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

Délibération n° 22FR/2022 du 13 décembre 2022

La Commission nationale pour la protection des données siégeant en formation restreinte, composée de Madame Tine A. Larsen, présidente, et de Messieurs Thierry Lallemang et Alain Herrmann, 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 10.2 ;

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. Lors de sa séance de délibération du 17 juillet 2020, la Commission nationale siégeant en formation plénière (ci-après : la « Formation Plénière ») a 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 : la « loi du 1er août 2018 ») et de désigner Monsieur Christophe Buschmann comme chef d'enquête.

   Ladite décision a précisé que l'enquête menée par la Commission nationale pour la protection des données (ci- après : la « CNPD » ou la « Commission nationale ») avait pour objet de contrôler l'application et le respect du RGPD et de la loi du 1er août 2018, et plus précisément la conformité aux articles 12.1, 13 et 14 du RGPD.

2. La Société A est [...] inscrit au Registre du Commerce et des Sociétés de Luxembourg sous le numéro [...], avec siège social à L - [...], [...] (ci-après : le « contrôlé »).

   Le contrôlé [est actif dans l'exploitation de portails internet et l'offre de services via ces portails].

3. La décision de la Commission nationale siégeant en formation restreinte (ci-après: la « Formation Restreinte ») sur l'issue de l'enquête se basera :

   - sur les traitements effectués par le contrôlé en rapport avec l'exploitation du site internet [de la Société A] (ci-après : le « site internet ») et contrôlés par les agents de la CNPD ; et

   - sur les dispositions légales et réglementaires prises en compte par le chef d'enquête dans sa communication des griefs.

   Le contrôlé a précisé qu'il n'opère pas d'application mobile.[1]

4. Par courrier du 26 août 2020, le chef d'enquête a envoyé un questionnaire préliminaire. Ce moment est référencé ultérieurement dans cette décision comme « au début de l'enquête ». Le contrôlé a répondu par courriel du 22 septembre 2020. Après une visite sur

[1] Voir page 7 du questionnaire préliminaire rempli.

place qui a eu lieu le 9 octobre 2020, le contrôlé et le service d'enquêtes de la CNPD ont procédé à un échange de courriers.[2]

5. Suite à cet échange, le chef d'enquête a établi le Rapport d'enquête n° [...] fondé sur la délibération du 17 juillet 2020 portant sur la conformité aux articles 12 point 1, 13 et 14 du RGPD daté au 29 avril 2021 (ci-après : le « rapport d'enquête »).

   Il ressort du rapport d'enquête[3] qu'afin de structurer les travaux d'enquête, le chef d'enquête a défini neuf objectifs de contrôle, à savoir :

   1) S'assurer que les informations sont disponibles ;

   2) S'assurer que les informations sont complètes ;

   3) S'assurer que l'absence d'une information est motivée par une exception valide ;

   4) S'assurer que les informations sont transmises selon des moyens appropriés ;

   5) S'assurer que les informations sont concises, transparentes, compréhensibles, et transmises en des termes clairs et simples ;

   6) S'assurer que les informations sont adaptées à la catégorie de personnes concernées ;

   7) S'assurer que les informations sont gratuites ;

   8) S'assurer que les informations sont aisément accessibles ; et

   9) S'assurer que les informations sont transmises lors des étapes-clé du traitement.

   Il est précisé dans le rapport d'enquête que les agents de la CNPD n'ont pas contrôlé « *la légalité des traitements effectués par le contrôlé* ». Dans ce contexte, il est donné l'exemple suivant : « *dans le cas où le responsable du traitement informe les personnes concernées que leurs données à caractère personnel sont conservées pendant un délai de 2 ans, les agents de la CNPD pourront vérifier que le responsable du traitement ne conserve pas lesdites données pour une durée différente. En revanche, les agents de la*

[2] Cf. Communication des griefs, point 9 pour une liste détaillée des échanges tout au long de l'enquête.
[3] Rapport d'enquête, page 7, point « *3.1 Objectifs de contrôle* ».

