Délibération SAN-2021-020 du 28 décembre 2021

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Etat juridique : En vigueur

Date de publication sur Légifrance : Jeudi 30 décembre 2021

Délibération de la formation restreinte n°SAN-2021-020 du 28 décembre 2021 concernant la société SLIMPAY

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, Monsieur Bertrand du MARAIS et Monsieur Alain DRU, 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 n° 78-17 du 6 janvier 1978 modifiée 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° 2020-107C de la présidente de la CNIL du 12 mai 2020 de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification auprès de la société SLIMPAY ;

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 avril 2021 ;

Vu le rapport de Madame Valérie PEUGEOT, commissaire rapporteure, notifié à la société SLIMPAY le 23 juin 2021 ;

Vu les observations écrites versées par la société SLIMPAY le 23 juillet 2021 ;

Vu les observations orales formulées lors de la séance de la formation restreinte ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 16 septembre 2021 :

- Madame Valérie PEUGEOT, commissaire, entendue en son rapport ;

En qualité de représentants de la société SLIMPAY :

- […] ;

La société SLIMPAY ayant eu la parole en dernier ;

Après en avoir délibéré, la formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. La société SLIMPAY (ci-après la " société ") est une société anonyme, immatriculée au registre du commerce et des sociétés de Paris, qui a pour activité le conseil en systèmes et logiciels informatiques. Son effectif est de 83 salariés.

2. La société est un établissement de paiement agréé, qui propose des services de paiements récurrents dans l'espace unique de paiement en euros (" Single Euro Payments Area " – SEPA). Elle propose à ses clients, les " marchands " qui sont des personnes morales, des solutions de gestion des abonnements et des paiements récurrents.

3. Dans le cadre des services fournis par la société à ses marchands, les données à caractère personnel traitées sont celles des débiteurs personnes physiques des marchands. Au 1er septembre 2020, la société SLIMPAY comptait […] débiteurs personnes physiques des marchands au sein de ses bases de données.

4. En 2019, la société a réalisé un chiffre d'affaires de […] euros et présentait un résultat net s'élevant à […] euros. En 2020, son chiffre d'affaires s'élevait à […] euros et elle présentait un résultat net de […] euros. La société a par ailleurs réalisé une levée de fonds de […] euros en 2015.

5. Dans le courant de l'été 2015, à l'occasion d'un projet de recherche interne sur un mécanisme de lutte contre la fraude, la société a réutilisé des données à caractère personnel contenues dans ses bases de données à des fins de test. Elle a ainsi importé des données à caractère personnel de débiteurs sur un serveur. Lorsque le projet de recherche s'est terminé en juillet 2016, les données sont restées stockées sur ce serveur, qui ne faisait pas l'objet d'une procédure de sécurité particulière et qui était librement accessible depuis Internet.

6. Le 14 février 2020, un des marchands client de la société lui a fait part de ces éléments. La société SLIMPAY a alors immédiatement procédé à l'isolement du serveur et à la mise sous séquestre des données, en vue de mettre fin à la violation de données à caractère personnel.

7. Le 17 février 2020, la société a notifié la violation de données à la Commission nationale de l'informatique et des libertés (ci-après la " Commission " ou la " CNIL ").

8. Le 26 février 2020, la société a effectué une notification complémentaire de violation de données à la CNIL, donnant davantage de précisions sur l'incident de sécurité, notamment sur les mesures mises en œuvre par la société, le nombre de personnes et le type de données à caractère personnel concernés par la violation de données.

9. Les données des débiteurs de […] marchands, correspondant à environ douze millions de débiteurs uniques, ont été concernées par cette violation. Les données à caractère personnel concernées par la violation sont des données d'état civil (civilité, nom, prénom), des coordonnées postales, électroniques et téléphoniques, et des informations bancaires (" Bank Identifier Code " - BIC/ " International Bank Account Number " - IBAN).

10. Les éléments transmis par la société ayant permis d'établir le caractère transfrontalier du traitement concerné, la CNIL a informé le 27 février 2020, conformément à l'article 56 du RGPD, l'ensemble des autorités de contrôle européennes de sa compétence pour agir en tant qu'autorité de contrôle chef de file et a ainsi ouvert la procédure pour la déclaration des autorités concernées sur ce cas.

11. En application de la décision n° 2020-107C de la présidente de la Commission du 12 mai 2020, la CNIL a effectué une mission de contrôle sur pièces auprès de la société, afin de vérifier le respect par cette dernière de l'ensemble 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 " loi Informatique et Libertés ") et du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le " RGPD "). Cette mission s'est effectuée par l'envoi d'un questionnaire à la société, adressé par lettre recommandée avec accusé de réception le 31 juillet 2020.

12. Par courriel du 5 août 2020, la déléguée à la protection des données de la société a sollicité un délai supplémentaire auprès de la délégation de la CNIL.

13. Par courriel du 6 août 2020, un délai supplémentaire a été accordée à la société jusqu'au 11 septembre 2020.

14. Le 11 septembre 2020, la société a transmis des éléments de réponse à la CNIL, par voie dématérialisée sécurisée.

15. Par courriels des 21 octobre et 2 décembre 2020, la délégation de la CNIL a sollicité des éléments complémentaires auprès de la société, notamment afin de savoir si la société avait procédé à une communication publique ou à une autre action similaire pour informer les personnes concernées par la violation de données et si le travail de recherche et développement sur lequel elle travaillait dans le cadre de la lutte contre la fraude imposait l'utilisation de données réelles non anonymisées. Ces éléments ont été transmis respectivement le 29 octobre et le 10 décembre 2020.

