# Décision de la Commission nationale siégeant en formation restreinte sur l'issue de l'enquête n° […] menée auprès de la Société A

Délibération n° 31FR/2021 du 5 août 2021

La Commission nationale pour la protection des données siégeant en formation restreinte composée de Mme Tine A. Larsen, présidente, et de Messieurs Thierry Lallemang et Christophe Buschmann, commissaires ;

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, et abrogeant la directive 95/46/CE ;

Vu la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, notamment son article 41 ;

Vu le règlement d'ordre intérieur de la Commission nationale pour la protection des données adopté par décision n°3AD/2020 en date du 22 janvier 2020, notamment son article 10 point 2 ;

Vu le règlement de la Commission nationale pour la protection des données relatif à la procédure d'enquête adopté par décision n°4AD/2020 en date du 22 janvier 2020, notamment son article 9 ;

Considérant ce qui suit :

## I. Faits et procédure

1. En date du 20 mai 2019, la Commission nationale pour la protection des données (ci-après : la « CNPD ») a été saisie d'une réclamation de […] (ci-après : « le réclamant ») introduite contre la Société A. Ce dernier a signalé à la CNPD que des courriers électroniques comprenant des données médicales, ainsi que des indications et des questions sensibles relatives à son état de santé, rédigés par son assurance et qui lui étaient destinés, auraient été envoyés à des destinataires tiers.

2. Plus précisément, le réclamant a affirmé qu'en date du 19 octobre 2018, une employée de la Société A aurait envoyé un courrier électronique à l'adresse e-mail « [...] », alors que son adresse e-mail correcte serait « [...] ». Cet e-mail comprenait dans le corps du texte, entre autres, le nom de famille du réclamant, son sexe, ainsi que des indications détaillées quant à certaines pathologies. Annexés audit e-mail se trouvaient trois formulaires distincts, à remplir par le réclamant, relatifs aux pathologies que ce dernier a déclaré auprès de son assurance dans le cadre de l'obtention d'une assurance-vie. Le 7 novembre 2018, l'employée de la Société A a effectivement informé le réclamant par e-mail que le courrier électronique précité du 19 octobre 2018 avait été envoyé à une adresse erronée.

3. Le réclamant a précisé par ailleurs qu'en date du 29 novembre 2018, un deuxième courrier électronique aurait été adressé par la même employée de la Société A à l'adresse e-mail « [...] » et qui comprenait dans le corps du texte son nom de famille, des questions très précises quant à une pathologie spécifique, le nom de famille du docteur de l'assurance-vie, une indication d'adresse dudit docteur, ainsi que deux formulaires non-remplis référençant ladite pathologie et destinés à être remplis par lui ou son docteur.

4. Par e-mail du 3 décembre 2018, la Société A a de nouveau contacté par e-mail le réclamant et l'a informé que des envois erronés répétitifs ont eu lieu et que le délégué à la protection des données (ci-après : « DPD ») de l'assurance a été notifié. Il y est précisé également que toutes les mesures seront prises pour éviter de tels incidents dans le futur.

5. Lors de sa séance de délibération du 5 juin 2019, la Commission nationale pour la protection des données siégeant en formation plénière (ci-après: « Formation Plénière ») a dès lors décidé d'ouvrir une enquête auprès de la Société A sur base de l'article 37 de la loi du 1er août 2018 portant organisation de la Commission nationale pour

la protection des données et du régime général sur la protection des données (ci-après : « loi du 1er août 2018 ») et de désigner Monsieur Marc Lemmer comme chef d'enquête.

6. Aux termes de la décision de la Formation Plénière l'enquête menée par la CNPD avait comme objet de vérifier le respect des dispositions du 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, et abrogeant la directive 95/46/CE (ci-après : « RGPD ») et de la loi du 1er août 2018.

7. En date du 19 juillet 2019, des agents de la CNPD ont effectué une visite dans les locaux de la Société A. Etant donné que le procès-verbal relatif à ladite mission d'enquête sur place ne mentionne que comme responsable du traitement contrôlé la Société A,[1] la décision de la Commission nationale pour la protection des données siégeant en formation restreinte sur l'issue de l'enquête (ci-après: « Formation Restreinte ») se limitera aux traitements contrôlés par les agents de la CNPD et effectués par la Société A.

8. La Société A est une […] inscrite au registre du Commerce et des Sociétés de Luxembourg sous le numéro B […] et ayant son siège social […] (ci-après « le contrôlé »). Le contrôlé [a pour objet de faire toutes opérations d'assurance et de réassurance de la branche « Vie » […]. » [2]

9. En date du 23 juillet 2019, le contrôlé a envoyé des précisions sur les questions demandées par les agents de la CNPD lors de leur visite sur place et concernant la possibilité de parler au DPD, ainsi que sur le registre interne des violations de données à caractère personnel. Des copies des courriers électroniques litigieux ont par ailleurs été annexées audit courrier.

10. Par courrier du 8 août 2019, le contrôlé a répondu au procès-verbal dressé par les agents de la CNPD, ainsi qu'aux questions supplémentaires posées par courrier de la CNPD du 29 juillet 2019.

[1] Voir notamment le procès-verbal no. […]/2019 relatif à la mission d'enquête sur place effectuée en date du 19 juillet 2019 auprès de la Société A.

[2] Selon les statuts coordonnés au […].

11. Par courrier du 17 septembre 2019, le contrôlé a répondu aux questions additionnelles posées par courrier de la CNPD du 5 septembre 2019.

12. A l'issue de son instruction, le chef d'enquête a notifié au contrôlé en date du 29 octobre 2019 une communication des griefs détaillant les manquements qu'il estimait constitués en l'espèce, et plus précisément une non-conformité aux exigences prescrites par les articles 5.1.f), 32.1. a) et b), 33.1, 33.5, 34.1 et 37.7 du RGPD.

13. Le 29 novembre 2019, le contrôlé a produit des observations écrites sur la communication des griefs.

14. Un courrier complémentaire à la communication des griefs a été adressé au contrôlé en date du 15 décembre 2020. Dans ce courrier, le chef d'enquête a proposé à la Formation Restreinte d'adopter cinq mesures correctrices différentes, ainsi que d'infliger au contrôlé une amende administrative d'un montant de 275.000 euros.

15. Par courrier du 27 janvier 2021, le contrôlé a produit des observations écrites sur le courrier complémentaire à la communication des griefs.

16. La présidente de la Formation Restreinte a informé le contrôlé par courrier du 29 avril 2021 que son affaire serait inscrite à la séance de la Formation Restreinte du 14 juillet 2021. Le contrôlé a confirmé sa présence à ladite séance en date du 1er juin 2021.

17. Lors de la séance de la Formation Restreinte du 14 juillet 2021, le chef d'enquête et le contrôlé ont exposé leurs observations orales à l'appui de leurs observations écrites et ont répondu aux questions posées par la Formation Restreinte. Le contrôlé a eu la parole en dernier.

## II. En droit

### II. 1. Quant aux motifs de la décision

#### A. Sur le manquement lié à l'obligation de documenter une violation de données à caractère personnel

1. Sur les principes

18. Selon les dispositions de l'article 33.5 du RGPD, le responsable du traitement est obligé de documenter « *toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier.* » La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect de cet article.

19. L'obligation de documenter une violation de données découle également du principe de responsabilité (« accountability ») repris aux articles 5.2 et 24 du RGPD exigeant que le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD.

20. Les obligations en la matière ont été explicitées par le Groupe de Travail Article 29 dans ses lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679 (ci-après : « WP 250rev.01 »).

21. A noter que le Comité européen de la protection des données (ci-après : « CEPD »), qui remplace depuis le 25 mai 2018 le Groupe de Travail Article 29, a repris et réapprouvé les documents adoptés par ledit Groupe entre le 25 mai 2016 et le 25 mai 2018, comme notamment lesdites lignes directrices.[3]

22. Le responsable du traitement peut décider de documenter les violations dans le cadre de son registre des activités de traitement tenu conformément à l'article 30 du RGPD. Un registre séparé n'est pas nécessaire, à condition que les informations concernant les violations soient clairement identifiables en tant que telles et puissent être extraites sur demande.[4] S'il appartient donc au responsable du traitement de déterminer la méthode et la structure à utiliser pour documenter une violation, certaines informations clés devraient être incluses en toutes circonstances comme requis par l'article 33.5 du RGPD.

[3] Voir décision Endorsement 1/2018 du CEPD du 25 mai 2018, disponible sous : https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

[4] Voir WP 250rev.01, page 30, note de bas de page 43.

23. Le WP 250rev.01 précise par ailleurs qu'en cas de *« manquement à cette obligation de documenter correctement une violation, l'autorité de contrôle pourrait exercer ses pouvoirs au titre de l'article 58 et/ou imposer une amende administrative conformément à l'article 83. »*

24. Pour déclencher l'obligation prévue à l'article 33.5 du RGPD, deux conditions cumulatives doivent dès lors être réunies :

- des données doivent faire l'objet d'une violation de données à caractère personnel au sens de l'article 4.12 du RGPD ;
- ces données sont à qualifier de données à caractère personnel au sens de l'article 4.1 du RGPD.

