des documents concernant des tiers. Le 29 novembre 2022, la MDPH du département du Nord a procédé à une notification de violation de données à caractère personnel auprès de la Commission nationale de l'informatique et des libertés (ci-après " la Commission " ou la " CNIL "). Suite à des investigations permettant de préciser les caractéristiques de la violation, la MDPH a complété sa notification le 6 mars 2023.

9. Ces notifications de violation de données transmises à la CNIL font état de la survenance de deux incidents de sécurité, liés selon la MDPH à des erreurs de paramétrage par la société NEXPUBLICA FRANCE.

10. Le premier incident s'est déroulé du 26 octobre au 8 novembre 2022. La MDPH a indiqué dans sa notification de violation qu'un paramétrage erroné de la part de NEXPUBLICA FRANCE a permis à des usagers d'accéder à des données de tiers, alors qu'ils n'avaient pas droit d'en connaître. Il est indiqué dans la notification de violation que 366 personnes ont ainsi pu accéder aux données de tiers présentes dans PCRM. La société indique que parmi ces 366 personnes, seuls deux usagers ont eu la possibilité technique d'accéder aux données à caractère personnel de tiers via ces paramétrages erronés.

11. Le second incident s'est déroulé du 26 octobre au 14 novembre 2022. D'après la MDPH, cette violation était également due à une erreur de paramétrage de la part de NEXPUBLICA FRANCE et a conduit à des anomalies d'affichage de pages. Certains usagers ont ainsi eu accès, en lecture seule, aux 5 000 premiers enregistrements de la base à travers six pages web

différentes du portail. La société a indiqué que neuf personnes se sont connectées au cours de cette période et ont pu avoir accès aux données de 14 170 personnes (un enregistrement pouvant concerner plusieurs personnes).

12. Dans les deux cas, la société a été dans l'incapacité de lister les données concernées par les violations. Elle a cependant pu exclure un accès aux pièces jointes (par exemple les justificatifs d'identité ou certificats médicaux) comprises dans le PCRM.

13. En application de la décision n° 2023-063C du 20 mars 2023 de la Présidente de la Commission, une délégation de la CNIL a effectué une mission de contrôle sur place du groupe INETUM afin de vérifier le respect des dispositions 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 " ou " la loi Informatique et Libertés ") et du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 sur la protection des données (ci-après " le RGPD " ou " le Règlement ").

14. Ce contrôle sur place a donné lieu à un procès-verbal n° 2023-063/1 du 24 mai 2023.

15. Les 14 juin et 6 et 29 septembre 2023, la société a fourni des éléments complémentaires sollicités par la délégation lors du contrôle sur place.

16. Aux fins d'instruction de ces éléments, la Présidente de la Commission a, le 13 mai 2025, désigné M. Fabien TARISSAN en qualité de rapporteur sur le fondement de l'article 22 de la loi du 6 janvier 1978 modifiée.

17. Le 17 juin 2025, à l'issue de son instruction, le rapporteur a fait signifier à la société un rapport aux termes duquel il estimait que la société avait commis un manquement à l'article 32 du RGPD et proposait à la formation restreinte de prononcer à son encontre une amende administrative. Il proposait également que cette décision soit rendue publique mais qu'il ne soit plus possible d'identifier nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

18. Le 29 juillet 2025, la société a produit des observations en réponse au rapport.

19. Le 29 août 2025, la réponse du rapporteur a été notifiée à la société.

20. Le 10 octobre 2025, la société a adressé de nouvelles observations en réponse.

21. Par courrier du 29 octobre 2025, le rapporteur a, en application de l'article 40, III, du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi Informatique et Libertés, informé la société que l'instruction était close.

22. Par courrier du 3 novembre 2025, la société a été informée que le dossier était inscrit à l'ordre du jour de la séance de la formation restreinte du 27 novembre 2025.

23. Le rapporteur et la société ont présenté des observations orales lors de la séance de la formation restreinte.

II. Motifs de la décision

A. Sur le respect du droit à un procès équitable

24. La société NEXPUBLICA FRANCE estime que les conditions dans lesquelles la procédure de sanction à son encontre a été menée contreviennent à l'article 6 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CESDH) et aux articles 41 et 47 de la Charte des droits fondamentaux de l'Union européenne.

25. Elle soutient d'abord que son droit à ne pas participer à sa propre incrimination a été méconnu dans la mesure où elle a été contrainte de produire les rapports d'audits qui fondent en grande partie la caractérisation du manquement. Par ailleurs elle estime que la procédure est entachée d'irrégularités en ce que la CNIL n'a pas procédé elle-même à des constatations afin d'établir la matérialité des vulnérabilités identifiées dans les rapports d'audits précités. Enfin, la société argue qu'elle n'a pas pu présenter une défense adéquate, le périmètre des faits qui lui sont reprochés étant trop imprécis.

26. En premier lieu, la formation restreinte note que les dispositions de l'article 19 de la loi Informatique et Libertés autorisent la délégation de contrôle à " demander communication de tous documents nécessaires à l'accomplissement de leur mission ". Elle relève également qu'il ressort de la jurisprudence constante de la Cour européenne des droits de l'Homme (CEDH) que le droit de ne pas s'incriminer soi-même ne proscrit pas l'usage, dans une procédure pénale, de données que l'on peut obtenir de l'accusé en recourant à des pouvoirs coercitifs mais qui existent indépendamment de la volonté du suspect, par exemple les documents recueillis en vertu d'un mandat (Saunders c. Royaume-Uni [GC], § 68, O'Halloran et Francis c. Royaume-Uni [GC], § 47).

27. Partant, la formation restreinte estime que les rapports d'audits ont été transmis conformément aux dispositions de l'article 19 de la loi Informatique et Libertés, au même titre que les autres pièces de l'instruction, sans préjuger d'éventuels

manquements, et sans que la société contribue donc à sa propre incrimination. En vertu de la jurisprudence de la CEDH ces pièces peuvent être examinées par la formation restreinte statuant sur l'existence ou non d'un manquement et, le cas échéant, sur le bien-fondé du prononcé d'une sanction.

28. En deuxième lieu, la formation restreinte relève que la force probante des documents versés à la procédure ne saurait être remise en cause. En effet, les audits dont il est question ont été soit commandités directement par la société (audit de code automatisé), soit par le responsable de traitement (tests d'intrusion). Ainsi, il s'agit d'évaluations faisant partie intégrante de la documentation interne de la société, sur lesquelles une autorité de contrôle peut s'appuyer afin d'apprécier le respect par la société de ses obligations.