CNPD ne se prononceront pas quant à la légalité de ce délai de 2 ans appliqué par le responsable du traitement. »[4]

L'enquête s'est par ailleurs focalisée sur les utilisateurs du site internet et n'a pas visé d'autres catégories de personnes concernées telles que les salariés du contrôlé.[5] Les utilisateurs sont en l'espèce les clients […] « de la Société A » et plus précisément […].[6]

Le rapport d'enquête a pour annexe les pièces recueillies par le service d'enquêtes de la CNPD et sur lesquelles le rapport d'enquête est basé (annexe 1), ainsi que le compte-rendu de la visite sur place des agents de la CNPD du 9 octobre 2020 précitée (annexe 2) (ci-après : le « Compte-Rendu »).

6. Lors de sa séance de délibération du 23 juillet 2021 la Formation Plénière a désigné Monsieur Marc Lemmer, commissaire, comme chef d'enquête en remplacement de Monsieur Christophe Buschmann, démissionnaire.

7. A l'issue de son instruction, le chef d'enquête a notifié au contrôlé en date du 13 janvier 2022 une communication des griefs (ci-après : « communication des griefs ») détaillant les manquements qu'il estimait constitués en l'espèce par rapport aux exigences prescrites par les articles 12.1 (obligation de transparence) et 13 du RGPD (droit à l'information).

   Le chef d'enquête a proposé à la Formation Restreinte d'adopter sept mesures correctrices différentes, ainsi que d'infliger au contrôlé une amende administrative d'un montant de 1.700 euros.

8. Le contrôlé a répondu à la communication des griefs par courrier du 10 février 2022.

9. Par courrier du 20 mai 2022, la présidente de la Formation Restreinte a informé le contrôlé que son affaire serait inscrite à la séance de la Formation Restreinte du 13 juillet 2022 et qu'il pouvait assister à cette séance. Le contrôlé a confirmé sa présence à ladite séance en date du 21 juin 2022.

10. Lors de cette séance le chef d'enquête, Monsieur Marc Lemmer, était présent. Le contrôlé était représenté par [...]. Le chef d'enquête et le représentant du contrôlé ont exposé leurs observations orales à l'appui de leurs observations écrites et ont répondu aux questions

[4] Rapport d'enquête, page 7, point « *2.3 Réserves* ».
[5] Rapport d'enquête, page 6, point « *2.2 Périmètre* ».
[6] Rapport d'enquête, page 9, point *« 4.2 Description du contrôlé* ».

posées par la Formation Restreinte. La Formation Restreinte a donné au contrôlé la possibilité d'envoyer endéans une semaine des informations complémentaires demandées lors de ladite séance. Le contrôlé a eu la parole en dernier.

11. Par courriel du 13 juillet 2022, le contrôlé a envoyé les informations complémentaires demandées par la Formation Restreinte le même jour.

II. En droit

II. 1. Sur les motifs de la décision

A. Sur le manquement lié à l'obligation de transparence

1. Sur les principes

12. Aux termes de l'article 12.1 du RGPD, le « *responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique. Lorsque la personne concernée en fait la demande, les informations peuvent être fournies oralement, à condition que l'identité de la personne concernée soit démontrée par d'autres moyens.* »

13. La transparence constitue un aspect fondamental des principes relatifs au traitement des données à caractère personnel.[7] Les obligations en la matière ont été explicitées par le Groupe de Travail Article 29 dans ses lignes directrices sur la transparence au sens du règlement (UE) 2016/679, dont la version révisée a été adoptée le 11 avril 2018 (ci-après : « WP 260 rév.01 » ou les « les lignes directrices sur la transparence »).

Ces lignes directrices explicitent en particulier les règles générales de transparence établies par l'article 12 du RGPD, et qui sont applicables à la communication d'informations aux personnes concernées (articles 13 et 14 du RGPD), aux communications adressées aux personnes concernées au sujet de l'exercice de leurs droits (articles 15 à 22 du

[7] Voir notamment les articles 5.1.a) et 12 du RGPD, voir aussi les considérants (39), (58) à (60) du RGPD.