1.1. Quant à la notion de donnée à caractère personnel

25. L'article 4.1 du RGPD définit une donnée à caractère personnel comme *« toute information se rapportant à une personne physique identifiée ou identifiable […]; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».*

26. D'après le considérant (26) du RGPD, pour *« déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. »*

27. Le Groupe de Travail Article 29 a estimé qu'on *« peut considérer une personne physique comme « identifiée » lorsque, au sein d'un groupe de personnes, elle se « distingue » de tous les autres membres de ce groupe. La personne physique est donc « identifiable » lorsque, même sans avoir encore été identifiée, il est possible de le faire*

*(comme l'exprime le suffixe «-able»). […] S'agissant des personnes « directement » identifiées ou identifiables, le nom de la personne est évidemment l'identifiant le plus courant et, dans la pratique, la notion de « personne identifiée » implique le plus souvent une référence au nom de cette personne. Afin de s'assurer de son identité, le nom de la personne doit parfois être associé à d'autres éléments d'information (date de naissance, nom des parents, adresse ou photo d'identité) afin d'éviter toute confusion entre cette personne et d'éventuels homonymes. […] Le nom peut également être le point de départ conduisant à des informations sur le domicile de la personne ou l'endroit où elle se trouve et à des informations sur les membres de sa famille (par le biais du nom de famille) et sur différentes relations juridiques et sociales associées à ce nom (scolarité/études, dossier médical, comptes bancaires). »* [5]

28. S'agissant des personnes « indirectement » identifiées ou identifiables, le Groupe de Travail Article 29 fait référence au « *phénomène des « combinaisons uniques », à quelque degré que ce soit. Pour les cas où, de prime abord, les identifiants sont insuffisants pour permettre à quiconque de distinguer une personne particulière, cette personne peut néanmoins être « identifiable », car ces informations combinées à d'autres éléments d'information (que ces derniers soient conservés par le responsable du traitement ou non) permettent de la distinguer parmi d'autres personnes.* » [6]

29. La Cour de justice de l'Union européenne (ci-après : « CJUE ») a statué dans ce sens en considérant que *« l'opération consistant à faire référence, sur une page Internet, à diverses personnes et à les identifier soit par leur nom, soit par d'autres moyens, par exemple leur numéro de téléphone ou des informations relatives à leurs conditions de travail et à leurs passe-temps, constitue un « traitement de données à caractère personnel automatisé en tout ou en partie, » au sens de l'article 3, paragraphe 1, de la directive 95/46 ».* [7]

[5] Avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin 2007, WP 136, p. 13 et 14.

[6] Avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin 2007, WP 136, p.14.

[7] Arrêt du 6 novembre 2003 dans l'affaire C-101/01 (Lindqvist), point 27. A noter que la Directive 95/46 a été abrogée par le RGPD, mais la définition d'une donnée à caractère personnel est restée quasiment identique.

1.2. Quant à la notion de violation de données à caractère personnel

30. L'article 4.12 du RGPD définit une violation de données à caractère personnel comme « *une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données* ».

31. Le WP 250rev.01 (p.7) précise dans ce contexte que « […] *le traitement non autorisé ou illicite peut inclure la divulgation de données à caractère personnel à des destinataires (ou l'accès à de telles données par ceux-ci) n'étant pas autorisés à les recevoir (ou à y avoir accès), ou toute autre forme de traitement en infraction au RGPD.* »

32. Le considérant (85) du RGPD détaille les conséquences sur les personnes concernées, car une *« violation de données à caractère personnel risque, si l'on n'intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels ou un préjudice moral tels qu'une perte de contrôle sur leurs données à caractère personnel ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données à caractère personnel protégées par le secret professionnel ou tout autre dommage économique ou social important. »*

2. En l'espèce

33. Lors de la visite sur site du 19 juillet 2019, les agents de la CNPD ont constaté que le registre des violations de données à caractère personnel, crée par le contrôlé en mai 2018, ne comprenait aucune inscription.[8]

34. Par courrier du 23 juillet 2019, le contrôlé a confirmé les faits à la base de la réclamation reçue par la CNPD,[9] tout en précisant que selon son appréciation, la combinaison des données divulguées (nom de famille et conditions de santé) ne permettait

[8] Constats 3 et 5 du procès-verbal no. […]/2019 relatif à la mission d'enquête sur place effectuée en date du 19 juillet 2019 auprès de la Société A.

[9] Voir paragraphes 2 à 4 da la présente décision.

pas d'identifier directement ou indirectement le réclamant. Il a affirmé par ailleurs avoir contacté la CNPD par téléphone dans ce contexte et avoir procédé à une recherche sur internet qui n'aurait affichée aucun lien au réclamant. Par conséquent, le contrôlé a estimé que les informations divulguées par les deux courriers électroniques ne seraient pas à qualifier de données à caractère personnel et que donc, aucune violation de telles données n'aurait eu lieu.[10]

35. Dans son courrier du 17 septembre 2019, le contrôlé a par ailleurs indiqué qu'en date du 3 décembre 2018, le « Chief Executive Officer » (ci-après : « CEO ») et le DPD ont été informés des incidents, tandis que le 4 décembre 2018 un document […] a été établi par le « […] » et envoyé au CEO et au DPD.[11]

36. Le chef d'enquête a estimé par contre que *« les courriers électroniques litigieux divulgués à des destinataires erronés comprennent clairement des données à caractère personnel. Ainsi, le courrier électronique du 19 octobre 2018 contenait notamment le patronyme du réclamant, son sexe, son adresse électronique contenant une erreur de frappe, mais permettant de déduire la première lettre du prénom du plaignant, ainsi que des indications détaillées sur trois pathologies concrètes dont est affligé le plaignant. Par ailleurs, se trouvaient annexés audit e-mail trois formulaires non-sécurisés distincts, à remplir par le réclamant, relatifs aux pathologies que ce dernier a déclaré auprès du responsable du traitement dans le cadre de l'obtention d'une assurance-vie. Ces formulaires contenaient également l'adresse de la société d'assurance-vie concernée. Alors que cette information d'adresse n'est pas une donnée à caractère personnel per se, cette information (et notamment le Luxembourg comme pays d'envoi) peut être associée au plaignant aux fins de l'identifier.* » (Communication des griefs, p.3.)

37. Par ailleurs, le chef d'enquête était d'avis que l'envoi de courriers électroniques contenant des données à caractère personnel à un destinataire erroné doit être qualifié de violation de données à caractère personnel, cette dernière ayant *« entraîné, de manière accidentelle, une divulgation de données à caractère personnel à des personnes tierces qui n'étaient pas autorisées à prendre connaissance des informations contenues dans les courriers électroniques et leurs annexes. S'y ajoute le fait aggravant que les données*

[10] Voir aussi le courrier du contrôlé du 29 novembre 2019.

[11] Voir annexes 1 et 2 du courrier du contrôlé du 17 septembre 2019.

*divulguées aux personnes non autorisées étaient des données de santé revêtant un caractère particulièrement « sensible » au regard de la vie privée de la personne concernée. »* Il en a conclu que le contrôlé n'a pas respecté son obligation de documenter ces deux violations de données à caractère personnel et que dès lors, il échet de retenir à son encontre une non-conformité aux prescrits de l'article 33.5 du RGPD (Communication des griefs, p.5).

2.1. Quant à la présence de données à caractère personnel

38. La Formation Restreinte tient tout d'abord à préciser qu'une personne physique est à considérer comme identifiable si des renseignements contiennent des éléments d'identification qui peuvent permettre de l'identifier directement ou indirectement. D'après la CJUE, « *l'utilisation par le législateur de l'Union du terme « indirectement » tend à indiquer que, afin de qualifier une information de donnée à caractère personnel, il n'est pas nécessaire que cette information permette, à elle seule, d'identifier la personne concernée*. »[12] Dans la mesure où le considérant (26) du RGPD fait référence aux moyens susceptibles d'être raisonnablement mis en œuvre tant par le responsable du traitement que par toute « autre personne » pour identifier la personne physique directement ou indirectement, le libellé de celui-ci suggère que, pour qu'une donnée puisse être qualifiée de « donnée à caractère personnel » au sens de l'article 4.1 du RGPD, « *il n'est pas requis que toutes les informations permettant d'identifier la personne concernée doivent se trouver entre les mains d'une seule personne.* »[13]

39. Comme mentionné au point 28 de la présente décision, le Groupe de travail Article 29 a considéré que *« la personne physique est donc « identifiable » lorsque, même sans avoir encore été identifié, il est possible de le faire. […] S'agissant de personnes « directement » identifiées ou identifiables, le nom de la personne est évidemment l'identifiant le plus courant […]. Afin de s'assurer de son identité, le nom de la personne doit parfois être associé à d'autres éléments d'information […] afin d'éviter toute confusion entre cette personne et d'éventuels homonymes. […] Le nom peut également être le point de départ conduisant à des informations sur le domicile de la personne ou l'endroit où elle*

[12] Arrêt du 19 octobre 2016 dans l'affaire C-582/14 (Patrick Breyer contre Bundesrepublik Deutschland), point 41.