29. En ce sens, la formation restreinte souligne que les audits en question ne constituent pas des jugements de valeur que le rapporteur se serait contenté de reprendre à son compte, mais le résultat d'analyses objectives du système d'information de la société, réalisées suivant une méthodologie précise et documentée. Elle note d'ailleurs que l'objet de ces audits n'était pas de se prononcer sur la conformité ou la non-conformité de la société, cette appréciation appartenant à la formation restreinte sur la base des explications fournies par le rapporteur et la société, qui ont pu librement discuter la valeur probante de ces pièces.

30. La formation restreinte relève plus précisément que l'évaluation et l'analyse de ces pièces ont été menées par le rapporteur, lequel a mis en relation, d'une part, le risque induit par le traitement pour les personnes concernées et, d'autre part, le niveau de sécurité mis en place par la société compte tenu de ce risque. Elle observe que dans ses écritures, le rapporteur ne s'est pas simplement contenté de reprendre le contenu des audits mais qu'il s'est attaché à analyser la nature des vulnérabilités relevées, leur gravité, leur persistance ainsi que leurs risques potentiels pour les données à caractère personnel des personnes concernées. Les rapports ont également été complétés par l'ensemble des pièces transmises, par les constatations directes réalisées par la délégation de contrôle, ainsi que par les déclarations de la société retranscrites dans le procès-verbal n° 2023-063/1 du 24 mai 2023.

31. La société a pu discuter l'ensemble de ces éléments dans le cadre de la présente procédure contradictoire.

32. Partant, la formation restreinte estime que le grief tiré de l'absence de matérialité des faits reprochés doit être écarté.

33. En dernier lieu, la formation restreinte relève qu'il ressort des pièces du dossier que le périmètre du manquement reproché à la société par le rapporteur est établi avec une précision suffisante, ce dernier ayant considéré dans ses écritures qu'au regard de l'état de l'art et des caractéristiques du traitement, le niveau global de sécurité des données à caractère personnel assuré par la société était insuffisant au regard des articles 5, paragraphe 1 alinéa f) et 32 du RGPD.

34. Enfin, la formation restreinte relève que la société a pu présenter ses observations en défense dans ses deux jeux d'écriture, ainsi qu'oralement lors de la séance de formation restreinte du 27 novembre 2025. En outre, à la demande de la société, le président de la formation restreinte lui a accordé un délai de dix jours supplémentaires afin de pouvoir produire un rapport d'expertise à l'appui de ses deuxièmes observations en défense.

35. Partant, la formation estime que le rapport de sanction, complété par la réponse du rapporteur, permettaient à la société NEXPUBLICA FRANCE de comprendre la portée du manquement qui lui était reproché, et que cette dernière a été mise en mesure d'assurer sa défense de manière adéquate.

36. Au vu de l'ensemble de ce qui précède, la formation restreinte considère que le grief tiré de la méconnaissance des droits de la défense doit être écarté.

B. Sur la responsabilité de la société NEXPUBLICA FRANCE vis-à-vis du traitement en cause

37. Aux termes de l'article 4, paragraphe 8 du RGPD, le sous-traitant est " la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ".

38. Le rapporteur considère que NEXPUBLICA FRANCE est sous-traitante de la MDPH du département du Nord pour la mise en œuvre du PCRM, et qu'il lui incombe à ce titre d'assurer un niveau de sécurité adéquat de la solution qu'elle propose.

39. Si la société ne conteste pas sa qualité de sous-traitante, elle entend néanmoins limiter la portée de sa responsabilité pour la mise en œuvre du PCRM. D'une part, elle considère n'avoir qu'une autonomie limitée vis-à-vis du responsable de traitement, qui définit le niveau de sécurité attendu pour le PCRM. D'autre part, elle estime que sa responsabilité dans le déploiement du PCRM doit être relativisée. En effet, elle soutient que certaines vulnérabilités relèvent de son prestataire hébergeur (…), et que par ailleurs elle ne peut être tenue pour responsable de composantes relevant de briques technologiques dont elle n'a pas assuré la conception. Enfin, la société s'interroge sur l'engagement de sa seule responsabilité dans le cadre de la présente procédure, alors qu'il ne relève pas de la pratique habituelle de la CNIL de ne sanctionner que le sous-traitant.

40. À titre liminaire, la formation restreinte rappelle que l'opportunité d'engager une procédure de sanction relève de la seule appréciation de la Présidente de la Commission. Cette décision se fonde sur les éléments collectés lors du contrôle.

1) S'agissant de la responsabilité de NEXPUBLICA FRANCE vis-à-vis du responsable de traitement

41. Aux termes de l'article 28, paragraphe 3, a) du RGPD, " le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique [qui] prévoit, notamment, que le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement […] ".

42. L'article 32-1 du RGPD dispose : " 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 […] ".

43. Les lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, adoptées par le CEPD le 7 juillet 2021 indiquent que " le sous-traitant ne doit traiter les données que selon les instructions du responsable du traitement. Ces instructions peuvent néanmoins lui laisser une certaine marge d'appréciation quant à la manière de servir au mieux les intérêts du responsable du traitement, en permettant au sous-traitant de choisir les moyens techniques et organisationnels les plus appropriés […] " et que " le niveau de détail des instructions données par le responsable du traitement au sous-traitant concernant les mesures à mettre en œuvre dépendra des circonstances spécifiques de l'espèce. […] Dans d'autres, il peut décrire les objectifs de sécurité minimaux à atteindre, tout en demandant au sous-traitant de proposer la mise en œuvre de mesures de sécurité spécifiques ".

44. La formation restreinte relève qu'il résulte de l'article 32 du RGPD que le sous-traitant est tenu de s'assurer que le traitement automatisé de données mis en œuvre pour le compte du responsable de traitement est suffisamment sécurisé. Le caractère suffisant des mesures de sécurité s'apprécie, d'une part, au regard des caractéristiques du traitement et des risques qu'il induit et, d'autre part, en tenant compte de l'état des connaissances et du coût des mesures de sécurité nécessaires.

45. Elle considère qu'indépendamment des obligations qui pèsent en propre sur le responsable du traitement, il revient au sous-traitant de proposer et de mettre en œuvre les solutions techniques et organisationnelles adéquates en matière de sécurité des traitements.

46. En l'espèce, compte tenu de son expertise en matière de développement de solutions informatiques et de ses obligations, il revenait à la société NEXPUBLICA FRANCE de rechercher les mesures techniques et organisationnelles de nature à assurer la confidentialité des données à caractère personnel traitées.