RGPD), et aux communications concernant les violations de données (article 34 du RGPD).[8]

Elles soulignent également qu'un « *aspect primordial du principe de transparence mis en lumière dans ces dispositions est que la personne concernée devrait être en mesure de déterminer à l'avance ce que la portée et les conséquences du traitement englobent afin de ne pas être prise au dépourvu à un stade ultérieur quant à la façon dont ses données à caractère personnel ont été utilisées.* »[9]

14. A noter que le Comité européen de la protection des données (ci-après : le « CEPD »), qui a succédé au Groupe de Travail Article 29 le 25 mai 2018, 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 la transparence.[10]

2. En l'espèce

2.1. Quant à l'exigence de fournir les informations d'une façon « concise et transparente »

15. Dans le cadre de l'objectif 2[11] le chef d'enquête s'est attendu, entre autres, à ce que « *les informations suivantes soient accessibles à travers la politique de protection des données, conformément à l'annexe de la guidance du Groupe de Travail Article 29 relative aux informations devant être communiquées à une personne concernée au titre de l'article 13 ou de l'article 14 du RGPD :*

[…] - Les coordonnées du DPD (si désigné) (cf. Test 2), […]

- La période de conservation des données ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette période (cf. Tests 8 et 21), […]. »

Les agents de la CNPD ont dès lors inspecté la politique de confidentialité de la Société A disponible sur le site internet du contrôlé et dont la dernière mise à jour au moment de l'analyse par les agents de la CNPD datait du […] 2018[12] (ci-après : la « politique de confidentialité ») et ont constaté qu'il y était indiqué que le contrôlé avait nommé un

[8] WP 260 rév.01, point 7.
[9] WP 260 rév.01, point 10.
[10] 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.
[11] « *Objectif 2 - S'assurer que les informations sont complètes* » ; Rapport d'enquête, page 15 et s.
[12] Voir pièce 1 annexée au rapport d'enquête.

délégué à la protection des données (ci-après : « DPD »). Par contre, *« il s'avère, après entretien des agents de la CNPD auprès du gérant de la Société A, que ces informations sont erronées. En effet, la Société A n'a pas nommé de DPD (cf. Test 2) […]. »*[13]

Par ailleurs, les agents de la CNPD ont comparé *« la durée de rétention indiquée dans la politique relative à la protection des données (ou le cas échéant les précisions disponibles dans le registre des traitement) avec la configuration du système respectivement la donnée la plus vieille disponible. […] Concernant un des cookies il a été constaté que la durée de rétention était de 2 ans i.e. bien supérieure à celle indiquée dans la politique de protection des données et ceci avec ou sans acceptation de l'utilisateur (PIECE 16, […]).»*[14]

16. Dans le cadre de l'objectif 5[15] le chef d'enquête s'est attendu, entre autres, à ce que *« la politique de protection des données reflète la réalité des traitements effectivement mis en place, c'est-à-dire sans anticipation de traitements qui pourraient éventuellement être mis en place par le contrôlé dans le futur (cf. Test 5) ».*

Dans ce contexte, les agents de la CNPD ont *« inspecté la politique de protection des données pour vérifier qu'elle reflète la réalité des traitements effectivement mis en place, c'est-à-dire sans anticipation de traitements qui pourraient éventuellement être mis en place par le contrôlé dans le futur. Pour ce faire, les agents de la CNPD ont comparé le contenu de la politique de protection des données avec les explications obtenues du contrôlé lors de l'entretien du 09/10/2020. »*[16] Ils se sont rendus compte lors de cette inspection qu'un traitement indiqué dans la politique de confidentialité n'était en réalité pas effectué, en l'occurrence le profilage. Suite aux entretiens menés auprès du contrôlé en date du 9 octobre 2020, les agents de la CNPD ont noté qu'un tel traitement n'était en réalité pas réalisé, mais mentionné dans la politique de protection des données pour anticiper l'intégration de futures activités. Or, il ressort du rapport d'enquête qu' *« il est attendu que la politique de protection des données reflète la réalité des traitements effectivement mis en place, c'est-à-dire sans anticipation de traitements qui pourraient éventuellement être mis en place par le contrôlé dans le futur. »*[17]

---

[13] Rapport d'enquête, page 28, point « *4.4.2.3.1 Inexactitude de l'information ».*
[14] Rapport d'enquête, page 28, point *« 4.4.2.2.20 Test 21 : Vérification de la durée de rétention ».*
[15] « Objectif 5 - S'assurer que les informations sont concises, transparentes, compréhensibles, et transmises en des termes clairs et simples » ; Rapport d'enquête, page 35 et s.
[16] Rapport d'enquête, page 38, point *« 4.4.5.2.5 Test 5 : Mise en place vs. Anticipation ».*
[17] Rapport d'enquête, page 38, point *« 4.4.5.2.5 Test 5 : Mise en place vs. Anticipation. »*