[13] Idem, point 43.

*se trouve […] et sur différentes relations juridiques et sociales associées à ce nom (scolarité / études, dossier médical, comptes bancaires). […] Tous ces nouveaux éléments d'information liés au nom peuvent permettre à quelqu'un de « zoomer » sur la personne en chair et en os, et grâce aux identifiants, l'élément d'information initial est alors associé à une personne physique que l'on peut distinguer d'autres personnes ».*[14]

40. En l'espèce, la Formation Restreinte tient à souligner que le courrier électronique du 19 octobre 2019 ne contenait pas uniquement le nom de famille du réclamant, mais aussi son sexe, son adresse électronique contenant une erreur de frappe, mais permettant de déduire la première lettre du prénom du réclamant, ainsi que des indications détaillées sur trois pathologies concrètes dont est atteintes le réclamant. Par ailleurs, l'adresse électronique de l'employée du contrôlé ayant envoyé le courriel litigieux, ainsi que les formulaires annexés audit courrier qui contenaient l'adresse de la société d'assurance vie concernée et notamment le Luxembourg comme pays d'envoi sont des informations qui peuvent être associées au réclamant aux fins de l'identifier.

41. Il en va de même pour ce qui concerne le courrier électronique envoyé erronément en date du 29 novembre 2018. Ont été divulgués le nom de famille du réclamant, son sexe, son adresse électronique contenant une erreur de frappe, mais permettant de déduire la première lettre de son prénom, des questions très précises quant à une pathologie spécifique, le nom de famille du docteur de l'assurance-vie et une indication de son adresse, ainsi que deux formulaires non-remplis référençant ladite pathologie.

42. La Formation Restreinte estime donc que, contrairement aux prétentions du contrôlé, les données transmises par les deux courriers électroniques litigieux permettent d'identifier le réclamant, du moins indirectement, et sont dès lors à qualifier comme données à caractère personnel au sens de l'article 4.1 du RGPD.

2.2. Quant à la présence d'une violation de données à caractère personnel

[14] Avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin 2007, WP 136, p. 13 et 14.

43. La Formation Restreinte constate tout d'abord que le document […] du contrôlé du 4 décembre 2018 est très sommaire et ne contient aucune analyse sur la qualification des données qui ont été divulguées par les deux courriers électroniques litigieux et sur leurs éventuelles conséquences pour la personne concernée. Elle ne peut dès lors pas accepter l'affirmation du contrôlé contenue dans son courrier du 29 novembre 2019[15] que ledit document contenait les informations essentielles requises par l'article 33.5 du RGPD, d'autant plus que ce [document] est daté presque sept semaines après l'envoi du premier courrier litigieux.

44. Ensuite, elle tient à rappeler que le WP 250rev.01 (p.8) classe les violations de données à caractère personnel selon trois principes de sécurité de l'information : *« violation de la confidentialité» – la divulgation ou l'accès non autorisés ou accidentels à des données à caractère personnel; «violation de l'intégrité» – l'altération non autorisée ou accidentelle de données à caractère personnel; «violation de la disponibilité» – la destruction ou la perte accidentelles ou non autorisées de l'accès à des données à caractère personnel. »*

45. L'envoi de courriers électroniques contenant des données à caractère personnel à un destinataire erroné est dès lors à qualifier de violation de données à caractère personnel du type « violation de la confidentialité », cette dernière ayant entraîné, de manière accidentelle, une divulgation de données à caractère personnel à des personnes tierces qui n'étaient pas autorisées à prendre connaissance des informations contenues dans les courriers électroniques et leurs annexes.

46. La Formation Restreinte constate donc que les deux conditions cumulatives déclenchant l'obligation prévue à l'article 33.5 du RGPD sont réunies, c'est-à-dire que des données à caractère personnel ont fait l'objet d'une violation de données à caractère personnel au sens des articles 4.1 et 4.12 du RGPD. Ainsi, que les violations doivent être notifiées à l'autorité de contrôle ou non, le contrôlé aurait dû documenter les violations

[15] Texte original: […]

dans son registre interne des violations de données à caractère personnel comme exigé par l'article 33.5 du RGPD.[16]

47. Au vu de ce qui précède, elle se rallie ainsi au constat du chef d'enquête[17] selon lequel le contrôlé n'a pas respecté son obligation de documenter ces deux violations de données à caractère personnel et qu'il échet donc de retenir à son encontre une non-conformité aux prescrits de l'article 33.5 du RGPD.

## B. Sur le manquement lié à l'obligation de notifier une violation de données à caractère personnel à l'autorité de contrôle

### 1. Sur les principes

48. Selon les dispositions de l'article 33.1 du RGPD, le responsable du traitement est tenu de notifier toute violation de données à caractère personnel à l'autorité de contrôle *« dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. »*

49. D'après le considérant (87) du RGPD, il *« convient de vérifier si toutes les mesures de protection techniques et organisationnelles appropriées ont été mises en œuvre pour établir immédiatement si une violation des données à caractère personnel s'est produite et pour informer rapidement l'autorité de contrôle et la personne concernée. Il convient d'établir que la notification a été faite dans les meilleurs délais, compte tenu en particulier de la nature et de la gravité de la violation des données à caractère personnel et de ses conséquences et effets négatifs pour la personne concernée. Une telle notification peut amener une autorité de contrôle à intervenir conformément à ses missions et à ses pouvoirs fixés par le présent règlement. »*

50. Dans le but de se conformer aux articles 33 et 34 du RGPD, le WP 250rev.01 recommande *« à la fois pour les responsables du traitement et les sous-traitants de disposer d'une procédure de notification documentée définissant la procédure à suivre*

[16] Voir WP250rev.01, p.30

[17] Communication des griefs, p. 5.

*lorsqu'une violation est détectée, y compris concernant la façon d'endiguer, de gérer et de remédier à l'incident, d'évaluer le risque et de notifier la violation. À cet égard, toujours afin de prouver leur conformité avec le RGPD, il pourrait être utile de démontrer que les employés ont été informés de l'existence de tels mécanismes et procédures et qu'ils savent comment réagir en cas de violation. »*

51. Le WP250rev.01 (p.31) conseille *« que le responsable du traitement documente également le raisonnement justifiant les décisions prises en réaction à la violation. En particulier, lorsqu'une violation n'est pas notifiée, la justification de cette décision devrait être documentée. Cette justification devrait inclure les raisons pour lesquelles le responsable du traitement considère que la violation est peu susceptible d'engendrer un risque pour les droits et libertés des individus. »*

52. En ce qui concerne précisément l'évaluation du risque pour les droits et libertés des individus présenté par une violation de données à caractère personnel, le WP250rev.01 (p.27) préconise que le responsable du traitement doit tenir compte des circonstances spécifiques de la violation, y compris la gravité des conséquences potentielles et la probabilité que celles-ci se produisent. Plus particulièrement, il recommande que l'évaluation tient compte des critères suivants: le type de violation, la nature, le caractère sensible et le volume des données à caractère personnel, la facilité d'identification des personnes concernées, la gravité des conséquences pour les personnes concernées, les caractéristiques particulières des personnes concernées et du responsable du traitement, ainsi que du nombre de personnes concernées.[18] En cas de doute, le responsable du traitement devrait opter pour la prudence et procéder à une notification (WP250rev.01 (p.29).

2. <u>En l'espèce</u>

53. Dans sa communication des griefs du 29 octobre 2019, le chef d'enquête a retenu qu'une *« divulgation de données sensibles, renseignant sur plusieurs pathologies sérieuses affligeant le plaignant, risque notamment de causer à ce dernier des dommages matériels ou moraux, tels qu'une discrimination, des pertes financières ou des dommages*

[18] Pour plus de détails, voir les pages 27 à 30 du WP250rev.01.

*économiques et sociaux importants si, par exemple, ces informations seraient publiées ou seraient transmises à d'autres tiers, voire à son employeur. Notons aussi qu'il s'agit également d'une perte de données qui étaient protégées aussi bien par le secret médical que par le secret des assurances et que le responsable du traitement, société d'assurance-vie est tenu à une obligation renforcée du respect de la confidentialité au vu des données très sensibles qu'il est amené à traiter ».* Il en a conclu que le contrôlé était dans l'obligation de notifier cette violation de données à caractère personnel à la CNPD et que dès lors il échet de retenir à son encontre une non-conformité aux prescrits de l'article 33.1 du RGPD. (Communication des griefs, p.5)

54. Dans son courrier de réponse à la communication des griefs du 29 novembre 2019, le contrôlé s'est référé à ses courriers antérieurs en soulignant de nouveau que, comme il a estimé que les informations divulguées par les deux courriers électroniques ne seraient pas à qualifier de données à caractère personnel et que donc, aucune violation de telles données n'aurait eu lieu, il s'en suit logiquement qu'il n'a pas non plus notifié cet incident à la CNPD.

55. La Formation Restreinte tient à souligner que l'article 33.1 indique clairement qu'une violation qui n'est « *pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques* » ne doit pas être notifiée à l'autorité de contrôle, mais doit uniquement être documentée dans le registre interne des violations des données.