47. C'est d'ailleurs ce qu'il ressort du cahier des clauses techniques particulières (CCTP), qui régit la relation de sous-traitance entre la MDPH du département du Nord et la société NEXPUBLICA FRANCE. La société est en charge de l'hébergement, de la maintenance en condition opérationnelle, de l'évolution logicielle et de l'assistance technique pour la solution PCRM. Le CCTP détermine à ce titre un certain nombre d'obligations qui incombent à NEXPUBLICA FRANCE pour assurer le bon fonctionnement du logiciel (par exemple, en déterminant les spécifications fonctionnelles et techniques, en réalisant des tests d'intégration, ou plus généralement en assurant des missions de maintenance éditeur).

48. La formation relève qu'en sa qualité de responsable de traitement, la MDPH conserve un contrôle sur les finalités de mise en œuvre du traitement, par exemple en définissant ses besoins ou encore en validant les devis en lien avec le PCRM. Cependant il ressort du CCTP que la société NEXPUBLICA FRANCE dispose d'une marge de manœuvre importante pour assurer la sécurité du PCRM. Il y est par exemple précisé que NEXPUBLICA FRANCE est tenue " à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art " ainsi que de mettre en place " les mesures nécessaires au respect des traitements déclarés. En particulier, [elle] assure la sécurité des données à caractère personnel qui pourraient lui être confiées par le Département du Nord ".

49. Ainsi la formation restreinte estime que, sans préjudice de la responsabilité propre du responsable de traitement, il incombe à la société NEXPUBLICA FRANCE d'assurer la sécurité des données à caractère personnel traitées dans le PCRM.

2) S'agissant de la responsabilité de NEXPUBLICA FRANCE vis-à-vis de ses sous-traitants ultérieurs

50. Aux termes de l'article 28, paragraphe 4 du RGPD, " lorsqu'un sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement [et] […] lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations. "

51. D'une part, la formation restreinte rappelle que la société NEXPUBLICA FRANCE sous-traite l'hébergement du PCRM à son sous-traitant ultérieur (…).

52. S'il ressort des dispositions de l'article 28, paragraphe 2 du RGPD, que " le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique [qui] prévoit, notamment, que le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement […] ", la formation restreinte observe qu'il ressort du CCTP que le responsable de traitement a autorisé la société NEXPUBLICA FRANCE à recruter un sous-traitant ultérieur.

53. Il ressort également du contrat de sous-traitance conclu entre (…) et NEXPUBLICA FRANCE que la société (…) assure uniquement un rôle d'hébergement des données, de mise à disposition de machines virtuelles, ainsi que de respect des modalités d'authentification, et que c'est NEXPUBLICA FRANCE qui fournit à (…) les " instructions et directives nécessaires à l'exécution des prestations ". La société (…) quant-à-elle " s'engage à ne traiter les données que sur la base et conformément aux instructions documentées du client et du donneur d'ordre [la société INETUM SOFTWARE FRANCE] ".

54. Si dans son avis 22/2024 relatif à certaines obligations découlant du recours à un ou plusieurs sous-traitant(s) ou sous-traitant(s) ultérieur(s), le CEPD précise que la décision finale de recruter un sous-traitant ultérieur et la responsabilité qui en découle, y compris en ce qui concerne la vérification du caractère suffisant des garanties fournies par le sous-traitant ultérieur, incombent au responsable du traitement, la formation restreinte relève que le CEPD indique également que " le sous-traitant initial devrait veiller à proposer des sous-traitants ultérieurs fournissant des garanties suffisantes. […] Cela est également cohérent avec le fait que, indépendamment des critères suggérés par le responsable du traitement pour sélectionner les sous-traitants supplémentaires, le sous-traitant initial demeure pleinement responsable, devant le responsable du traitement, de l'exécution des obligations des sous-traitants ultérieurs (article 28, paragraphe 4, du RGPD) ".

55. Comme la société l'indique, la responsabilité du sous-traitant devant l'autorité de contrôle n'est pas automatique pour les actes des sous-traitants ultérieurs. Cependant, en l'espèce, la formation restreinte estime que la société NEXPUBLICA FRANCE reste à titre principal responsable du respect des règles en matière de protection des données à caractère personnel par son sous-traitant ultérieur, et ce sans préjudice de la responsabilité propre de la MDPH du département du Nord. La formation restreinte note également qu'il ressort des pièces de l'instruction que NEXPUBLICA FRANCE avait, en tout état de cause, connaissance d'éventuelles failles de sécurité résultant des mesures – ou de l'absence de mesure – mises en œuvre par la société (…).

56. D'autre part, la formation restreinte relève que si la société n'a pas développé l'application PCRM dans son intégralité et qu'elle a notamment intégré une brique technologique (…) développée par la société (…), ce choix ne résulte pas d'une demande expresse du responsable de traitement. En effet, il ressort des pièces du dossier que si la MDPH du département du Nord prescrit le recours à certains logiciels spécifiques dans le CCTP, tel n'est pas le cas de la brique logicielle développée par la société (…).

57. La formation restreinte relève ainsi que le recours à (…) relève d'un choix technique de la société NEXPUBLICA FRANCE et qu'à ce titre, il lui appartient de s'assurer que cette brique logicielle est exempte de vulnérabilités, au regard des finalités, des moyens et des risques pour le traitement en cause.

58. Compte-tenu des éléments susmentionnés, la société NEXPUBLICA FRANCE ne saurait en l'espèce limiter sa responsabilité propre vis-à-vis d'acteurs tiers.

C. Sur le manquement à l'obligation d'assurer la sécurité des données à caractère personnel traitées

59. L'article 32-1 du RGPD dispose : " 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 :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;

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

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement […] ".

60. L’article 32-2 du RGPD prévoit : " Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite ".

61. Le rapporteur estime que le niveau de sécurité assuré par un responsable de traitement ou un sous-traitant doit s’apprécier au regard du risque lié à la divulgation et à l’accès non autorisé aux données contenues dans le PCRM. En l’espèce, il souligne que le traitement comporte de nombreuses données à caractère personnel, dont des catégories particulières au sens de l’article 9, paragraphe 1 du RGPD. Il considère que la société a commis un manquement à l’article 32 du RGPD en n’assurant pas un niveau de sécurité des données traitées suffisamment élevé pour le PCRM, dans le cadre de ses activités de sous-traitance pour le compte de la MDPH du département du Nord.