16. Aux fins d'instruction de ce dossier, la présidente de la Commission a, le 12 avril 2021, désigné Madame Valérie PEUGEOT en qualité de rapporteure sur le fondement de l'article 39 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi du 6 janvier 1978 modifiée.

17. À l'issue de son instruction, la rapporteure a, le 23 juin 2021, fait notifier à la société SLIMPAY un rapport détaillant les manquements au RGPD qu'elle estimait constitués en l'espèce. Un courrier lui était également remis, l'informant que le dossier était inscrit à l'ordre du jour de la formation restreinte du 16 septembre 2021.

18. Ce rapport proposait à la formation restreinte de la Commission de prononcer à l'encontre de la société une amende administrative, au regard des manquements constitués aux articles 28 paragraphes 3 et 4, 32 et 34 du RGPD. Il proposait également que la décision de sanction 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.

19. Le 23 juillet 2021, la société a produit des observations en réponse.

20. La société et la rapporteure ont présenté des observations orales lors de la séance du 16 septembre 2021.

II. Motifs de la décision

21. Aux termes de l'article 56 paragraphe 1 du Règlement, " l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant, conformément à la procédure prévue à l'article 60 ".

22. En l'espèce, la formation restreinte relève que le siège social de la société, établissement unique de la société SLIMPAY, se trouve en France et qu'elle est immatriculée au registre du commerce et des sociétés en France depuis l'origine, ce qui

conduit à faire de la CNIL l'autorité de contrôle chef de file compétente concernant les traitements transfrontaliers effectués par cette société, conformément à l'article 56 paragraphe 1 du Règlement.

23. Faisant application du mécanisme de coopération et de cohérence prévu au chapitre VII du RGPD, la CNIL a informé, le 27 février 2020, l'ensemble des autorités de contrôle européennes de sa compétence pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par la société, ouvrant ainsi la procédure pour la déclaration des autorités concernées sur ce cas. Les autorités de contrôle des pays suivants se sont déclarées concernées par la présente procédure : Allemagne, Espagne, Italie et Pays-Bas.

24. En application de l'article 60, paragraphe 3, du RGPD, le projet de décision adopté par la formation restreinte a été transmis à ces autorités de contrôle le 25 novembre 2021.

25. Au 24 décembre 2021, aucune des autorités de contrôle concernées n'avait formulé d'objection pertinente et motivée à l'égard de ce projet de décision, de sorte que, en application de l'article 60, paragraphe 6, du RGPD, ces dernières sont réputées l'avoir approuvé.

A. Sur le statut de la société en termes de responsabilité de traitement

26. Aux termes de l'article 4 du RGPD, le responsable de traitement est défini 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 " (point 7) et 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 " (point 8).

27. L'article 28-10 du RGPD prévoit quant à lui que " sans préjudice des articles 82, 83 et 84, si, en violation du présent règlement, un sous-traitant détermine les finalités et les moyens du traitement, il est considéré comme un responsable du traitement pour ce qui concerne ce traitement ".

28. La rapporteure relève que la société SLIMPAY agit en qualité de responsable du traitement concerné par la violation de données et en tant que sous-traitant pour les traitements mis en œuvre dans le cadre des services fournis aux marchands, responsables de traitement.

29. En défense, la société ne conteste pas l'analyse de la rapporteure sur ce point.

30. La formation restreinte considère que la notion de responsable de traitement doit faire l'objet d'une appréciation concrète prenant en compte l'ensemble des éléments permettant d'attribuer cette qualité à une entité. À ce titre, elle relève qu'il ressort des éléments communiqués à la CNIL que la société SLIMPAY agit en qualité de sous-traitant pour les traitements mis en œuvre dans le cadre des services fournis aux marchands, responsables de traitement, dans la mesure où la société ne détermine pas les finalités de traitement des données. Ces services constituent l'essentiel de son activité (services de paiements récurrents, mandats SEPA, etc.).

31. La formation restreinte relève également que la société fait elle-même appel, dans le cadre des services fournis aux marchands, aux services de sous-traitants. Ainsi que l'indique la société, les sous-traitants de SLIMPAY sont donc des sous-traitants de second niveau vis-à-vis des marchands.

32. La formation restreinte considère par ailleurs que la société SLIMPAY agissait en qualité de responsable du traitement concerné par la violation de données, celui-ci étant un traitement de recherche interne concernant un mécanisme de lutte contre la fraude, dont elle a déterminé seule les finalités et les moyens. La société indique d'ailleurs elle-même agir en tant que responsable de traitement, dans la notification complémentaire de violation de données qu'elle a transmise à la CNIL le 26 février 2020.

33. Il appartient dès lors à la formation restreinte d'examiner, au regard de ces qualités, les griefs formulés par la rapporteure à l'encontre de la société.

B. Sur la caractérisation des manquements au regard du RGPD

34. À titre liminaire, la formation restreinte relève que, en défense, la société conteste le fait que des manquements sans lien avec la violation de données à caractère personnel puissent être retenus, alors que celle-ci est à l'origine de la procédure.

35. La formation restreinte considère que le fait que les investigations de la CNIL aient été initialement motivées par la survenance de la violation de données, à la suite de sa notification, est sans incidence sur la possibilité de constater l'existence d'autres manquements au RGPD au regard des faits constatés dans le cadre des investigations menées par la délégation de contrôle de la CNIL.