17. Par ailleurs, les *« agents de la CNPD ont inspecté le site internet et la politique de protection des données de la Société A pour évaluer le caractère concis et transparent des informations communiquées, ainsi que l'efficacité et le caractère succinct de leur présentation. »*[18]

    Ils ont constaté dans ce contexte concernant les durées de conservation *« une incohérence entre la durée de conservation indiquée dans la politique de protection des données (6 mois après la dernière utilisation des données personnelles) et celle du registre de traitement (jusqu'à la clôture du compte). »*[19]

18. Dans la communication des griefs, le chef d'enquête a dès lors constaté que certaines informations contenues dans la politique de protection des données du contrôlé ne reflétaient pas la réalité, car la politique faisait référence à l'utilisation de la technique de profilage non mise en place par le contrôlé et elle indiquait que le contrôlé avait nommé un DPD, alors que ce n'était pas le cas au moment de la visite de la CNPD.[20]

    Par ailleurs, le chef d'enquête a fait référence aux deux cas « *pour lesquels il existe une différence entre la durée de rétention indiquée dans la politique de confidentialité et la durée de rétention effectivement appliquée.*

    Le premier cas concerne la politique cookies qui indique que sans action de la part de l'utilisateur, les cookies ont une durée de vie limitée à 13 mois maximum, cette durée n'étant pas prolongée automatiquement lors des nouvelles visites sur le site. Les agents de la CNPD ont toutefois constaté que la durée de rétention d'un des cookies ([…]) était en réalité de 2 ans, contrairement à ce qui est indiqué dans la politique.

    Le deuxième cas concerne la politique de protection des données qui mentionne une durée de rétention de 6 mois après la dernière connexion de l'utilisateur sur le site alors qu'en réalité, les données relatives aux commandes des clients sont supprimées après clôture du compte de l'utilisateur, comme indiqué dans le registre des traitements. »[21]

    Ainsi, le chef d'enquête a retenu que *« les conditions de l'article 12.1 du RGPD quant à la loyauté et la transparence de l'information n'ont pas été respectées ».*[22]

[18] Rapport d'enquête, page 36, point *« 4.4.5.2.1 Test 1 : Concis et transparent ».*
[19] Rapport d'enquête, page 36, point *« 4.4.5.2.1 Test 1 : Concis et transparent ».*
[20] Communication des griefs, point 18.
[21] Communication des griefs, point 18.
[22] Communication des griefs, points 20.

19. La Formation Restreinte rappelle que l'article 12.1 du RGPD exige entre autres que les informations requises soient fournies d'une façon concise et transparente.

    Elle relève que les lignes directrices sur la transparence indiquent que *« l'exigence que la fourniture d'informations aux personnes concernées et que les communications qui leur sont adressées soient réalisées d'une manière « concise et transparente » signifie que les responsables du traitement devraient présenter les informations/communications de façon efficace et succincte afin d'éviter de noyer d'informations les personnes concernées. »*[23]

20. La Formation Restreinte constate que la politique de confidentialité mentionnait dans la partie […] ce qui suit : *« […]. Ce traitement implique une technique de profilage. »*[24]

    Toutefois, même si c'était indiqué dans la politique de confidentialité, il ressort du Compte-Rendu que le contrôlé ne procédait pas à des analyses comportementales, c'est-à-dire au profilage et que *« cette discordance était due au fait qu'au moment de la rédaction de la politique de protection des données, la Société A ne connaissait encore pas précisément son périmètre d'action. »*[25]

21. Elle constate de même que la politique de confidentialité mentionnait que le contrôlé avait nommé un DPD, alors qu'il avait précisé lors de la visite sur place du 9 octobre 2020 *« qu'il n'y avait à proprement parler pas de DPD « officiel ». Selon les articles 37 à 39 du RGPD et l'analyse interne effectuée par l'organisme, la Société A a conclu que la nomination d'un DPD n'était pas requise.»*[26]

22. La Formation Restreinte considère dès lors que la fourniture d'informations aux utilisateurs qui correspondent à des traitements qui ne sont pas effectués, c'est-à-dire le profilage, ou qui ne reflètent pas la réalité, donc la mention erronée de la nomination d'un DPD, semait confusion et faisait obstacle à ce que les informations requises soient présentées aux utilisateurs du site internet de façon efficace et succincte.