56. Un des facteurs clés dans l'évaluation du risque est le type et le caractère sensible des données à caractère personnel qui ont été compromises par la violation. D'après le WP250rev.01 (p. 27), *« plus les données sont sensibles, plus le risque de dommage sera élevé pour les personnes concernées […].* »

57. En l'espèce, il convient de prendre en compte que les données divulguées aux personnes non autorisées relevaient des catégories particulières de données, et plus spécifiquement des données de santé[19] du réclamant, revêtant un caractère particulièrement « sensible » au regard de sa vie privée. Le traitement portant sur de telles

[19] Voir la définition des données concernant la santé prévue à l'article 4.15 du RGPD *: « données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne. »*

catégories particulières de données à caractère personnel est même spécifiquement encadré par l'article 9 du RGPD.

58. Alors qu'en général, plus le nombre de personnes concernées est élevé, plus les conséquences potentielles d'une violation sont nombreuses, la Formation Restreinte se rallie par ailleurs au WP250rev.01 (p. 29) qu'une *« violation peut cependant également avoir de graves conséquences ne serait-ce que pour une seule personne en fonction de la nature des données à caractère personnel et du contexte dans lequel elles ont été compromises. »* Par ailleurs, même si ce n'est qu'une quantité limitée de données à caractère personnel impliquée par la violation, en raison du caractère hautement sensible desdites données, les dommages potentiels pour le réclamant sont particulièrement graves, car la violation pourrait entraîner des dommages matériels ou moraux, tels qu'une discrimination, des pertes financières ou des dommages économiques et sociaux importants si, par exemple, ces informations seraient publiées ou seraient transmises à d'autres tiers, voire à son employeur.[20]

59. En ce qui concerne le volet « sécurité », développé plus en détail sous le point « D. Sur le manquement lié à l'obligation de garantir la sécurité des traitements de données à caractère personnel », il est important de souligner que *« si les données à caractère personnel ont été rendues incompréhensibles pour tout tiers non autorisé et si les données en question constituent une copie ou qu'il en existe une sauvegarde, une violation de la confidentialité portant sur des données à caractère personnel correctement cryptées ne doit pas être notifiée à l'autorité de contrôle. La raison en est qu'une telle violation est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. »* (WP250rev01, p.21). Or, la Formation Restreinte constate que les deux courriers litigieux n'ont pas du tout été protégés par des techniques garantissant une protection efficace selon l'état de l'art actuel, comme un chiffrement par encryptage ou l'utilisation de mots de passe solides et partagés séparément, d'autant plus que des informations particulièrement sensibles étaient contenues dans les courriers électroniques litigieux.

[20] Voir aussi le WP250rev.01, p.28.

60. Même *« lorsqu'une violation n'est pas notifiée, la justification de cette décision devrait être documentée. Cette justification devrait inclure les raisons pour lesquelles le responsable du traitement considère que la violation est peu susceptible d'engendrer un risque pour les droits et libertés des individus. »* (WP250rev.01 (p.31). La Formation Restreinte constate néanmoins que le document […] du contrôlé du 4 décembre 2018 n'est pas très détaillé et ne contient surtout pas d'explications pourquoi le contrôlé estimait que la violation n'engendrait pas de risque pour les droits et libertés du réclamant et que donc, aucune notification aurait été nécessaire.

61. Notons aussi que la « *nature et le rôle du responsable du traitement ainsi que de ses activités peuvent affecter le niveau de risque qu'engendre une violation pour les personnes concernées.* » (WP250rev.01 (p.29). En considérant que le contrôlé est une société d'assurance […] - vie et que les données à caractère personnel divulguées étaient tant protégées par le secret médical prévu par l'article 458 du Code pénal luxembourgeois, que par le secret professionnel des assurances conformément à l'article 300 de la loi modifiée du 7 décembre 2015 sur le secteur des assurances, le contrôlé était tenu à une obligation renforcée du respect de la confidentialité au vu des données très sensibles qu'il est amené à traiter.

62. Le CEPD conseille dans ce contexte dans ses lignes directrices 01/2021 sur des exemples en matière de notifications de violations de données du 14 janvier 2021 que si un courrier électronique a été envoyé à un destinataire non autorisé / erroné, le responsable du traitement devra envoyer un courrier additionnel audit destinataire demandant de supprimer le courrier litigieux.[21] La Formation Restreinte dispose néanmoins d'aucune documentation qui prouverait que le contrôlé a demandé aux destinataires non autorisés, c'est-à-dire aux propriétaires des adresses […] de supprimer les courriers électroniques litigieux. Lors de l'audience de la Formation Restreinte du 14 juillet 2021, le contrôlé a précisé que les propriétaires des adresses susmentionnées n'ont pas répondu aux deux courriers litigieux, mais que l'employée ayant envoyé lesdits courriers n'a pas eu de réponse comme quoi les adresses susmentionnées n'existaient

[21] Texte original, paragraphe 117 : *« If an email is sent to an incorrect/unauthorised recipient, it is recommended that the data controller should Bcc a follow up email to the unintended recipients apologising, instructing that the offending email should be deleted, and advising recipients that they do not have the right to further use the email addresses identified to them. »*

pas. Dès lors, sans aucune information sur les destinataires des deux courriers électroniques, ils ne peuvent pas être considérés comme « fiables », c'est-à-dire comme un destinataire envers lesquels le contrôlé aurait eu un certain degré de confiance « *de manière à pouvoir raisonnablement s'attendre à ce que ce dernier ne lise pas les données envoyées par erreur ou n'y accède pas et à ce qu'il satisfasse à sa demande de les lui renvoyer.* ». [22]

63. Au vu de de tous ces éléments, la Formation Restreinte conclut que les deux violations de données à caractère personnel en question étaient susceptibles d'engendrer un risque pour les droits et libertés du réclamant et que donc, le contrôlé aurait dû les notifier à la CNPD. Il échet dès lors de retenir à son encontre une non-conformité aux prescrits de l'article 33.1 du RGPD.

## C. Sur le manquement lié à l'obligation de communiquer à la personne concernée une violation de données à caractère personnel

### 1. Sur les principes

64. L'article 34 du RGPD prévoit ce qui suit :

*« 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:*

[22] Voir WP250rev.01 (p.29).

*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.*

*4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie. »*

65. Le considérant (86) du RGPD précise que la *« […] communication devrait décrire la nature de la violation des données à caractère personnel et formuler des recommandations à la personne physique concernée pour atténuer les effets négatifs potentiels. Il convient que de telles communications aux personnes concernées soient effectuées aussi rapidement qu'il est raisonnablement possible […]. »*

2. <u>En l'espèce</u>

66. Dans sa communication des griefs du 29 octobre 2019 (p.6), le chef d'enquête a estimé qu'alors *« même s'il est établi en l'espèce que le responsable du traitement a effectivement contacté le plaignant à deux reprises, il ne pourra pas être argué que les obligations de l'article 34 ont néanmoins été respectées. En effet, à part le fait que le responsable admet ne pas être en présence d'une violation de données à caractère personnel, les conditions du paragraphe (2) dudit article n'ont pas été respectées dans le cadre des communications effectuées avec la personne concernée. »* Il était ainsi d'avis

que le contrôlé se trouvait dans l'obligation de communiquer une violation de données à caractère personnel au réclamant, étant donné que cette violation présentait un risque élevé pour les droits et libertés de la personne concernée et qu'il a omis de le faire. Pour cette raison, le chef d'enquête a retenu à l'encontre du contrôlé une non-conformité aux prescrits de l'article 34.1 du RGPD.

67. Dans son courrier de réponse à la communication des griefs du 29 novembre 2019, le contrôlé a expliqué que, comme il a estimé que les informations divulguées par les deux courriers électroniques ne seraient pas à qualifier de données à caractère personnel et que donc, aucune violation de telles données n'aurait eu lieu, il n'a pas non plus communiqué la violation au réclamant dans les conditions de l'article 34 du RGPD. Par contre, il a estimé avoir toujours été transparent envers le réclamant en l'informant des incidents et que leur CEO et leur DPD lui ont expliqué le cas plus en détail.