36. En effet, il résulte de l'article 8 de la loi Informatique et Libertés que la CNIL, d'une part, peut procéder à des vérifications portant sur tous traitements et, le cas échéant, obtenir des copies de tous documents ou supports d'information utiles à ses missions, d'autre part, doit veiller à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de ladite loi et aux autres dispositions relatives à la protection des données à caractère personnel prévues par les textes législatifs et réglementaires, le droit de l'Union européenne et les engagements internationaux de la France.

37. Dans ce cadre, et en application de l'article 20 de la loi Informatique et Libertés, la formation restreinte prend les mesures et prononce les sanctions à l'encontre des responsables de traitement ou des sous-traitants qui ne respectent pas les obligations découlant du RGPD et de ladite loi.

1. Sur le manquement à l'obligation d'encadrer par un acte juridique formalisé les traitements effectués par un sous-traitant ultérieur

38. Aux termes de l'article 28 paragraphe 3 du RGPD, " Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement. Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant :

a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis ; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;

b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;

c) prend toutes les mesures requises en vertu de l'article 32 ;

d) respecte les conditions visées aux paragraphes 2 et 4 pour recruter un autre sous-traitant ; […] ".

39. En application du paragraphe 4 de ce même article, lorsqu'un sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection de données que celles fixées dans le contrat entre le responsable du traitement et le sous-traitant sont imposées à cet autre sous-traitant par un contrat ou au moyen d'un autre acte juridique, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement. 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.

40. Dans le cadre des investigations menées par la CNIL, la société SLIMPAY a indiqué recourir à […] sous-traitants agissant sous son autorité en tant que sous-traitants de second niveau vis-à-vis des marchands, pour les services qu'elle fournit à ces derniers (services de paiements récurrents, mandats SEPA, etc.). La société a également précisé adresser à ces sous-traitants un " questionnaire relatif à la sous-traitance " afin de se conformer au RGPD. Sur ledit questionnaire, il est indiqué : " en sa qualité de prestataire de services de paiement, SlimPay est déterminée à respecter les dispositions du règlement sur la protection des données à caractère personnel (règlement (UE) 2016/679). A cette fin, nous devons nous assurer que le traitement des données effectué par nos partenaires est conforme aux exigences légales. ".

41. La rapporteure a considéré que les démarches effectuées par la société auprès de ses sous-traitants par le biais de ces questionnaires n'étaient pas suffisantes pour satisfaire à ses obligations et s'assurer que les sous-traitants ultérieurs présentent les garanties suffisantes requises. Elle a en outre relevé que les contrats et avenants conclus avec trois sociétés ne contenaient pas l'ensemble des clauses prévues par l'article 28 paragraphe 3 du RGPD et que ceux conclus avec trois autres sociétés ne comportaient aucune des mentions obligatoires prévues par ce même article.

42. En défense, la société explique mettre en œuvre des mesures concrètes pour assurer sa conformité à la réglementation relative à la protection des données dans le cadre d'une démarche continue, non seulement en s'appuyant sur la documentation de conformité fournie par ses sous-traitants, lesquels proposent des engagements contractuels standards, mais aussi par le biais de questionnaires ponctuels. Elle précise que les questionnaires communiqués lors du contrôle de la CNIL n'avaient pour objectif que de justifier des vérifications opérées par SLIMPAY auprès de ses sous-traitants, ajoutant que, faute pour lesdits sous-traitants de fournir une documentation contractuelle encadrant les garanties en matière de protection des données, il est prévu de leur soumettre un tel accord. La société SLIMPAY fait également état des négociations en cours avec certaines sociétés sur la signature d'avenants relatifs à la protection des données personnelles.

43. En premier lieu, la formation restreinte relève que la société n'a pas apporté la preuve que le questionnaire évoqué est complété par les sous-traitants ultérieurs. En tout état de cause, quand bien même il le serait, la formation restreinte souligne que ledit questionnaire n'a qu'une valeur déclarative et qu'il ne constitue pas un acte juridique contraignant par lequel le sous-traitant ultérieur s'engage à respecter les éléments définis. L'envoi de ce questionnaire ne permet donc pas de répondre aux obligations posées à l'article 28 paragraphes 3 et 4.

44. En deuxième lieu, la formation restreinte relève que certains des contrats conclus par la société avec ses sous-traitants ne contiennent pas l'ensemble des clauses prévues par l'article 28 paragraphe 3 du RGPD. En ce sens, elle note que les contrats et avenants conclus avec […] ne précisent pas l'ensemble des mentions obligatoires au titre de l'article 28 du RGPD, dont notamment le type de données concernées ainsi que les obligations et droits du responsable de traitement. De même, dans le contrat et les avenants conclus avec […] - le type de données ainsi que les obligations et droits du responsable de traitement ne sont pas mentionnés.

45. La formation restreinte relève en outre que les contrats et avenants conclus avec les sociétés […] ne contiennent aucune des mentions obligatoires prévues par l'article 28 du RGPD.

46. En troisième lieu, la formation restreinte note que la société SLIMPAY a fourni, dans le cadre de la procédure de sanction, un exemple d'avenant " protection des données personnelles " conclu avec la société […] en juillet 2021 et qu'elle a précisé que des négociations sont en cours avec les sociétés […]. La formation restreinte prend acte de la mise en conformité partielle dans le cadre de la présente procédure. Il n'en demeure pas moins que le fait que la société ait entamé des démarches auprès des sous-traitants dans le cadre de la présente procédure démontre bien qu'elle n'était pas en conformité au moment des investigations menées par la CNIL.

47. Elle ne l'est d'ailleurs toujours pas s'agissant de certains contrats, continuant ainsi à méconnaître l'obligation d'encadrer par un acte juridique formalisé les traitements effectués par un sous-traitant ultérieur.