62. En défense, la société NEXPUBLICA FRANCE fait valoir que le rapporteur s’est contenté d’exposer la sensibilité des données traitées et les risques pour les personnes concernées afin de conclure à l’inadéquation des mesures de sécurité mises en œuvre, sans démontrer en quoi elle a manqué aux obligations – de moyens et non de résultat – prévues par l’article 32 du RGPD, ni indiquer quelles mesures elle aurait dû mettre en place.

63. Si elle reconnaît " l’existence théorique d’un risque informatique ", elle estime que ni le simple fait qu’une vulnérabilité puisse être exploitée en théorie, ni la survenance d’un incident de sécurité ne suffisent à caractériser un manquement au RGPD. Elle ajoute que les violations de données n’ont pas été causées par une défaillance structurelle du PCRM mais par des erreurs d'exploitation ponctuelles du logiciel, en rien liées aux vulnérabilités. À l’appui de ses déclarations, la société produit une évaluation externe réalisée par un expert en informatique et en droit de l’informatique, tendant à démontrer qu’elle a alloué des moyens significatifs matériels et humains au développement et à la maintenance du PCRM, dans le respect de l’état de l’art. Enfin, elle conteste les vulnérabilités relevées par le rapporteur, estimant qu’il ne tient pas compte de l’ensemble des mesures techniques mises en œuvre pour le PCRM, et qu’en tout état de cause elles ont été corrigées rapidement.

64. À titre liminaire, la formation restreinte rappelle que l’obligation de sécurité prévue par l’article 32 du RGPD est une obligation de moyens. Ainsi, tout défaut de sécurité n’entraine pas nécessairement un manquement à cette disposition. Le respect de l’obligation de moyens par un responsable de traitement ou un sous-traitant s’apprécie au regard du caractère approprié des mesures techniques et organisationnelles mises en œuvre, en tenant compte des risques et en appréciant si la nature, la teneur et la mise en œuvre de ces mesures sont adaptées à ces risques.

65. Cette analyse a été confirmée par la CJUE dans son arrêt " Natsionalna agentsia za prihodite " (14 décembre 2023, C/2024/1065, point 47), qui rappelle que l’absence de violation de données à caractère personnel ne suffit pas à démontrer l’absence de manquement, pas plus que la survenance d’une violation de données ne suffit à caractériser en elle-même l’existence d’un manquement à l’article 32 du RGPD. Des défauts de sécurité peuvent être sanctionnés en tant que tels en raison du risque qu’ils ont fait peser sur l’intégrité des données traitées. La formation restreinte sanctionne régulièrement des manquements à l’obligation de sécurité sans que ceux-ci soient nécessairement à l’origine d’une violation de données, tels qu’une politique de mot de passe insuffisamment robuste (délibération de la formation restreinte n° SAN-2018-009 du 6 septembre 2018, publiée), le stockage de mots de passe en clair (délibération de la formation restreinte n° SAN-2022-018 du 8 septembre 2022), l’absence de politique d’habilitation (délibération de la formation restreinte n° SAN-2021-019 du 29 octobre 2021, publiée) ou encore l’utilisation d’une version obsolète du protocole TLS (décision du président de la formation restreinte n° SANPS-2024-011 du 31 janvier 2024, non publiée).

66. De la même façon, un manquement à l’obligation d’assurer la sécurité des données traitées peut être caractérisé par la faiblesse généralisée d’un système d’information, ce qui a déjà sanctionné par le passé (délibération de la formation restreinte n° SAN-2023-022 du 29 décembre 2023, non publiée).

67. Sur ce point, la formation restreinte observe que l’ANSSI applique le principe de " défense en profondeur " aux systèmes d’information, qui consiste à ne pas faire reposer la sécurité " sur un élément mais sur un ensemble cohérent. Cela signifie donc qu’il ne doit en théorie pas exister de point sur lequel tout l’édifice repose ", c’est-à-dire que toute faille de sécurité potentielle d’un composant logiciel doit être compensée par au moins un second niveau de sécurité (voir le Memento sur le concept de défense en profondeur appliquée aux systèmes d’information, version 1.1 du 19 juillet 2004). La formation restreinte note que l’ANSSI fait reposer ce concept sur le postulat que " tout composant d’un système peut être défaillant ou compromis. Ce postulat, qui s’applique également aux fonctions de sécurité d’un SI [système d’information], est confirmé régulièrement par l’actualité sur les vulnérabilités de nombreux produits et logiciels " (voir la note blanche Système d'information hybride et sécurité : un retour à la réalité, 10 août 2021).

68. En l’espèce, la formation restreinte note que le PCRM comporte de nombreuses données à caractère personnel, dont des données d’identité, des données de santé, des données relatives au handicap, le numéro de sécurité sociale (NIR), ainsi que des données révélant des informations sur la situation financière, la vie personnelle et professionnelle, la vie familiale, quotidienne, scolaire ou encore professionnelle des personnes concernées. La compromission de ces données

peut avoir des conséquences graves pour les personnes (usurpation d'identité, tentative d'hameçonnage (ou phishing), falsification de documents médicaux, chantage ou message de détresse factices, risques de discriminations etc.). La formation restreinte souligne également que le cumul de ces données, qui sont susceptibles d'être agrégées et combinées, fournit des informations extrêmement précises sur de nombreux pans de la vie des personnes concernées (par exemple sur les établissements fréquentés et le type exact de suivi de la personne, son niveau d'autonomie, les aménagements et le niveau d'aide dont elle bénéficie pour sa vie quotidienne, etc.).

(i) S'agissant des constats des audits réalisés par la solution (…) sur l'application PCRM

69. Le rapporteur estime que les différents audits de code (…) réalisés sur le PCRM permettent de révéler de nombreuses vulnérabilités critiques et importantes.

70. En défense, la société NEXPUBLICA FRANCE entend limiter la portée de ces audits, car ils résultent d'analyses automatisées du code qui peuvent faire émerger des faux positifs en raison de l'absence d'une contextualisation technique. Elle souligne à ce titre que plusieurs vulnérabilités identifiées n'étaient en réalité pas exploitables. Enfin, elle ajoute avoir corrigé rapidement et indépendamment de toute intervention de la CNIL les failles identifiées par les deux audits de 2021, comme en témoignent les résultats des audits de 2023 et 2024.