68. La Formation Restreinte tient à souligner dans ce contexte que c'est uniquement lorsqu'une violation est susceptible d'engendrer un risque « élevé » pour les droits et libertés des personnes physiques que ces dernières doivent également être informées par le responsable du traitement. Le seuil à atteindre est par conséquent plus élevé pour la communication aux personnes concernées que pour la notification à l'autorité de contrôle. Alors que la notion de « risque élevé » n'est pas définie par le RGPD, le WP250rev.01 (p.26) précise qu'un tel risque élevé *« existe lorsqu'une violation est susceptible d'engendrer des dommages physiques, matériels ou un préjudice moral pour les personnes dont les données ont fait l'objet de la violation. Des exemples de tels dommages sont la discrimination, le vol ou l'usurpation d'identité, la perte financière ou l'atteinte à la réputation. Lorsque la violation implique […] des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes, de tels dommages sont considérés comme susceptibles de se produire.* » [23]

69. En se référant aux arguments développés aux points 55 à 63 de la présente décision, la Formation restreinte estime que les données à caractère personnel impliquées par les violations sont des données très sensibles concernant la santé du réclamant qui

[23] Voir aussi les considérants (75) et (85) du RGPD.

pourraient entraîner des dommages matériels ou moraux, tels qu'une discrimination, des pertes financières ou des dommages économiques et sociaux importants si, par exemple, ces informations seraient publiées ou seraient transmises à d'autres tiers, voire à son employeur. Elle est dès lors d'avis que les deux violations présentaient un risque élevé pour les droits et libertés du réclamant et que le contrôlé se trouvait dans l'obligation de lui les communiquer au sens de l'article 34.1 du RGPD. Conformément au paragraphe 2 dudit article, le responsable du traitement devrait au moins fournir les informations suivantes :

- une description de la nature de la violation ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact ;
- une description des conséquences probables de la violation ;
- une description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation, y compris, le cas échéant, des mesures pour en atténuer les éventuelles conséquences négatives.

70. En l'espèce, la Formation Restreinte constate que le 7 novembre 2018, presque trois semaines après l'envoi du premier courrier électronique litigieux du 19 octobre 2019, le réclamant a été informé par le contrôlé par mail que malheureusement une adresse erronée a été utilisée et que ce n'est qu'en date de ce jour que cette erreur a été découverte. En ce qui concerne le deuxième courrier litigieux du 29 novembre 2018, le réclamant en a été informé par mail du 3 décembre 2018 qui précisait que des envois erronés répétitifs ont eu lieu et que le DPD de l'assurance a été notifié. Il y était indiqué également que toutes les mesures seront prises pour éviter de tels incidents dans le futur. Par ailleurs, le CEO du contrôlé a proposé au réclamant par courriel du 27 février 2019 une conversation téléphonique pour discuter des incidents. Le DPD lui a envoyé par ailleurs un courrier électronique supplémentaire en date du 26 mars 2019 par lequel il a expliqué au réclamant que le contrôlé a considéré que, même si les données envoyées de manière erronée par les deux courriers électroniques auraient été lues par un tiers, elles ne seraient pas à qualifier de données à caractère personnel, et que donc il n'a pas considéré les incidents comme violations de données.

71. Même si la Formation restreinte considère qu'une certaine information du réclamant a eu lieu, elle estime néanmoins que les exigences de l'article 34.1 du RGPD

n'ont pas été respectées et que les communications au contrôlé ne contiennent pas les informations prévues au paragraphe 2 dudit article.

72. Au vu de ce qui précède, la Formation Restreinte conclut que l'article 34.1 du RGPD n'a pas été respecté par le contrôlé.

## D. Sur le manquement lié à l'obligation de garantir la sécurité des traitements de données à caractère personnel

### 1. Sur les principes

73. D'après l'article 5.1.f) du RGPD, les données à caractère personnel doivent être *« traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité). »*

74. 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 est tenu aux termes du paragraphe (1) de l'article 32 du RGPD de mettre *« 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 ; […] »*

### 2. En l'espèce

75. Dans son courrier du 8 août 2019, le contrôlé a exposé au chef d'enquête sa procédure de communication avec ses clients. Il y a expliqué que la communication par voie électronique se fait soit en utilisant un portail électronique […] soit par courrier électronique. Dans ce dernier cas, le contrôlé contacterait le client pour lui demander son consentement quant à la possibilité d'envoyer des courriers électroniques contenant des

données médicales sensibles par email et en cas de consentement, le personnel devrait limiter le contenu sensible au minimum. Par ailleurs, le contrôlé a également précisé dans ledit courrier que les pièces jointes aux courriers électroniques et contenant des informations sensibles seraient protégées par des mots de passe partagés séparément.

76. Le contrôlé est revenu sur la question de la protection des données en cas d'envoi de courriers électroniques dans un courrier du 17 septembre 2019, où il a expliqué que les mesures de sécurité détaillées dans son courrier précité du 8 août 2019 ne concerneraient uniquement des documents contenant des informations sensibles. Comme les questionnaires envoyés au réclamant étaient vides, ils ne contenaient, d'après le contrôlé, pas de telles informations et en sus, comme aucune personne liée à ces questionnaires n'était identifiable, une protection n'était pas nécessaire. Le courrier précité du 17 septembre 2019 contient par ailleurs en annexe le document […] et qui indique que dorénavant tous les courriers électroniques seraient envoyés d'une boîte mail commun, que tous les fichiers PDF seraient protégés par mots de passe et les noms seraient remplacés par des initiales.

77. Selon le chef d'enquête les informations contenues dans les courriers électroniques litigieux avaient, par contre, un caractère sensible et n'étaient *« manifestement pas protégées de manière adéquate afin de ne pas pouvoir être accédées ou lues par les destinataires incorrects des e-mails. Au vu du caractère particulièrement sensible des informations contenues dans les courriers électroniques litigieux, un chiffrement par encryptage ou toute technique garantissant une protection similaire aurait, selon l'état de l'art actuel et des bonnes pratiques applicables en la matière, dû être appliqué aux communications en l'espèce afin de garantir un niveau de sécurité adapté des risques d'atteinte à la vie privée de la personne concernée.* » (Communication des griefs, p.7). Il en conclue que le contrôlé n'a pas respecté son obligation de garantir la sécurité des traitements de données à caractère personnel et qu'il échet de retenir à son encontre une non-conformité aux prescrits des articles 5.1.f) et 32.1. a) et b) du RGPD.

78. Dans son courrier de réponse à la communication des griefs du 29 novembre 2019, le contrôlé a rappelé que, suite aux envois erronés, des mesures de sécurité additionnelles ont été mises en place afin d'éviter de tels incidents dans le futur. Il s'est référé de nouveau au [document] du 4 décembre 2018 en réitérant que dorénavant tous

les courriers électroniques seraient envoyés d'une boîte mail commun, que tous les fichiers PDF seraient protégés par mots de passe et les noms seraient remplacés par des initiales.

79. La Formation Restreinte note tout d'abord que le formulaire […] envoyé par le contrôlé par courrier du 17 septembre 2019[24] comporte en sa page […] la phrase suivante : « *I authorise […] to send emails containing sensitive medical information to the email address indicated below* » avec deux cases à cocher (« Yes » et « No »), dont la case « Yes » a été cochée, et une ligne […] sur laquelle le réclamant avait indiqué son adresse mail […].

80. Néanmoins, sans analyser si le consentement donné correspond aux exigences d'un consentement valable au sens de l'article 4.11 du RGPD, la signature d'une telle clause n'exonère en rien le contrôlé de ses obligations résultant des articles 5.1.f) et 32.1. a) et b) du RGPD cités ci-avant. La protection de la confidentialité et de la sécurité des données à caractère personnel constitue un enjeu encore plus important en cas de traitement de données sensibles (données de santé) dans la mesure où la divulgation de ces données pourrait causer un préjudice grave aux clients du contrôlé […].

81. La Formation Restreinte note par ailleurs que l'article 34.3 du RGPD prévoit dans ce contexte que la communication à la personne concernée d'une violation de données n'est pas nécessaire si *« 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 ».* Par exemple, en cas de violation de la confidentialité de données à caractère personnel qui ont été cryptées à l'aide d'un algorithme de pointe et que la confidentialité de la clé de cryptage est intacte, les données sont en principe incompréhensibles et la violation n'est donc pas susceptible de porter atteinte aux personnes concernées et n'aurait pas besoin de leur être communiquée.[25] Par ailleurs, le WP250 rev.01 contient des exemples concrets dans

[24] Voir annexe 3 du courrier du contrôlé du 17 septembre 2019.

[25] WP250 rev01. p. 21

lesquelles la notification d'une violation à l'autorité de contrôle est ou n'est pas obligatoire, en fonction des mesures de sécurité en place, telles que des moyens de cryptage sécurisés ou des mots de passe hachés et salés en mode sécurisé.[26]

82. Ces considérations témoignent de l'importance qu'a accordé le législateur européen, tout comme le CEPD aux mesures de sécurité qui peuvent, le cas échéant, permettre d'éviter une violation ou en cas de survenance, d'en mitiger les risques pour les droits et libertés des personnes physiques.

83. En considérant qu'en l'espèce, les courriers électroniques litigieux du 19 octobre 2018 et du 29 novembre 2018 ne contenaient pas uniquement en annexe des formulaires distincts à remplir relatifs aux pathologies du réclamant qui ont été déclarés auprès de son assurance, mais comprenaient en plus dans le corps du texte des indications et questions très détaillées quant aux pathologies très spécifiques dont est affecté le réclamant, la Formation Restreinte considère qu'indubitablement des données sensibles relatives à la santé du réclamant ont été divulguées par lesdits courriers.