48. Dès lors, au regard de l'ensemble de ces éléments, la formation restreinte considère que le manquement à l'article 28 paragraphes 3 et 4 du RGPD est caractérisé.

2. Sur le manquement à l'obligation d'assurer la sécurité des données

49. Aux termes de l'article 32 du RGPD, " 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 :

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.

2. 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 […] ".

a) Sur le défaut de sécurité ayant entraîné la violation de données à caractère personnel

- Sur la caractérisation du manquement

50. La rapporteure relève qu'il ressort des éléments communiqués à la CNIL que, dans le cadre d'un projet de recherche mené en 2015, SLIMPAY a réutilisé des données à caractère personnel de débiteurs aux fins de test d'un dispositif de lutte contre la fraude. Le projet s'est terminé l'année suivante, en juillet 2016, mais les données sont restées hébergées sur un serveur ne faisant l'objet d'aucune mesure de sécurité particulière. Le 14 février 2020, la société a été avertie par un de ses clients de la possibilité d'accéder librement à ces données depuis Internet au moyen d'une URL simplement composée d'une adresse IP et d'un port de communication, sans autre restriction d'accès ou mesure de sécurité. La société a, le soir-même, procédé à l'isolement du serveur contenant les données à caractère personnel concernées.

51. Selon la rapporteure, le manquement commis par la société quant à son obligation de sécurité a ainsi débuté en 2015, lorsque les données des clients des marchands ont été importées sur un serveur ne faisant l'objet d'aucune mesure de sécurité, et il a perduré puisqu'il n'a pris fin qu'en février 2020, après que la société a été alertée par l'un de ses clients. Elle considère, dès lors qu'il s'agit d'un manquement continu, qu'il convient de sanctionner sous l'angle du RGPD et qu'une telle analyse a été récemment confortée par le Conseil d'État dans sa décision du 1er mars 2021 concernant la société Futura Internationale.

52. S'agissant des faits constitutifs du manquement, la rapporteure souligne que l'accès au serveur en question n'était encadré d'aucune mesure de restriction d'accès satisfaisante et que la société n'avait mis en place aucune mesure de journalisation des accès au serveur.

53. En défense, la société SLIMPAY conteste l'analyse de la rapporteure selon laquelle le principe de non-rétroactivité de la sanction pénale plus sévère ne saurait s'appliquer aux manquements qui continuent à produire des effets dans le temps, au point que même débutés sous l'empire de la loi Informatique et Libertés, ils persistent sous l'égide du RGPD et doivent dès lors être qualifiés de continus et appréhendés, pour la période postérieure à l'entrée en vigueur du RGPD, par l'application des dispositions dudit Règlement. Pour ce faire, elle s'appuie également sur l'arrêt du Conseil d'Etat du 1er mars 2021 relatif à la société Futura Internationale, considérant que cette jurisprudence s'applique à un cas d'espèce distinct du présent dossier : dans l'arrêt Futura Internationale, le Conseil d'État a pris soin de préciser que des manquements délibérés n'avaient pas été corrigés malgré la mise en demeure de la CNIL. Cette jurisprudence n'est donc pas transposable au cas d'espèce selon la société dans la mesure où elle s'est d'office vu proposer une sanction sans mise en demeure ni injonction préalable de la CNIL et qu'elle a en outre collaboré de manière diligente et de bonne foi avec la CNIL dès la notification de l'incident.

54. En outre, la société SLIMPAY explique que la vulnérabilité du serveur est la conséquence d'une négligence humaine isolée et non d'une carence de son dispositif technique et organisationnel. Elle rappelle que l'obligation générale de sécurité des entreprises doit s'analyser en une obligation de moyens et non de résultat. Elle ajoute qu'elle a mis fin à la violation de données immédiatement après en avoir été informée. Elle indique également que l'exploitation de données conservées dans le serveur nécessitait des connaissances informatiques et l'utilisation d'outils spécifiques, que les données présentes sur le serveur dataient de 2012 à 2013 et que, par conséquent, elles étaient difficilement exploitables par un attaquant. Elle relève enfin que l'adresse IP du serveur n'était pas référencée sur un moteur de recherche.

55. Lors de la séance de la formation restreinte, la société a précisé que la négligence humaine évoquée dans ses écritures était en réalité imputable […]. Elle a largement insisté sur le fait qu'elle n'avait pas commis, en tant que responsable de traitement, de manquement à ses obligations en matière de sécurité dans la mesure où l'erreur a été commise par […].

56. En premier lieu, s'agissant du principe de non-rétroactivité, la formation restreinte considère que, dans la mesure où la violation de données à caractère personnel, ainsi que le défaut de sécurité dans lequel elle a trouvé son origine ont perduré après le 25 mai 2018, date de l'entrée en application du RGPD, c'est au regard de ce texte que les manquements reprochés à la société SLIMPAY doivent être appréciés. Cette analyse a été confortée par le Conseil d'État dans sa décision du 1er mars 2021 concernant la société Futura Internationale. Dans cette affaire faisant suite à une plainte relative à du démarchage téléphonique de la part de la société Futura Internationale, le Conseil d'État a considéré que, si les manquements de la société ont été constatés lors d'une mission de contrôle à laquelle a procédé la CNIL avant l'entrée en application du RGPD, ils se sont poursuivis après cette date. Le Conseil d'État en a conclu que " c'est ainsi à bon droit que la CNIL, constatant le caractère continu des manquements relevés […], a considéré le RGPD applicable aux faits de l'espèce et apprécié les manquements au regard de celui-ci " (Conseil d'État, 10ème-9ème chambres réunies, 1er mars 2021, Futura Internationale, n° 437808).