71. La formation restreinte observe que les bilans (…) sont des audits de code automatisés (qui effectuent une première analyse du code source pour y détecter d'éventuelles vulnérabilités de sécurité et erreurs de programmation connues) qui nécessitent d'être interprétés afin d'en assurer la fiabilité, notamment pour éliminer les " faux-positifs ", c'est-à-dire lorsque l'outil d'analyse signale à tort qu'une règle de sécurité a été enfreinte. Elle estime néanmoins que ces audits permettent d'offrir une première analyse de la robustesse du code et de la présence ou non de vulnérabilités connues.

72. La formation restreinte observe à ce titre que le premier bilan du 14 avril 2021 a listé 199 vulnérabilités, dont 14 " critiques " et 129 " hautes " ; le deuxième bilan du 14 octobre 2021 a listé 103 vulnérabilités, dont 34 " critiques " et 65 " hautes ". La formation restreinte relève d'une part, l'augmentation du nombre de vulnérabilités " critiques " et, d'autre part, la persistance de nombreuses vulnérabilités entre les deux audits qui se sont déroulés à six mois d'intervalle. Elle considère que lorsque des vulnérabilité critiques sont identifiées, de façon certaine ou même potentielle, il revient à l'entité chargée de la sécurité de prendre rapidement des mesures afin qu'elles ne puissent être exploitées par un attaquant.

73. Elle note également la présence de 14 failles (vulnérabilités) dans le premier audit, et de 18 dans le deuxième, qui figurent dans le top 10 des catégories de risques les plus critiques en matière de sécurité des applications web listés par l'OWASP (Open Worldwide Application Security Project, qui est une communauté en ligne travaillant sur la sécurité des applications web et publie des recommandations à ce titre). L'ANSSI recommande, pour la sélection d'un logiciel libre, que ce logiciel soit conforme aux recommandations de l'OWASP.

74. Parmi les nombreuses vulnérabilités identifiées, la formation restreinte relève que plusieurs peuvent nuire à la confidentialité ou à l'intégrité des données traitées (par exemple (…)).

75. À titre d'exemple, la vulnérabilité (…).

76. Comme pour d'autres vulnérabilités, la société ne conteste pas son existence, mais soutient qu'elle ne pose pas de risque en pratique car d'autres facteurs empêchent son exploitation (en l'espèce, elle affirme (…)). Or, la formation restreinte relève que (…). Un individu connaissant la faille pouvait donc l'exploiter, et par exemple supprimer des messages entre un usager et le gestionnaire en (…). Cela démontre précisément la nécessité de disposer d'une " défense en profondeur " et de ne pas faire reposer la sécurité de tout le logiciel PCRM sur la sécurité d'un unique composant, celui-ci pouvant être contourné.

77. En outre, la formation restreinte note que le rapporteur relevait d'autres vulnérabilités identifiées par les audits faisant peser un risque critique sur la confidentialité des données traitées dans le PCRM, tels (…). La formation restreinte relève que si la société a indiqué avoir corrigé ces vulnérabilités, elle n'a pas contesté leur existence et leur degré de criticité.

78. La formation restreinte souligne que ce n'est qu'à la suite des violations de données intervenues en 2022 que la société a progressivement mobilisé ses ressources afin d'éliminer la quasi-totalité des vulnérabilités affectant le PCRM. Or, la persistance d'autant de vulnérabilités critiques durant plusieurs mois (a minima à partir du premier des rapports (…) d'avril 2021, et jusqu'à la violation de données fin 2022) met en lumière le manque d'attention portée par la société à la sécurisation des données qu'elle traite pour le compte du responsable de traitement.

79. La formation restreinte note que le bilan (…) du 14 février 2023 ne listait plus que trois vulnérabilités, dont aucune critique ou importante, et que le bilan du 12 décembre 2024 ne listait plus aucune vulnérabilité – ce qui reflète les correctifs apportés par NEXPUBLICA FRANCE à la suite des violations de données.

(ii) S'agissant des constats réalisés par les audits de la société (…)

80. Le rapporteur estime que le niveau de sécurité insuffisant du PCRM ressort également des deux audits réalisés par la société (…), qui révèlent de nombreuses vulnérabilités.

81. La société ne conteste pas les vulnérabilités mises en lumière par les deux rapports d'audits (…). Elle souligne néanmoins les avoir corrigées rapidement, et regrette que le rapporteur n'ait pas pris en compte la démarche de correction et d'amélioration continue du PCRM – ainsi qu'en atteste par exemple la baisse de criticité de la vulnérabilité relative (…).

82. La formation restreinte relève tout d'abord que c'est le responsable de traitement qui a mandaté la société (…) afin de procéder à des audits afin d'évaluer le niveau de sécurité de l'application PCRM, à la suite des violations de données. Elle relève ensuite que le premier rapport de décembre 2022 a mis en évidence " un niveau de sécurité moyen " avec des vulnérabilités importantes, dont une faille " critique " permettant à un utilisateur, en l'absence de contrôle des permissions d'accès aux ressources, de lire des documents ne lui appartenant pas.

83. La société indique sur ce point que la vulnérabilité était due à une erreur humaine et qu'elle apparaissait encore dans le test d'intrusion (…) de décembre 2022, car les correctifs déployés directement après l'incident de sécurité de novembre 2022 n'avaient pris effet qu'en janvier 2023.

84. La formation restreinte relève que le second rapport d'audit de mars 2023 faisait apparaitre que certaines vulnérabilités identifiées dans le rapport de décembre 2022 n'avaient pas été corrigées. À titre d'exemple, la formation restreinte relève une vulnérabilité liée à (…).

85. Les deux vulnérabilités précitées, qui ne constituent que des exemples parmi d'autres des vulnérabilités critiques affectant le PCRM, démontrent que la société NEXPUBLICA FRANCE n'a pas mis en place les conditions propices à garantir la confidentialité et l'intégrité des données pour le PCRM, compte tenu de ses caractéristiques rappelées au paragraphe 68.

86. La société NEXPUBLICA FRANCE indique avoir depuis corrigé les failles relevées dans les rapports (…), ce dont la formation restreinte prend acte.

(iii) S'agissant du chiffrement des données du PCRM

87. Le rapporteur estime que la société n'utilise pas les technologies à l'état de l'art pour le chiffrement des données du PCRM.

88. La société n'a pas répondu sur ce point.

89. La formation restreinte relève que l'ANSSI a indiqué dans son bulletin d'actualité CERTFR-2017-ACT-013 du 27 mars 2017 que " l'utilisation de mécanismes cryptographiques de signature reposant sur SHA-1 est à présent l'objet d'une vulnérabilité immédiatement exploitable et doit être abandonnée […] ". Des responsables de traitement ayant recours à la fonction SHA-1 ont déjà été sanctionnés par la CNIL, cette technologie n'étant plus considérée comme conforme à l'état de l'art (voir délibération de la formation restreinte n° SAN-2023-023 du 29 décembre 2023, publiée).