23. Elle relève par ailleurs que les lignes directrices sur la transparence indiquent qu'un « *aspect primordial du principe de transparence mis en lumière dans ces dispositions est que la personne concernée devrait être en mesure de déterminer à l'avance ce que la portée et les conséquences du traitement englobent afin de ne pas être prise au dépourvu*

[23] WP 260 rév.01, point 8.
[24] Voir page 2 de la politique de confidentialité.
[25] Compte-rendu du 9 octobre 2020, page 9.
[26] Compte-rendu du 9 octobre 2020, page 8.

à un stade ultérieur quant à la façon dont ses données à caractère personnel ont été utilisées. »[27] Il en résulte que le responsable du traitement doit fournir aux personnes concernées des informations exactes et complètes sur l'intégralité des traitements effectués sur leurs données à caractère personnel.

24. La Formation Restreinte constate à cet égard qu'il y a une différence entre la durée de rétention indiquée dans la politique de confidentialité pour les données à caractère personnel de l'utilisateur *(« six mois à compter de la dernière connexion sur le Site »*) et la durée de rétention mentionnée dans le registre des activités de traitements du contrôlé (ci-après : le « registre »).[28] En effet, d'après le registre, la suppression des données[29] n'a lieu qu'après la clôture du compte du client, sauf pour les données comptables qui sont sauvegardées pendant 10 ans.[30] Il en résulte que le contrôlé n'a pas fourni d'informations exactes sur l'intégralité des traitements effectués sur les données à caractère personnel des utilisateurs, et plus précisément sur la durée de conservation des données à caractère personnel des utilisateurs.

25. Au vu de ce qui précède, la Formation Restreinte se rallie dès lors à l'avis du chef d'enquête qu'au début de l'enquête de la CNPD[31] il y avait un manquement à l'obligation de transparence découlant de l'article 12.1 du RGPD et au regard de l'article 13.1.b) et 13.2.a) du RGPD, et plus précisément à l'exigence de fournir les informations requises d'une façon concise et transparente.

26. Quant aux mesures prises par le contrôlé après la visite sur place des agents de la CNPD, la Formation Restreinte y revient au point 64, ainsi qu'au Chapitre II.2, Section 2.2 de cette décision.

27. Finalement, en ce qui concerne la durée de rétention d'un des cookies (« […] »), la Formation Restreinte rappelle que le dépôt ou la lecture d'informations sur l'équipement terminal de l'utilisateur sont encadrés par la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques (ci-après : « loi modifiée du 30 mai 2005 »). Si l'utilisation de cookies mène en plus dudit dépôt ou de la lecture d'informations sur l'équipement terminal de l'utilisateur « *à la collecte (ou à tout*

[27] WP 260 rév.01, point 10.
[28] Voir Pièce 9 annexée au rapport d'enquête.
[29] Il s'agit des données suivantes : Nom, Prénom, Adresse, Mot de passe (en cas de création d'un compte).
[30] Il s'agit des données suivantes : Données comptables/administratives […].
[31] Communication des griefs, point 20.

autre traitement) de données à caractère personnel (par exemple, lorsque les cookies sont utilisés afin de collecter des données sur les préférences d'achat d'un utilisateur déterminé), l'ensemble des règles du RGPD sera en outre à respecter, ce qui implique notamment que le traitement devra reposer sur une condition de licéité distincte (article 6 du RGPD) et qu'une information conforme aux articles 12 à 14 du RGPD devra être fournie à la personne concernée ».[32]

En effet, la jurisprudence de la Cour de justice de l'Union européenne[33] a confirmé qu'il est possible que le traitement relève à la fois du champ d'application matériel de la directive « vie privée et communications électroniques »[34] et de celui du RGPD.[35]

Or, comme le contrôle de l'application et du respect de la loi susmentionnée du 30 mai 2005 n'était pas dans le périmètre de l'enquête en cause, la Formation Restreinte ne statue pas dans la présente décision sur la conformité du contrôlé par rapport aux exigences posées par cette loi.