57. La formation restreinte rappelle en outre que, conformément à l'article 20 de la loi Informatique et Libertés, le président de la CNIL n'est pas tenu d'adresser une mise en demeure à l'organisme avant d'ouvrir une procédure de sanction à son encontre.

58. En deuxième lieu, la formation restreinte relève que l'accès au serveur en question n'était encadré d'aucune mesure de restriction d'accès satisfaisante dans la mesure où il était possible d'y accéder à partir d'une URL composée d'une adresse IP facilement identifiable à l'aide de programmes de balayage de ports, qui sont disponibles sur le web et souvent utilisés par les attaquants afin de détecter des serveurs non ou mal sécurisés.

59. La formation restreinte relève également que la société n'avait mis en place aucune mesure de journalisation des accès au serveur, ce qui aurait pourtant permis de détecter les actions effectuées sur le serveur. En effet, la mise en place d'une journalisation des activités, c'est-à-dire un enregistrement des activités dans des " fichiers journaux " ou " logs ", notamment pour les accès aux différents serveurs d'un système d'information, est cruciale en ce qu'elle permet de tracer les activités et de détecter toutes les anomalies ou évènements liés à la sécurité, comme les accès frauduleux et les utilisations abusives de données à caractère personnel. Ainsi, dans ses recommandations de sécurité pour la mise en œuvre d'un système de journalisation, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) relevait que " les journaux d'évènements constituent une brique technique indispensable à la gestion de la sécurité des systèmes d'information " dans la mesure où ils peuvent être utilisés " a priori pour détecter des incidents de sécurité " et a posteriori pour " comprendre le cheminement d'une attaque et […] évaluer son impact ".

60. La formation restreinte note par ailleurs que les données contenues dans le serveur pouvaient facilement être lues puisqu'elles étaient conservées dans des formats lisibles au moyen d'un simple éditeur de texte ou d'outils disponibles et bien documentés sur Internet.

61. Ainsi, l'absence de mise en place de mesure de sécurité protégeant le serveur en cause, notamment de restriction des accès aux seules personnes qui auraient dues être autorisées, a provoqué l'accessibilité des données concernées depuis Internet et ces données étaient aisément lisibles en raison du format dans lequel elles étaient conservées.

62. En troisième lieu, la formation restreinte estime que l'argument de la société, consistant à dire qu'elle ne serait pas responsable du manquement à ses obligations en matière de sécurité dans la mesure où l'erreur a été commise par […], ne saurait emporter la conviction.

63. Tout d'abord, la formation restreinte relève que les défauts de sécurité ne résultent pas d'une erreur humaine isolée, mais d'insuffisances répétées, dès lors que la société aurait dû veiller à assurer la sécurité des données en cause à plusieurs étapes. À cet égard, lorsqu'elle a décidé de réutiliser les données pour son projet interne, il lui appartenait de vérifier que le serveur utilisé à ces fins n'était accessible que par les personnes autorisées. La même exigence de surveillance s'imposait a minima à la société lorsqu'elle a achevé son projet de recherche. Aussi, la société ne saurait rejeter la responsabilité de ces insuffisances répétées sur une erreur humaine isolée […], lequel, en tout état de cause, agissait en sa qualité de salarié sur les instructions de la société et pour son compte.

64. Ensuite, la sécurité d'un système d'information repose sur un ensemble de mesures, techniques et procédurales, et non sur la seule compétence des personnes […]. La mise en œuvre effective de ces mesures techniques et procédurales devant justement pallier les carences humaines. La société aurait ainsi dû prévoir des garde-fous complémentaires. La formation restreinte considère que cette situation reflète un problème organisationnel au sein de la société.

65. Dès lors, la formation restreinte considère que la société SLIMPAY a méconnu son obligation résultant des dispositions de l'article 32 du Règlement.

- Sur la portée du manquement

66. La société soutient que le manquement n'a pas causé de préjudice aux personnes concernées par la violation de données à caractère personnel, aucune de ces personnes ne lui ayant fait part d'une utilisation frauduleuse de ses données à caractère personnel. Elle explique avoir fait réaliser un audit par une société tierce, la société […], après la découverte de la vulnérabilité, lequel fait apparaître que les données présentes sur le serveur n'ont pas été exploitées par un attaquant.

67. S'agissant de la portée de ce manquement, la formation restreinte relève qu'il ressort du complément à la notification envoyé le 26 février 2020 aux services de la CNIL que la violation de données à caractère personnel a compromis les données à caractère personnel de 12 478 819 ressortissants européens.

68. La formation restreinte considère que l'absence de preuve d'une utilisation frauduleuse des données est sans incidence sur la caractérisation du manquement à l'obligation de sécurité. En effet, le risque d'utilisation frauduleuse des données à caractère personnel était réel, indépendamment des cas de fraude, dans la mesure où les données de nombreuses personnes ont été rendues accessibles à des tiers non autorisés. L'absence de dommage avéré pour les

personnes concernées n'a pas d'incidence sur l'existence du défaut de sécurité, qui constitue le manquement à l'article 32 du RGPD.

69. La formation restreinte rappelle également que des données d'état civil (civilité, nom, prénom), des coordonnées postales, électroniques et téléphoniques, et des informations bancaires (BIC/IBAN) ont été compromises.