90. La formation restreinte rappelle qu'un hachage à l'état de l'art permet de garantir l'intégrité des données en associant à un message, à un fichier ou à un répertoire, une empreinte unique calculable et vérifiable par tous. Elle rappelle de nouveau l'importance, pour un logiciel tel que le PCRM, de détecter si un message ou une information a été modifiée. En effet il s'agit d'une plateforme d'échange avec l'administration, permettant le dépôt et le suivi des demandes de prestations sociales pour les personnes en situation de handicap.

91. La formation restreinte considère ainsi qu'en ayant recours à la fonction SHA-1 pour certaines suites cryptographiques du protocole TLS 1.2, dans le cadre (…) et alors que cette fonction présente des vulnérabilités connues depuis 2017, la société NEXPUBLICA FRANCE n'utilise pas les technologies à l'état de l'art et manque à son obligation au titre de l'article 32 du RGPD de garantir l'intégrité des données.

(iv) S'agissant des autres mesures mises en place par la société

92. La société met en avant d'autres mesures prises pour le PCRM, afin de démontrer le niveau de sécurité et la maturité du logiciel. À ce titre, elle indique par exemple avoir mis en place une authentification multifacteur dès le lancement du PCRM, soit bien avant que la CNIL n'émette une recommandation à ce sujet. Par ailleurs, elle indique avoir mis en place depuis février 2023 un système de journalisation complémentaire, permettant d'enregistrer de manière horodatée chaque action des usagers.

93. La formation restreinte prend acte de la mise en place des mesures de journalisation complémentaires afin de permettre davantage de granularité dans le suivi des activités du PCRM. Elle observe toutefois, comme le relève le rapporteur, que l'impossibilité pour la société d'indiquer quelles données ont fait l'objet des violations met en lumière une

traçabilité inefficiente des actions effectuées sur le PCRM. La formation restreinte rappelle à ce titre qu'il est recommandé de prévoir une traçabilité " active ", c'est-à-dire de formaliser un processus permettant de générer des alertes et de les traiter en cas de suspicion de comportement anormal (voir en ce sens la délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation).

94. D'autre part, la formation restreinte souligne que le rapporteur ne faisait pas grief à la société de n'avoir pas mis en place une authentification multifacteur, et qu'en tout état de cause il s'agit d'une mesure élémentaire de sécurité à mettre en œuvre, en particulier s'agissant d'un traitement comportant des données sensibles comme c'est le cas du PCRM.

95. En conclusion, la formation restreinte considère que l'absence de lignes de défense coordonnées, la multiplicité des vulnérabilités pourtant connues et leur absence de correction rapide démontrent que les mesures mises en place par la société NEXPUBLICA FRANCE n'étaient pas suffisantes afin d'assurer la sécurité des données traitées dans le PCRM.

96. La formation restreinte considère que l'expertise transmise par la société à l'appui de ses deuxièmes observations en défense ne remet pas en cause cette conclusion sur le niveau de sécurité insuffisant du PCRM. La formation restreinte relève que l'analyse détaille les étapes de développement d'un logiciel, et qu'elle explique qu'un logiciel est par nature " un produit vivant et évolutif, susceptible de comporter des anomalies, qu'il convient de corriger dans le cadre de la maintenance ". Elle conclut que ce sont de telles anomalies, lors d'une mise à jour du PCRM, qui ont conduit aux violations de données, et non pas une faiblesse de construction de cette version du logiciel.

97. La formation restreinte ne remet pas en cause le fait que le PCRM a suivi ces différentes étapes de mise en production, ni le fait que le cycle de vie d'un logiciel puisse nécessiter des correctifs et, en tout état de cause, une maintenance continue. Cependant, si l'expertise s'attache à démontrer que les incidents de sécurité étaient liés à des erreurs ponctuelles lors d'une montée de version du logiciel, la formation restreinte rappelle que ce ne sont pas les violations de données qui caractérisent le manquement, mais la faiblesse généralisée des mesures de sécurité du PCRM. L'expertise transmise n'aborde pas les vulnérabilités relevées par le rapporteur.

98. Or c'est bien le caractère évident des failles relevées, portant sur des vulnérabilités pourtant documentées par la doctrine et de l'état de l'art, ainsi que leur persistance, qui démontrent que la société NEXPUBLICA FRANCE n'a pas respecté son obligation de moyens d'assurer la sécurité des données traitées, et qui caractérisent le manquement à l'article 32 du RGPD. La formation restreinte estime qu'il ressort de l'instruction que la société NEXPUBLICA FRANCE a laissé perdurer des problèmes structurels dans son PCRM, conduisant à un niveau global de sécurité faible et à l'absence de mise en œuvre d'un système de " défense en profondeur ".

99. La formation restreinte ajoute que la spécialisation de la société dans le conseil en systèmes et logiciels informatiques rend inopérants ses arguments selon lesquels le PCRM était en phase initiale de mise en production et qu'elle avait donc des connaissances nécessairement limitées pour garantir la conformité du logiciel. En effet, si la mise en production d'un logiciel peut s'accompagner de dysfonctionnements et implique des correctifs et mises à jour réguliers – ce qui relève d'ailleurs de bonnes pratiques – une société spécialisée en développement de solutions informatiques ne saurait invoquer son manque de connaissances lorsqu'un de ses produits révèle des vulnérabilités flagrantes qu'elle a laissé perdurer plusieurs mois.

100. La formation restreinte relève que la société a apporté des correctifs à la suite des violations de données. Cependant elle rappelle que ce n'est pas l'absence de réaction de la société à la suite des incidents de sécurité qui lui est reproché, mais la mise en production du PCRM présentant de telles failles, puis l'absence de correction rapide des vulnérabilités lors de leur identification dans les différents rapports d'audits.

101. Au regard de l'ensemble de ces éléments, la formation restreinte considère que la société n'a pas mis en œuvre des moyens suffisants pour garantir un niveau de sécurité approprié des données à caractère personnel du PCRM.

102. Si la formation restreinte note que des correctifs ont été apportés suite aux violations de données déclarées, ainsi qu'en témoignent notamment les rapports d'audits les plus récents, elle estime néanmoins que le la société a manqué à ses obligations issues de l'article 32 du RGPD et que le manquement est caractérisé pour le passé.