84. De ce fait, un chiffrement par encryptage, des mots de passe ou toute technique garantissant une protection similaire selon l'état de l'art actuel et des bonnes pratiques applicables en la matière, auraient dû être appliqués aux communications en l'espèce afin de garantir un niveau de sécurité adapté aux risques d'atteinte à la vie privée de la personne concernée, surtout pour une entreprise comme celle du contrôlé. Néanmoins, comme l'envoi des deux courriers électroniques litigieux n'était protégé par aucune mesure technique permettant notamment de garantir la confidentialité des messages et documents transmis, la Formation Restreinte estime que le contrôlé n'a pas respecté ses obligations en matière de sécurité prévues aux articles 5.1.f) et 32.1. a) et b) du RGPD. Si de telles mesures de sécurité auraient été en place dès le départ, les violations de données à caractère personnel auraient même pu être évitées, ou au moins, leurs conséquences auraient pu être mitigées.

85. Au vu de ce qui précède, la Formation Restreinte conclut que les articles 5.1.f) et 32.1. a) et b) du RGPD n'ont pas été respectés par le contrôlé.

[26] Voir pour les détails WP250 rev01. p. 20 à 22.

**E. Sur le manquement lié à l'obligation de communication des coordonnées du délégué à la protection des données à l'autorité de contrôle**

1. Sur les principes

86. Aux termes de l'article 31.1 du RGPD, le responsable du traitement et le sous-traitant doivent obligatoirement désigner un DPD lorsque :

*« a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;*

*b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou*

*c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10. »*

87. L'article 37.7 du RGPD prévoit dans ce contexte que *« le responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'autorité de contrôle. »*

88. Les obligations en la matière ont été explicitées par le Groupe de Travail Article 29 dans ses lignes directrices concernant les délégués à la protection des données (DPD) dont la version révisée a été adoptée le 5 avril 2017. A noter que le CEPD a repris et réapprouvé les documents adoptés par ledit Groupe entre le 25 mai 2016 et le 25 mai 2018, comme précisément les lignes directrices précitées sur le DPD.[27]

2. En l'espèce

[27] Voir décision Endorsement 1/2018 du CEPD du 25 mai 2018, disponible sous : https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

89. Lors de la visite sur place du 29 juillet 2019, il a été affirmé aux agents de la CNPD que […] absent lors de l'enquête sur place, a été désigné comme DPD. Cependant, les agents de la CNPD ont constaté que la désignation de ce dernier n'a pas fait l'objet d'une notification à la CNPD telle que prévue à l'article 37.7 du RGPD et qu'aucune explication par rapport à cette omission n'a été fournie.[28]

90. Par courrier du 23 juillet 2019, le contrôlé a précisé que le DPD était à l'étranger lors de la visite sur place des agents de la CNPD et a affirmé que […] a été désigné DPD de la société début 2018.

91. Dans la communication des griefs du 29 octobre 2019, le chef d'enquête a néanmoins estimé que les coordonnées du DPD désigné par le contrôlé n'ont pas été communiquées en bonne et due forme à la CNPD et que l'information quant à la désignation du DPD dans la lettre du contrôlé du 23 juillet 2019 *« n'est pas de nature à énerver ce constat, alors que ni les informations à minima à transmettre, ni la procédure prévue par la CNPD n'ont été respectées. »*

92. Dans son courrier de réponse à la communication des griefs du 29 novembre 2019, le contrôlé a réitéré que les coordonnées du DPD ont été révélées aux agents de la CNPD lors de leur visite sur place et dans son courrier du 23 juillet 2019. Il a noté par ailleurs que l'article 37.7 du RGPD exige uniquement que les coordonnées du DPD sont communiquées à l'autorité de contrôle, sans imposant un formalisme particulier à respecter. Pour la communication des coordonnées du nouveau DPD, le contrôlé a indiqué avoir utilisé le formulaire mis à disposition par la CNPD.

93. La Formation Restreinte estime dans ce contexte que le formulaire mis à disposition sur le site de la CNPD et permettant de transmettre les coordonnées du DPD à la CNPD vise uniquement à faciliter ce processus pour les responsables du traitement / sous-traitants, tout en permettant d'éviter de devoir demander des informations éventuellement manquantes. Par contre, la communication des coordonnées du DPD par un autre moyen de communication, par exemple par courrier postal, est tout à fait

[28] Voir constat 1 du procès-verbal no. […]/2019 relatif à la mission d'enquête sur place effectuée en date du 19 juillet 2019 auprès de la Société A.

acceptable, pourvu que les informations nécessaires, comme détaillées dans ledit formulaire, y sont incluses.

94. Néanmoins, elle constate qu'au moment de la visite sur site par les agents de la CNPD en date du 29 juillet 2019, c'est-à-dire plus qu'une année après l'entrée en application du RGPD, les coordonnés du DPD du contrôlé n'avaient pas été communiquées, par quelque moyen que ce soit, à la CNPD.

95. Au vu de ce qui précède, la Formation Restreinte conclut qu'au moment de la visite sur site par les agents de la CNPD, l'article 37.7 du RGPD n'était pas respecté par le contrôlé.

## II. 2. Sur les mesures correctrices et amendes

### 1. Les principes

96. Conformément à l'article 12 de la loi du 1er août 2018, la CNPD dispose du pouvoir d'adopter toutes les mesures correctrices prévues à l'article 58.2 du RGPD :

*« a) avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du présent règlement ;*

*b) rappeler à l'ordre un responsable du traitement ou un sous-traitant lorsque les opérations de traitement ont entraîné une violation des dispositions du présent règlement ;*

*c) ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits en application du présent règlement ;*

*d) ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du présent règlement, le cas échéant, de manière spécifique et dans un délai déterminé ;*

*e) ordonner au responsable du traitement de communiquer à la personne concernée une violation de données à caractère personnel;*

*f) imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement ;*

*g) ordonner la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement en application des articles 16, 17 et 18 et la notification de ces mesures aux destinataires auxquels les données à caractère personnel ont été divulguées en application de l'article 17, paragraphe 2, et de l'article 19 ;*

*h) retirer une certification ou ordonner à l'organisme de certification de retirer une certification délivrée en application des articles 42 et 43, ou ordonner à l'organisme de certification de ne pas délivrer de certification si les exigences applicables à la certification ne sont pas ou plus satisfaites ;*

*i) imposer une amende administrative en application de l'article 83, en complément ou à la place des mesures visées au présent paragraphe, en fonction des caractéristiques propres à chaque cas ;*

*j) ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale. »*

97. Conformément à l'article 48 de la loi du 1er août 2018, la CNPD peut imposer des amendes administratives telles que prévues à l'article 83 du RGPD, sauf à l'encontre de l'État ou des communes.

98. L'article 83 du RGPD prévoit que chaque autorité de contrôle veille à ce que les amendes administratives imposées soient, dans chaque cas, effectives, proportionnées et dissuasives, avant de préciser les éléments qui doivent être pris en compte pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de cette amende :

*« a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi ;*

*b) le fait que la violation a été commise délibérément ou par négligence ;*

*c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ;*

*d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en oeuvre en vertu des articles 25 et 32 ;*

*e) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant ;*

*f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs ;*

*g) les catégories de données à caractère personnel concernées par la violation ;*

*h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation;*

*i) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures ;*

*j) l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42 ; et*

*k) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation* ».

99. La Formation Restreinte tient à préciser que les faits pris en compte dans le cadre de la présente décision sont ceux constatés au début de l'enquête. Les éventuelles modifications relatives aux traitements de données faisant l'objet de l'enquête intervenues

ultérieurement, même si elles permettent d'établir entièrement ou partiellement la conformité, ne permettent pas d'annuler rétroactivement un manquement constaté.

100. Néanmoins, les démarches effectuées par le contrôlé pour se mettre en conformité avec le RGPD au cours de la procédure d'enquête ou pour remédier aux manquements relevés par le chef d'enquête dans la communication des griefs, sont prises en compte par la Formation Restreinte dans le cadre des éventuelles mesures correctrices et/ou de la fixation du montant d'une éventuelle amende administrative à prononcer.

2. En l'espèce

2.1. Quant à l'imposition d'une amende administrative

101. Dans son courrier complémentaire à la communication des griefs du 15 décembre 2020, le chef d'enquête proposait à la Formation Restreinte d'infliger une amende administrative au contrôlé d'un montant de 275.000 euros.

102. Dans sa réponse audit courrier complémentaire du 27 janvier 2021, le contrôlé a estimé que sur base des critères prévus à l'article 83.2 du RGPD, le montant proposé par le chef d'enquête était disproportionné. Il a notamment fait valoir que la prétendue violation ne concernait qu'une seule personne par l'envoi d'uniquement deux courriers électroniques erronés, que la violation n'aurait pas duré dans le temps et que la personne concernée n'aurait subi aucun dommage. Par ailleurs, la prétendue violation n'aurait été que le résultat d'une erreur humaine regrettable, mais n'aurait pas été intentionnelle et pas liée au manque de supervision par le contrôlé en matière de protection des données.