70. Elle souligne à cet égard qu'au regard de la nature de ces données à caractère personnel, les personnes concernées par la violation sont exposées au risque d'une réutilisation de leurs données à caractère personnel par des attaquants. En effet, elles encourent le risque que leurs données directement identifiantes fassent l'objet d'un accès illicite, revendues à des tiers et réutilisées dans d'autres schémas d'attaques, notamment l'hameçonnage (ou " phishing "), technique consistant à se faire passer pour un organisme officiel (organisme de sécurité sociale, banque, etc.) qui demande par exemple à sa " proie " de confirmer ses données bancaires. En outre, ces personnes sont particulièrement exposées à des risques d'usurpation d'identité.

b) Sur le grief d'insuffisance de la robustesse des mots de passe d'accès à l'interface utilisateur

71. La rapporteure relève que les mots de passe permettant aux marchands d'accéder à leur espace " client " sont conservés avec la fonction de hachage SHA-1 qui est obsolète. Elle note également que ces mots de passe peuvent n'être composés que d'un seul caractère, ce qui ne permet pas d'assurer la sécurité des données auxquelles ils donnent accès.

72. En défense, la société explique qu'une erreur s'est glissée dans les premières informations communiquées par SLIMPAY lors du contrôle sur pièces. Elle indique que l'emploi de la fonction de hachage SHA-1 concerne uniquement l'ancienne interface utilisateur mise à disposition par SLIMPAY et actuellement en cours de décommissionnement, et non l'interface actuelle. Elle précise que les accès à cette ancienne interface ont été révoqués et que seuls deux marchands utilisent encore cette solution bien que SLIMPAY leur ait dûment notifié la nécessité de migrer dans les meilleurs délais vers la nouvelle solution.

73. La société ajoute que la nouvelle solution utilise la fonction de hachage Bcrypt recommandée par la CNIL pour stocker les mots de passe sur une base de données dédiée. La dernière version de l'interface actuelle embarque une fonction dite " anti brute-force ", qui intègre une authentification multi-facteurs et impose de recourir à un mot de passe d'une longueur de 10 à 128 caractères, comprenant quatre typologies de caractères (majuscule, minuscule, chiffre et caractère spécial).

74. La formation restreinte relève d'abord que, dans ses observations en réponse au rapport de sanction, la société a transmis des informations différentes de celles communiquées lors du contrôle sur pièces s'agissant de la fonction de hachage utilisée pour le stockage des mots de passe permettant aux marchands d'accéder à leur espace " client ". La société a ainsi indiqué que l'utilisation de la fonction de hachage obsolète (SHA-1) concerne uniquement l'ancienne interface utilisateur, en cours de décommissionnement, et qui est utilisée par deux marchands. La formation restreinte relève ensuite que les deux marchands en question ont été mis en demeure de migrer dans les meilleurs délais vers la dernière version de l'interface, qui utilise une fonction de hachage satisfaisante. La formation restreinte observe enfin que les éléments du dossier ne permettent pas de remettre en cause les déclarations actuelles de la société.

75. La formation restreinte prend dès lors acte de ces déclarations et considère qu'il n'y a pas lieu de retenir de manquement relatif à l'obligation de sécurité en raison d'une robustesse insuffisante des mots de passe d'accès à l'interface utilisateur, permettant aux marchands d'accéder aux données à caractère personnel se rapportant à leur compte.

3. Sur le manquement à l'obligation de communication aux personnes concernées d'une violation de données à caractère personnel

76. Aux termes de l'article 34 du RGPD, " 1. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).

3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie :

a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;

b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser ;

c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace. […] ".

77. Le considérant 86 du RGPD prévoit que, lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne physique, le responsable du traitement devrait la communiquer à la personne concernée dans les meilleurs délais afin qu'elle puisse prendre les précautions qui s'imposent.

78. En l'espèce, la rapporteure relève qu'à la suite de la violation de données, la société SLIMPAY, qui dispose d'une " procédure de traitement des violations de données personnelles ", a considéré que le risque lié à celle-ci n'était pas élevé pour les personnes concernées et qu'elle ne devait par conséquent pas les informer.

79. La rapporteure considère toutefois qu'au regard de la nature des données à caractère personnel, du volume de personnes concernées, de la facilité d'identifier les personnes touchées par la violation et des conséquences possibles pour les personnes concernées, le risque associé à la violation peut être considéré comme élevé et qu'une communication aux personnes concernées aurait dû être faite.

80. En défense, la société SLIMPAY indique qu'elle a informé à bref délai les marchands pour le compte desquels elle avait collecté les données objet de la violation de données, et qu'ils ont ainsi été mis en mesure, en leur qualité de responsables de traitement, d'informer les personnes concernées s'ils l'estimaient nécessaire.

81. La société précise en outre que, quand bien même le traitement mené à des fins d'amélioration de la lutte contre la fraude était mis en œuvre par SLIMPAY en qualité de responsable de traitement, les données sur la base desquelles le traitement a été réalisé ont été initialement collectées et traitées par SLIMPAY en qualité de sous-traitant pour le compte de ces marchands. Il n'était donc pas possible selon elle d'informer les débiteurs concernés directement sans l'accord de ces marchands.

82. La société considère en tout état de cause que le format des données et les circonstances entourant la violation de données l'ont amenée à conclure à l'absence de risque élevé pour les personnes concernées au sens de l'article 34 du RGPD, au regard des éléments suivants :

- le format des données ne permettait pas d'appréhender directement la nature, ni le contenu des données ;

- aucune divulgation des données imputable à SLIMPAY n'a été établie ;

- aucune usurpation ou tentative d'usurpation d'identité n'a été rapportée par un débiteur auprès de SLIMPAY ;

- la nature des données ne permettait pas de conclure à un risque élevé de fraude financière ;

- le risque pour une personne concernée paraissait inopérant dans la mesure où tout débiteur dispose de la faculté de s'opposer à un prélèvement indu sans justification pendant huit semaines et jusqu'à treize mois après la transaction avec une justification.