III. Sur les mesures correctrices

103. L'article 20-IV de la loi n° 78-17 du 6 janvier 1978 modifiée prévoit que : " 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 […] saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : […]

104. 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 ".

105. L'article 83 du RGPD, tel que visé par l'article 20, paragraphe IV, de la loi Informatique et Libertés, prévoit quant à lui 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.

106. La CJUE a rappelé à cet égard que " seule une amende administrative dont le montant est déterminé en fonction de la capacité économique réelle ou matérielle de son destinataire […] est susceptible de réunir les trois conditions énoncées à l'article 83, paragraphe 1, du RGPD, à savoir d'être à la fois effective, proportionnée et dissuasive " (CJUE, grande chambre, 5 décembre 2023, C-807/21, " Deutsche Wohnen " ; CJUE, cinquième chambre, 13 février 2025, C-383/23, " Ilva A/S "),

107. L'article 22, alinéa 2 de la loi Informatique et Libertés dispose ensuite que " la formation restreinte peut rendre publiques les mesures qu'elle prend ".

A. Sur le prononcé d'une amende administrative et son montant

108. La formation restreinte rappelle qu'il convient d'examiner les critères pertinents de l'article 83 du RGPD pour décider s'il y a lieu d'imposer une amende administrative à la société et, le cas échéant, pour déterminer son montant.

1. Sur le prononcé de l'amende

109. Le rapporteur propose à la formation restreinte de prononcer à l'encontre de la société une amende administrative au regard du manquement constitué à l'article 32 du RGPD.

110. En défense, la société fait valoir que l'amende administrative proposée par le rapporteur est manifestement disproportionnée au regard des critères de l'article 83 du RGPD et qu'un rappel à l'ordre serait une mesure correctrice plus appropriée. Elle soutient d'abord que le manquement constaté ne présente aucun caractère de gravité, notamment car le PCRM n'est déployé qu'auprès de deux clients, que les vulnérabilités étaient limitées dans le temps, et que le rapporteur surestime le nombre de personnes et la sensibilité des données concernées par les violations. L'absence de préjudice se manifeste notamment par le fait qu'aucune plainte de personne concernée n'a été enregistrée. En outre, elle conteste toute négligence, soulignant qu'elle n'a jamais été sanctionnée par la formation restreinte auparavant. Sa bonne foi se matérialise selon elle notamment par sa pleine coopération avec les services de la CNIL ainsi que par la rapidité avec laquelle elle a apporté les mesures correctives nécessaires. Enfin, la société demande à la formation restreinte de tenir compte de son autonomie limitée dans la mise en œuvre du traitement, tant vis-à-vis du responsable de traitement, la MDPH, que du sous-traitant ultérieur, la société (…).

111. À titre liminaire, la formation restreinte rappelle que, pour évaluer l'opportunité de prononcer une amende, elle doit tenir compte des critères précisés à l'article 83 du RGPD tels que la nature, la gravité et la durée de la violation, la portée ou la finalité du traitement concerné, le nombre de personnes concernées, les mesures prises par le responsable du traitement pour atténuer le dommage subi par les personnes concernées, le fait que la violation ait été commise par négligence, le degré de coopération avec l'autorité de contrôle, les catégories de données concernées et le niveau de dommage subi par les personnes.

112. En premier lieu, la formation restreinte considère qu'il y a lieu de faire application du critère prévu à l'article 83, paragraphe 2, a) du RGPD relatif à la nature, à la gravité et à la durée de la violation, compte tenu de la nature, de la portée ou de la finalité des traitements concernés ainsi que du nombre de personnes concernées.

113. La formation restreinte considère que le manquement constaté est grave et que la méconnaissance de l'état de l'art et de principes élémentaires en matière de sécurité ont fait courir un risque pour la sécurité des données à caractère personnel des personnes concernées. S'ajoute à la gravité du manquement le fait que le traitement concerne en majorité des personnes vulnérables au sens des Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est " susceptible d'engendrer un risque élevé " aux fins du règlement (UE) 2016/679. Cette vulnérabilité se traduit, entre autres, par le déséquilibre flagrant entre la société et les personnes concernées, celles-ci n'ayant pas d'autre choix que de voir leurs données traitées par le PCRM si elles souhaitent bénéficier de certaines prestations.

114. La formation restreinte relève en outre que le PCRM comptait (…) comptes utilisateurs en mai 2023 et la MDPH du département du Nord traite environ (…) dossiers actifs par an. Par ailleurs la société a indiqué que les violations ont potentiellement concerné deux personnes pour la première et 14 170 pour la deuxième, ce qui représente environ (…) % des usagers et un nombre approximatif de (…) enregistrements.

115. Le fait qu'aucune intrusion de tiers au PCRM n'a été détectée, et que les données n'ont été rendues accessibles qu'en lecture seule, n'en atténue pas la gravité. En effet, il n'en résulte pas moins que les données ont été rendues accessibles à des tiers non autorisés et des données affichées, même en lecture seule, peuvent toujours être copiées.

116. En deuxième lieu, la formation restreinte estime qu'il convient de tenir compte du critère prévu à l'article 83, paragraphe 2, b) du RGPD, relatif au fait que la violation ait été commise délibérément ou par négligence.

117. La formation restreinte considère que le manquement résulte d'une négligence de la part de la société NEXPUBLICA FRANCE, qui n'a pas pris en compte l'état de l'art dans la mise en œuvre de mesures techniques et organisationnelles pour le PCRM – et ce surtout alors que le conseil en systèmes et logiciels informatiques est son cœur d'activité. Ce n'est qu'après la survenance des violations de données en octobre 2022, puis l'intervention du responsable de traitement qui a diligenté des tests d'intrusion, que la société a apporté des correctifs à certaines des vulnérabilités constatées – alors même que la réalisation d'audits par la société mettait en évidence des vulnérabilités critiques dès 2021. Comme indiqué au II.C. de la présente délibération et contrairement à ce qu'affirme la société, elle n'a pas apporté la preuve de la correction de toutes les vulnérabilités dès qu'elles ont été portées à sa connaissance et avant le contrôle réalisé par la CNIL.

118. En troisième lieu, la formation restreinte considère qu'il y a lieu de tenir compte, en application de l'article 83, paragraphe 2, d) du RGPD, du degré de responsabilité du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'il a mises en œuvre en vertu des articles 25 et 32 du RGPD.