103. Afin de décider s'il y a lieu d'imposer une amende administrative et pour décider, le cas échéant, du montant de cette amende, la Formation Restreinte prend en compte les éléments prévus par l'article 83.2 du RGPD :

- Quant à la nature et à la gravité de la violation (article 83.2.a) du RGPD), la Formation Restreinte relève qu'en ce qui concerne le manquement à l'article 5.1.f) du RGPD, il est constitutif d'un manquement aux principes fondamentaux du RGPD (et du droit de la protection des données en général), à savoir au principe d'intégrité et de confidentialité consacré au Chapitre II « Principes » du RGPD.

Quant au manquement de ne pas avoir mis en place les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, conformément à l'article 32.1 du RGPD, la Formation Restreinte considère que face aux risques représentés par les violations de données à caractère personnel, le législateur européen a entendu renforcer les obligations des responsables de traitement en matière de sécurité des traitements. Ainsi, selon le considérant (83) du RGPD et afin de « *de garantir la sécurité et de prévenir tout traitement effectué en violation du présent Règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents au traitement et mette en œuvre des mesures pour les atténuer, telles que le chiffrement. Ces mesures devraient assurer un niveau de sécurité approprié, y compris la confidentialité, compte tenu de l'état des connaissances et des coûts de mise en œuvre par rapport aux risques et à la nature des données à caractère personnel à protéger. […]* . Or, en considérant que les deux courriers électroniques litigieux n'ont pas été protégés par des techniques garantissant une protection efficace selon l'état de l'art actuel, comme un chiffrement par encryptage ou l'utilisation de mots de passe solides, d'autant plus que des informations particulièrement sensibles étaient contenues dans les courriers électroniques litigieux, la Formation Restreinte estime que le contrôlé n'a pas mesuré à sa juste valeur l'importance de la sécurisation des données personnelles contenues dans ses systèmes.

En considérant par ailleurs que le contrôlé est un acteur […] dans le secteur de l'assurance-vie avec […] employés au Luxembourg[29] et […][30] et que les données à caractère personnel divulguées étaient tant protégées par le secret médical prévu par l'article 458 du Code pénal luxembourgeois, que par le secret professionnel des assurances conformément à l'article 300 de la loi modifiée du 7 décembre 2015 sur le secteur des assurances, le contrôlé était tenu à une obligation renforcée du respect de la confidentialité au vu des données très sensibles qu'il est amené à traiter.

[29] Voir […]

[30] Voir […]

Quant au manquement de n'avoir pas documenté les violations de données à caractère personnel en interne et ne les avoir pas notifiées à la CNPD, ni communiquées à la personne concernée, la Formation Restreinte observe que lesdits manquements trouvaient leur origine dans une interprétation erronée, aux yeux du chef d'enquête et de la Formation Restreinte, de deux notions de base de la protection des données, c'est-à-dire les notions de « données à caractère personnel » et de « violations de données à caractère personnel » au sens des articles 4 points 1) et 12) du RGPD. Or, en tant que société d'assurance-vie traitant à grande échelle des données sensibles de ses clients, le contrôlé aurait dû avoir les connaissances nécessaires en la matière pour pouvoir procéder à une qualification correcte des faits.

- Quant au critère de durée (article 83.2.a) du RGPD), la Formation Restreinte constate que les manquements aux articles 5.1.f), 32.1. a) et b), 33.1, 33.5 et 34.1 du RGPD ont duré dans le temps, à tout le moins depuis la première violation des données du 19 octobre 2019 et jusqu'au jour de la visite sur place, tandis que la violation de l'article 37.7 du RGPD a duré du 25 mai 2018 jusqu'au moins au jour de la visite sur place. La Formation Restreinte rappelle ici que deux ans ont séparé l'entrée en vigueur du RGPD de son entrée en application pour permettre aux responsables de traitement de se conformer aux obligations qui leur incombent. D'autant plus, une obligation comparable de mettre en œuvre les mesures techniques et organisationnelles appropriées en fonction du risque d'atteinte à la vie privée, ainsi que de l'état de l'art et des coûts liés à leur mise en œuvre existait déjà en application des articles 22 et 23 de la loi abrogée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

- Quant au nombre de personnes concernées (article 83.2.a) du RGPD), la Formation relève qu'en général, plus le nombre de personnes concernées est élevé, plus les conséquences potentielles d'une violation sont nombreuses. Par contre, elle estime qu'en l'espèce, la violation peut également avoir de graves conséquences ne serait-ce que pour une seule personne, c'est-à-dire le réclamant, en raison de la nature des données à caractère personnel et du contexte dans

lequel elles ont été compromises. Ainsi, en raison du caractère hautement sensible desdites données, les dommages potentiels pour le réclamant sont particulièrement graves, car la violation pourrait entraîner des dommages matériels ou moraux, tels qu'une discrimination, des pertes financières ou des dommages économiques et sociaux importants si, par exemple, ces informations seraient publiées ou seraient transmises à d'autres tiers, voire à son employeur.

Par ailleurs, la Formation Restreinte estime que comme les manquements constatés s'inscrivent dans la pratique quotidienne du contrôlé et sont consécutifs à l'absence de mise en place de mesures de sécurité adéquates en cas d'envoi de données sensibles par courrier électronique, un grand nombre d'autres personnes, au-delà du seul réclamant, sont potentiellement impactées par lesdits manquements. En effet, comme les données en cause n'étaient identifiées par le contrôlé ni comme données à caractère personnel, ni comme données sensibles (données de santé) au sens de l'article 9 du RGPD, il y a un risque que beaucoup d'autres cas où des clients ont opté pour l'envoi de données médicales sensibles par courrier électronique et où les mesures de sécurité étaient aussi insuffisantes, n'ont pas été détectés par le contrôlé.

La Formation Restreinte est donc d'avis que le nombre de personnes potentiellement concernées est élevé.

– Quant à la question de savoir si les manquements ont été commis délibérément ou non (par négligence) (article 83.2.b) du RGPD), la Formation Restreinte rappelle que « non délibérément » signifie qu'il n'y a pas eu d'intention de commettre la violation, bien que le responsable du traitement ou le sous-traitant n'ait pas respecté l'obligation de diligence qui lui incombe en vertu de la législation.

En l'espèce, la Formation Restreinte est d'avis que les faits et les manquements constatés ne traduisent pas une intention délibérée de violer le RGPD dans le chef du contrôlé. Par contre, étant donné que des données à caractère personnel très sensibles ont été envoyées à deux reprises à des tiers non autorisés, une certaine négligence est à retenir.

- Quant aux mesures prises par le contrôlé pour atténuer le dommage subi par les personnes concernées (article 83.2.c) du RGPD), la Formation Restreinte tient compte des mesures prises par le contrôlé et renvoie au chapitre II.2. section 2.2. de cette décision pour les explications y afférentes.

- Quant au degré de responsabilité du responsable du traitement, compte tenu des mesures techniques et organisationnelles qu'il a mise en œuvre en vertu des articles 25 et 32 (article 83.2.d) du RGPD), la Formation Restreinte prend en compte que les deux courriers litigieux n'ont pas été protégés par des techniques garantissant une protection efficace selon l'état de l'art actuel, comme un chiffrement par encryptage ou l'utilisation de mots de passe, d'autant plus que des informations particulièrement sensibles étaient contenues dans les courriers électroniques litigieux.

- Quant aux catégories de données à caractère personnel concernées par la violation (article 83.2.g) du RGPD), il convient de prendre en compte que les données divulguées aux personnes non autorisées relevaient des catégories particulières de données, et alors qu'il s'agissait plus spécifiquement des données de santé du réclamant, revêtant un caractère particulièrement « sensible » au regard de sa vie privée.

- Quant à la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation (article 83.2.h) du RGPD), la Formation Restreinte tient à renvoyer aux points 55 à 63 de la présente décision où elle est parvenue à la conclusion que le contrôlé aurait dû notifier les violations à la CNPD, mais ne l'a pas fait. Ainsi, la violation est venue à la connaissance de la CNPD par l'introduction d'une réclamation de la personne concernée.

104. La Formation Restreinte constate que les autres critères de l'article 83.2 du RGPD ne sont ni pertinents, ni susceptibles d'influer sur sa décision quant à l'imposition d'une amende administrative et son montant.

105. S'agissant du manquement à l'obligation de notifier les violations de données à la CNPD, en application de l'article 33.1 du RGPD, la Formation Restreinte considère que ce manquement est lié à la base à une interprétation juridique erronée des événements par le contrôlé. En effet, comme il a estimé que les informations divulguées par les deux courriers électroniques ne seraient pas à qualifier de données à caractère personnel et que donc, aucune violation de telles données n'aurait eu lieu, il s'en suit dans sa logique qu'il n'avait pas non plus besoin de notifier ces incidents à la CNPD. Elle considère dès lors, qu'au regard des circonstances de l'espèce, il n'y a pas lieu d'assoir son amende sur le fondement de ce manquement, bien qu'il soit caractérisé.