83. La société rappelle en outre qu'elle ne disposait pas de l'ensemble des adresses de messagerie des personnes concernées. Elle en conclut donc que l'information individuelle des débiteurs se serait révélée impossible pour une large partie d'entre eux. Elle considère par ailleurs qu'une communication publique n'aurait pas été pertinente dans la mesure où ses services étant offerts à des clients professionnels, la majorité des débiteurs concernés n'auraient pas été en mesure de déterminer si leurs données avaient ou non été traitées par elle, intervenant de manière non visible en qualité de prestataire de services de paiement.

84. En premier lieu, la formation restreinte considère que l'argument invoqué par SLIMPAY pour s'affranchir de sa responsabilité, selon lequel les données sur la base desquelles le traitement a été réalisé ont été initialement collectées et traitées par SLIMPAY en qualité de sous-traitant pour le compte des marchands, ne saurait emporter la conviction. Le fait que les données en question aient été initialement traitées pour une autre finalité pour laquelle la société agit en tant que sous-traitant est sans incidence sur son obligation au titre de l'article 34 du RGPD dans la mesure où elle a réutilisé ces données pour son propre compte, en tant que responsable de traitement.

85. En deuxième lieu, la formation restreinte considère qu'au regard de la nature des données à caractère personnel (comportant notamment des informations bancaires), du volume de personnes concernées (plus de 12 millions), de la facilité d'identifier les personnes touchées par la violation à partir des données accessibles et des conséquences possibles pour les personnes concernées (risques d'hameçonnage ou d'usurpation d'identité), le risque associé à la violation devait être considéré comme élevé.

86. En troisième lieu, la formation restreinte relève que l'article 34-3 du RGPD prévoit que la communication aux personnes concernées n'est pas nécessaire dans certains cas, notamment si le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées, s'il a pris des mesures ultérieures qui garantissent que le risque élevé pour les personnes n'est plus susceptible de se matérialiser ou si elle exigerait des efforts disproportionnés. La formation restreinte considère que la société ne saurait se prévaloir de ces dispositions dans la mesure où elle n'a pas mis en œuvre de mesures de protection appropriées pour assurer la sécurité des données affectées par la violation (afin de limiter leur accès aux seules personnes autorisées). En outre, si la société a fermé le serveur concerné, les données sont restées accessibles entre novembre 2015 et février 2020, soit pendant une très longue période.

87. S'agissant ensuite de l'argument de la société selon lequel l'information individuelle de l'ensemble des débiteurs aurait nécessité des efforts disproportionnés, la formation restreinte relève que la société disposait de 6 250 310 adresses de messagerie électronique, soit environ de la moitié des personnes concernées. Elle aurait donc à tout le moins pu informer ces personnes de la violation de données, sans que cela représente un effort disproportionné.

88. S'agissant de l'argument de la société selon lequel une communication publique sur son site web n'aurait pas été pertinente puisque la majorité des débiteurs concernés n'auraient pas été en mesure de déterminer s'ils avaient eu ou non recours aux services de SLIMPAY, qui intervient de manière opaque en qualité de prestataire de services de paiement, la formation restreinte relève tout d'abord que le site web de la société comporte les noms de certains de ses clients et que les débiteurs de ces marchands auraient ainsi pu être en mesure de savoir que leurs données étaient potentiellement traitées par SLIMPAY et possiblement concernées par la violation. À cet égard, elle rappelle que toute personne physique peut exercer ses droits prévus par le RGPD auprès de toute société et ainsi obtenir des informations sur la question de savoir si ses données sont ou non traitées par ladite société. En cas de communication publique, les personnes qui le

souhaitent auraient donc pu contacter la société afin de savoir si elles étaient concernées par la violation de données. Ensuite, la formation restreinte observe que l'information relative à une violation de données de cette ampleur peut être reprise sur le web (réseaux sociaux, journaux et sites spécialisés, etc.). Une communication publique sur le site web de l'organisme peut ainsi être un point de départ et l'information peut prendre ensuite une dimension bien plus importante.

89. Compte tenu de ces éléments, la formation restreinte considère que la société a méconnu ses obligations au titre de l'article 34 du RGPD, relatif à la communication aux personnes concernées d'une violation de données à caractère personnel.

III. Sur les mesures correctrices et leur publicité

90. 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° A l'exception des cas où le traitement est mis en œuvre par l'Etat, 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 ".

91. 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.

92. En premier lieu, sur le principe du prononcé d'une amende, la société soutient en défense qu'une telle mesure n'est pas justifiée. La société affirme qu'elle s'est conformée à ses obligations légales et réglementaires et qu'elle a coopéré avec la CNIL de manière diligente et en toute bonne foi depuis la prise de connaissance de l'incident de sécurité. Elle souligne notamment qu'elle a notifié la violation de données à la CNIL dès sa prise de connaissance dans le délai réglementaire de 72 heures, fait diligenter des investigations ayant permis de conclure à une absence de risque pour les droits et libertés des personnes concernées, mis en place des mesures correctives très rapidement et informé les marchands concernés à bref délai.

93. 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.

94. La formation restreinte relève tout d'abord que les manquements concernent un nombre très important de personnes, puisque la violation de données a concerné plus de 12 millions de débiteurs.