119. Or, comme démontré au point II.B., la formation restreinte estime que la société NEXPUBLICA FRANCE ne saurait se défaire de ses responsabilités de mise en œuvre de mesures techniques et organisationnelles adaptées pour le PCRM.

120. En quatrième lieu, la formation restreinte entend tenir compte des catégories de données à caractère personnel concernées par le manquement, en application de l'article 83, paragraphe 2, g) du RGPD.

121. La formation restreinte rappelle que le traitement en cause comporte des données relatives à la santé, et notamment au handicap, qui sont des catégories particulières de données au sens de l'article 9 du RGPD, dites données " sensibles ". La formation restreinte souligne que bien qu'il ne soit pas rapporté que des documents médicaux aient été compromis, il n'en demeure pas moins que les lacunes en termes de sécurité ont fait peser un risque certain sur la confidentialité de ces données " sensibles ".

122. Par ailleurs les données effectivement compromises, relatives aux descriptifs des prestations rattachées aux dossiers des usagers, donnent de nombreuses indications sur l'identité et les situations personnelles des personnes concernées, y compris des données de mineurs. La formation restreinte ajoute que le simple fait de figurer dans le traitement et de percevoir des prestations permet de déduire que la personne est en situation de handicap.

123. Enfin, c'est aussi le cumul de toutes les données traitées qui permet de fournir des indications précises et complètes sur la quasi-totalité des aspects de la vie intime et privée des personnes concernées et de leurs proches.

124. Au regard de l'ensemble de ces éléments, la formation restreinte considère que le prononcé d'une amende apparait justifié.

2. Sur le montant de l'amende

125. En défense, la société considère que le montant de l'amende proposée par le rapporteur est disproportionné au regard de son chiffre d'affaires, des décisions récentes de la formation restreinte, ainsi que (…). De plus et par analogie avec les règles du droit de la concurrence, elle estime que la part du chiffre d'affaires lié au PCRM dans son chiffre d'affaires global devrait être prise en compte dans la détermination du montant de l'amende, en lieu et place de son chiffre d'affaires global.

126. La formation restreinte rappelle tout d'abord que l'article 83 du RGPD, pour déterminer le montant de l'amende, fait référence à un montant (jusqu'à 10 000 000 d'euros) ou, dans le cas d'une entreprise, à un pourcentage du chiffre d'affaires annuel (jusqu'à 2%), le montant le plus élevé étant retenu. Elle rappelle que les amendes administratives doivent être dissuasives et proportionnées.

127. S'agissant de la comparaison avec des amendes prononcées dans d'autres procédures, la société ne peut utilement comparer sa situation à celles d'autres entreprises ayant été sanctionnées pour des manquements prétendument similaires, dans la mesure où le montant d'une amende doit être déterminé au cas par cas. Le Conseil d'État a en ce sens considéré que " la circonstance que des amendes d'un montant plus faible, en proportion de leur chiffre d'affaires mondial, auraient été prononcées par la formation restreinte de la CNIL à l'encontre d'autres sociétés est sans incidence sur la proportionnalité de la sanction infligée à la société requérante " (CE, 10ème et 9ème chambre réunie, 14 mai 2024, société VOODOO, n° 472221).

128. Par ailleurs la formation restreinte rappelle que si des éléments tels que les bénéfices et pertes réalisés par la société, ou encore le chiffre d'affaires généré spécifiquement par le PCRM, peuvent être pris en compte au titre de l'évaluation des critères de l'article 83 du RGPD, ils ne peuvent se substituer au chiffre d'affaires de la société qui reste le seul élément de détermination du plafond de l'amende maximale encourue. La CJUE a estimé que " seule une amende administrative dont le montant est déterminé en fonction de la capacité économique réelle ou matérielle de son destinataire […] est susceptible de réunir les trois conditions énoncées à l'article 83, paragraphe 1, du RGPD, à savoir d'être à la fois effective, proportionnée et dissuasive " (" Deutsche Wohnen " et " Ilva A/S " précités). Ainsi la formation restreinte estime que le droit applicable ne lui impose pas de se limiter au chiffre d'affaires du produit en cause – en l'espèce le PCRM – pour déterminer le montant maximal de l'amende encourue.

129. Enfin, la formation restreinte estime que (…) – en l'espèce des courriers non publics échangés dans le cadre d'instructions avec des tiers – ne sauraient utilement être invoqués. En effet la formation restreinte ne prend en considération, afin de déterminer le montant de l'amende, que le manquement constaté en lien avec le PCRM dans la présente procédure.

130. Compte tenu de ce qui précède, la formation restreinte considère qu'il y a lieu de retenir le chiffre d'affaire de l'entreprise. Elle rappelle qu'en 2024, la société NEXPUBLICA FRANCE a réalisé un chiffre d'affaire de (…) d'euros, pour un résultat net de (…) d'euros.

131. Dès lors, au regard de la responsabilité de la société NEXPUBLICA FRANCE, de ses capacités financières et des critères pertinents de l'article 83, paragraphe 2 du RGPD évoqués ci-avant, la formation restreinte estime qu'une amende administrative d'un montant d'un million sept-cent mille euros (1 700 000 €), au regard du manquement constitué à l'article 32 du RGPD, apparaît justifiée.

B. Sur la publicité de la sanction

132. La société conteste la proposition du rapporteur de rendre publique la présente délibération, estimant cette mesure non nécessaire étant donné que les manquements sont désormais corrigés. Elle estime que (…). La publicité de la décision porterait une atteinte grave et immédiate à son image alors qu'elle vient de prendre son autonomie juridique et organisationnelle.

133. La formation restreinte considère que (…). Par ailleurs si la société a changé de dénomination sociale, la formation restreinte relève qu'elle continue à éditer et héberger le PCRM pour la MDPH du département du Nord, dans la continuité des activités d'INETUM SOFTWARE FRANCE. Ainsi la publicité se justifie au regard de la gravité avérée du manquement en cause, de la sensibilité du traitement, de la négligence dont a fait preuve la société ainsi que du nombre de personnes concernées, lesquelles se doivent d'être informées.

134. Elle estime que cette mesure apparait proportionnée dès lors que la décision n'identifiera plus nommément la société à l'issue d'un délai de deux ans à compter de sa publication.

PAR CES MOTIFS

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

- de prononcer à l'encontre de la société NEXPUBLICA FRANCE, une amende administrative d'un montant d'un million sept-cent mille euros (1 700 000 €) au regard du manquement à l'article 32 du RGPD ;

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

Le Président

Philippe-Pierre CABOURDIN

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