106. S'agissant du manquement à l'obligation de communiquer les violations de données à la personne concernée, en application de l'article 34.1 du RGPD, la Formation Restreinte considère qu'une information partielle du réclamant a eu lieu, d'une part, et que ce manquement est aussi lié à la base à une interprétation juridique erronée des événements par le contrôlé, d'autre part. En effet, comme il a estimé que les informations divulguées par les deux courriers électroniques ne seraient pas à qualifier de données à caractère personnel et que donc, aucune violation de telles données n'aurait eu lieu, il s'en suit dans sa logique qu'il n'y avait pas non plus lieu de communiquer ces incidents à la personne concernée conformément à l'article 34.1 du RGPD. Elle considère dès lors, qu'au regard des circonstances de l'espèce, il n'y a pas lieu d'assoir son amende sur le fondement de ce manquement, bien qu'il soit caractérisé.

107. S'agissant du manquement à l'obligation de communiquer les coordonnés de contact à l'autorité de contrôle, en application de l'article 37.7 du RGPD, la Formation Restreinte considère que l'obligation essentielle est d'avoir désigné pour le 25 mai 2018 un DPD en cas d'application d'une des trois conditions prévues à l'article 37.1 du RGPD. En effet, le DPD occupe une place fondamentale au sein du cadre juridique créé par le RGPD. Elle considère dès lors, comme le contrôlé avait désigné début 2018 un DPD, mais avait uniquement omis de communiquer ses coordonnées à la CNPD, qu'il n'y a pas lieu d'assoir son amende sur le fondement de ce manquement, bien qu'il soit caractérisé.

108. La Formation Restreinte relève aussi que si plusieurs mesures ont été mises en place par le contrôlé afin de remédier en totalité ou en partie à certains manquements, celles-ci n'ont été adoptées qu'à la suite du contrôle des agents de la CNPD en date du 19 juillet 2019 (voir aussi le point 99 de la présente décision).

109. Dès lors, la Formation restreinte considère que le prononcé d'une amende administrative est justifié au regard des critères posés par l'article 83.2 du RGPD pour manquement aux articles 5.1.f), 32.1. a) et b) et 33.5 du RGPD.

110. S'agissant du montant de l'amende administrative, la Formation Restreinte rappelle que le paragraphe 3 de l'article 83 du RGPD 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 un manquement à l'article 5 du RGPD est reproché au contrôlé, le montant maximum de l'amende pouvant être retenu s'élève à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

111. Au regard des critères pertinents de l'article 83.2 du RGPD évoqués ci-avant et en prenant en considération la taille du contrôlé et les informations sur ses finances […] la Formation Restreinte considère que le prononcé d'une amende de cent trente-cinq mille euros (135.000 euros) apparaît à la fois effectif, proportionné et dissuasif, conformément aux exigences de l'article 83.1 du RGPD.

2.2. Quant à la prise de mesures correctrices

112. L'adoption des mesures correctrices suivantes, qui devraient être implémentées dans un délai de trois mois, sous peine d'astreintes à hauteur de 750 euros par jour de retard, a été proposée par le chef d'enquête à la Formation Restreinte dans son courrier complémentaire à la communication des griefs du 15 décembre 2020:

*« a) Ordonner au responsable du traitement de documenter toute violation de données à caractère personnel, par exemple au moyen d'un « registre des violations » ;*

*b) Ordonner au responsable du traitement de notifier toute violation de données à caractère personnel à la CNPD, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques ;*

*c) Ordonner au responsable du traitement de notifier, dans les meilleurs délais, toute violation de données à caractère personnel à la personne concernée lorsque la*

*violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique ;*

*d) Ordonner au responsable du traitement de mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris le chiffrement des données à caractère personnel relevant de l'article 9 du RGPD, afin de garantir leur confidentialité ;*

*e) Ordonner au responsable du traitement de publier les coordonnées du délégué à la protection des données désigné et de les communiquer à la CNPD. »*

113. Dans sa réponse audit courrier complémentaire du 27 janvier 2021, le contrôlé renvoyait à son courrier du 29 novembre 2019 dans lequel il avait pris position par rapport à tous les manquements mentionnés dans la communication des griefs. Par ailleurs, il a mentionné que toutes les mesures correctrices proposées par le chef d'enquête seraient déjà implémentées. Ainsi, chaque violation de données serait inscrite dans […] y inclus les incidents en cause, et serait notifiée à la CNPD (à moins qu'il n'y a pas de risque pour les droits et libertés des personnes concernées) et à la personne concernée (à moins qu'il n'y a pas de risque élevé pour les droits et libertés des personnes concernées). Par ailleurs, des mesures de sécurité seraient mises en place et les coordonnées du DPD ont été publiées sur leur site et communiquées à la CNPD par courrier du 11 octobre 2019.

114. Quant aux mesures correctrices proposées par le chef d'enquête et par référence au point 100 de la présente décision, la Formation Restreinte prend en compte les démarches effectuées par le contrôlé, suite à la visite des agents de la CNPD, afin de se conformer aux dispositions des articles 5.1.f), 32.1. a) et b), 33.1, 33.5, 34.1 et 37.7 du RGPD, comme détaillées dans ses courriers du 23 juillet 2019, du 8 août 2019, du 17 septembre 2019, du 29 novembre 2019, ainsi que du 29 janvier 2021. Plus particulièrement, elle prend note des faits suivants :

- Quant à l'obligation de documenter en interne toute violation de données à caractère personnel, de les notifier, le cas échéant, à la CNPD, et de les communiquer, le cas échéant, aux personnes concernées, la Formation Restreinte note que dorénavant, le contrôlé inscrit chaque violation de données dans un […] y inclus les incidents en cause, les notifie à la CNPD (à moins qu'il n'y a pas de risque pour les droits et libertés des personnes concernées) et à la personne

concernée (à moins qu'il n'y a pas de risque élevé pour les droits et libertés des personnes concernées).

Par ailleurs, la Formation Restreinte constate que depuis la première notification d'une violation de données reçue par le contrôlé en date du 11 octobre 2019, une vingtaine de violations de données a été notifiée à la CNPD.

En considération des mesures de mise en conformité prises par le contrôlé en l'espèce et le point 100 de la présente décision, la Formation Restreinte considère dès lors qu'il n'y a pas lieu de prononcer les mesures correctrices proposées par le chef d'enquête et reprises sous a), b) et c) du point 112 ci-avant.

- Quant à l'obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris le chiffrement des données à caractère personnel relevant de l'article 9 du RGPD, afin de garantir leur confidentialité, le contrôlé a indiqué que des mesures de sécurité auraient été mises en place, comme par exemple l'envoi de courriers électroniques d'une boîte mail commun, protection de l'envoi des fichiers PDF par mots de passe, remplacement des noms par des initiales et chiffrement des données à caractère personnel visées par l'article 9 du RGPD.

  Néanmoins, la Formation Restreinte ne dispose pas de la documentation permettant de démontrer la mise en œuvre de ces mesures de mise en conformité par le contrôlé. Elle considère dès lors qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête et reprise sous d) du point 112 ci-avant.

- Quant à l'obligation de publier les coordonnées du DPD désigné et de les communiquer à la CNPD, la Formation Restreinte constate que les coordonnées du DPD ont été publiées sur le site du contrôlé et communiquées à la CNPD par une déclaration reçue le 17 octobre 2019.

  En considération des mesures de mise en conformité prises par le contrôlé en l'espèce et le point 100 de la présente décision, la Formation Restreinte considère dès lors qu'il n'y ait pas lieu de prononcer la mesure correctrice proposée par le chef d'enquête et reprise sous e) du point 112 ci-avant.

La Formation Restreinte estime par ailleurs qu'il n'y a pas lieu d'infliger une astreinte au contrôlé pour le contraindre à respecter ces mesures correctrices.

**Compte tenu des développements qui précèdent, la Commission nationale siégeant en formation restreinte et délibérant à l'unanimité des voix décide :**

- de retenir les manquements aux articles 5.1.f), 32.1. a) et b), 33.1, 33.5, 34.1 et 37.7 du RGPD ;

- de prononcer à l'encontre de la Société A une amende administrative d'un montant de cent trente-cinq mille euros (135.000 euros) au regard des manquements constitués aux articles 5.1.f), 32.1. a) et b) et 33.5 du RGPD ;

- de prononcer à l'encontre de la Société A une injonction de mettre en conformité le traitement avec les articles 5.1.f) et 32.1. a) et b) du RGPD dans un délai de deux mois suivant la notification de la décision de la Formation restreinte, en particulier :

- protéger l'envoi de courriers électroniques contenant des catégories particulières de données au sens de l'article 9 du RGPD par des mesures de sécurité appropriées, comme le chiffrement par encryptage, des mots de passe solides et partagées séparément ou par toute autre technique garantissant une protection similaire selon l'état de l'art actuel et des bonnes pratiques applicables en la matière.

Ainsi décidé à Belvaux en date du 5 août 2021.

Pour la Commission nationale pour la protection des données siégeant en formation restreinte

| | | |
|---|---|---|
| Tine A. Larsen | Thierry Lallemang | Christophe Buschmann |
| Présidente | Commissaire | Commissaire |

## Indication des voies de recours

La présente décision administrative peut faire l'objet d'un recours en réformation dans les trois mois qui suivent sa notification. Ce recours est à porter devant le tribunal administratif et doit obligatoirement être introduit par le biais d'un avocat à la Cour d'un des Ordres des avocats.