95. La formation restreinte relève ensuite que les données accessibles (civilité, nom, prénom, adresse électronique, adresse postale, numéro de téléphone, BIC/IBAN) permettent d'obtenir des informations très précises sur les personnes concernées en révélant leur identité et leurs coordonnées. En outre, des données particulières sont en cause dès lors que certaines sont relatives à des informations financières. Le fait notamment que figure l'IBAN n'est pas anodin. Comme la Banque de France l'a indiqué dans son ouvrage " Paiements et infrastructures de marché à l'ère digitale ", les IBAN sont des données de paiement " sensibles " (au sens courant du terme) car pouvant être utilisées pour commettre des fraudes. Le Comité européen de la protection des données qualifie ce type de données de " hautement personnelles ". La formation restreinte considère que la société aurait dû faire preuve d'une vigilance particulière en ce qui concerne la sécurisation de telles données, lesquelles peuvent être réutilisées par des tiers non autorisés, portant ainsi préjudice aux personnes concernées par la violation de données. Celles-ci sont par exemple exposées à un risque d'usurpation d'identité ou d'hameçonnage (ou " phishing ", c'est-à-dire l'envoi de courriers frauduleux aux fins d'obtention de données) dès lors que leur identité complète, associée à leur adresse électronique pour un grand nombre, était librement accessible.

96. La formation restreinte relève enfin que les données sont restées accessibles pendant une très longue période, entre la fin de l'import des données sur le serveur en novembre 2015 et la découverte de l'incident par la société le 14 février 2020, et ce alors que le traitement concerné, le projet de recherche, avait pris fin en juillet 2016. Il ressort des éléments figurant au dossier que, préalablement à la survenance de la violation de données, la société n'avait pas pris les mesures élémentaires en termes de sécurité. Ce n'est qu'à la faveur d'un signalement par un marchand que le défaut de sécurité a été porté à la connaissance de la société.

97. Si la formation restreinte relève que la société SLIMPAY a immédiatement réagi à la violation de données dès sa découverte en février 2020 et qu'elle a coopéré tout au long de la procédure avec les services de la CNIL, elle considère que la violation de données résulte d'une négligence des règles élémentaires de sécurité des systèmes d'information qui a conduit à rendre accessibles à des tiers non autorisés les données à caractère personnel traitées par la société.

98. La formation restreinte rappelle que les négligences commises en matière de sécurité étaient particulièrement graves : l'accès au serveur en cause n'était encadré d'aucune mesure de restriction d'accès satisfaisante, la société n'avait mis en place aucune mesure de journalisation des accès au serveur et les données contenues dans le serveur pouvaient facilement être lues.

99. La formation restreinte note que cette négligence est d'autant plus grave au regard du secteur d'activité de la société qui se targue par ailleurs d'être le leader européen des paiements récurrents et qui est une société dont la gestion de systèmes d'information complexes est le cœur de métier.

100. La formation restreinte relève en outre que, en méconnaissance de l'article 34 du RGPD, la société n'a pas informé les personnes concernées de la survenance de la violation de données, alors qu'elle disposait de plus de 6 millions d'adresses de messagerie électronique pour ce faire, soit environ de la moitié des personnes concernées, et qu'elle aurait pu informer la moitié restante par le biais d'une communication publique sur son site.

101. La formation restreinte rappelle enfin que la société a eu recours à des sous-traitants agissant sous son autorité en tant que sous-traitants de second niveau vis-à-vis des marchands, pour les services qu'elle fournit à ces derniers, sans avoir effectué de démarches suffisantes pour s'assurer que ces derniers présentent les garanties requises et sans avoir conclu avec certains d'entre eux de contrats contenant l'ensemble des clauses prévues par l'article 28 paragraphe 3 du RGPD.

102. En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative au regard des manquements aux articles 28 paragraphes 3 et 4 du RGPD, 32 et 34 du RGPD.

103. En deuxième lieu, s'agissant du montant de l'amende, la société considère que celui proposé par la rapporteure est disproportionné au regard de sa situation économique. Elle insiste sur sa situation financière déficitaire et précise qu'une amende élevée aurait un impact catastrophique pour les emplois qu'elle tente de pérenniser.

104. 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 la société un manquement aux articles 28, 32 et 34 du Règlement, le montant maximum de l'amende pouvant être retenu s'élève à 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

105. La formation restreinte rappelle également que les amendes administratives doivent être dissuasives mais proportionnées. Elle considère en particulier que l'activité de la société 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 la société fait état d'un chiffre d'affaires de […] euros en 2019 et de […] euros en 2020, pour un résultat net s'élevant à […] euros en 2019 et à […] euros en 2020.

106. Au vu de ces éléments, la formation restreinte considère que le prononcé d'une amende de 180 000 euros apparaît justifié.

107. En troisième lieu, s'agissant de la publicité de la sanction, la société SLIMPAY fait valoir qu'elle tente de se faire une place sur un marché international très concurrentiel de prestataires de services de paiement, majoritairement dominé par des sociétés chinoises et américaines, qui sont peu soucieuses de la protection des données des Européens. Elle ajoute déployer des efforts substantiels depuis plus de dix ans pour devenir un partenaire de confiance pour les acteurs économiques européens, précisant qu'une sanction publique anéantirait durablement les résultats obtenus grâce à ses efforts.

108. La formation restreinte considère que la publicité de la sanction se justifie au regard de la gravité des manquements commis, de leur persistance et du nombre de personnes concernées.

PAR CES MOTIFS

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

- **prononcer à l'encontre de la société SLIMPAY une amende administrative d'un montant de 180 000 (cent quatre-vingt mille) euros ;**

- 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

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.