2.2. Quant à l'exigence de fournir les informations d'une façon « aisément accessible »

28. Dans le cadre de l'objectif 4[36] le chef d'enquête s'est attendu, entre autres, à ce « *que toutes les mises à jour substantielles de la politique de protection des données fassent l'objet d'une communication active (e-mail informatif, pop-up sur le site internet, etc.) avec un résumé des (principales) modifications (cf. Test 5). »*[37]

Les agents de la CNPD ont constaté qu'il *« a été précisé au cours des entretiens menés qu'en cas d'évolution de la politique de protection des données, la Société A en informerait les utilisateurs par email, ce qui est en contradiction avec les indications de la politique de protection des données qui précise qu'il est de la responsabilité des utilisateurs de*

[32] Lignes directrices de la CNPD en matière de cookies et d'autres traceurs, point 2., disponibles sous : https://cnpd.public.lu/fr/dossiers-thematiques/cookies/contexte-juridique.html.
[33] Affaire « Planet 49 », CJUE, C-673/17, 1er octobre 2019, points 42 et 65.
[34] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, telle que modifiée.
[35] CEPD, Avis 5/2019 relatif aux interactions entre la directive « vie privée et communications électroniques » et le RGPD, en particulier en ce qui concerne la compétence, les missions et les pouvoirs des autorités de protection des données, adopté le 12 mars 2019, point 30. et s.
[36] « *Objectif 4 - S'assurer que les informations sont transmises selon des moyens appropriés*; Rapport d'enquête, page 32 et s.
[37] Rapport d'enquête, page 31, Ad Objectif 4, point *« 4.4.4.1 Attentes ».*

s'informer quant aux éventuels changements de la politique de protection des données (cf. Test 5). »[38]

29. Pour cette raison, le chef d'enquête a retenu que les *« conditions de l'article 12, paragraphe 1 du RGPD quant à l'accessibilité de l'information (au niveau des mises à jour) n'ont pas été respectées. »*[39]

30. La Formation Restreinte se réfère dans ce contexte aux lignes directrices sur la transparence indiquant que le *« critère «aisément accessible» signifie que la personne concernée ne devrait pas avoir à rechercher les informations mais devrait pouvoir tout de suite y accéder […] »* et que le *« responsable du traitement devrait respecter les mêmes principes lorsqu'il communique l'avis ou la déclaration initial(e) sur la protection de la vie privée et toute modification substantielle apportée ultérieurement à cet avis ou à cette déclaration »* et *« qu'une notification de modification devrait toujours être communiquée par un moyen adapté (par exemple, e-mail, courrier postal, fenêtre contextuelle sur une page web ou autre moyen captant efficacement l'attention de la personne concernée) spécifiquement consacré à la modification (par exemple, séparée d'un contenu de marketing direct), et cette communication doit respecter les prescriptions de l'article 12 […]. Les mentions contenues dans l'avis ou la déclaration sur la protection de la vie privée indiquant que la personne concernée devrait régulièrement vérifier l'avis ou la déclaration sur la vie privée afin d'en connaître les éventuelles modifications ou mises à jour sont jugées non seulement insuffisantes. »*[40]

    Elle rappelle que *« le responsable du traitement devrait également, lors de la notification de modifications aux personnes concernées, leur expliquer l'incidence que ces modifications pourraient avoir sur elles. »*[41]

31. La Formation Restreinte constate que, même s'il ressort du rapport d'enquête que le contrôlé avait prévu d'informer les utilisateurs par mail en cas de future mise à jour de la politique de confidentialité[42], ladite politique mentionnait que les *« […]»*[43]

[38] Rapport d'enquête, page 34, point *« 4.4.4.3.3 Informations contradictoires ».*
[39] Communication des griefs, point 26.
[40] WP 260 rév.01, points 11 et 29.
[41] WP 260 rév. 01, point 31.
[42] Rapport d'enquête, page 33, point « 4.4.4.2.5 Test 5 ».
[43] Voir pièce 1 annexée au rapport d'enquête, point « […] ».

D'après la politique de confidentialité, les utilisateurs n'étaient donc pas systématiquement informés de manière active en cas de modification substantielle de ladite politique.

32. Elle estime dès lors que le contrôlé a manqué au début de l'enquête de la CNPD à l'obligation de transparence découlant de l'article 12.1 du RGPD, et plus précisément à l'exigence de fournir les informations requises d'une façon aisément accessible.

2.3. Quant aux exigences de fournir les informations d'une façon « compréhensible » et « en des termes clairs et simples »

2.3.1 Au niveau de la traduction

33. Dans le cadre de l'objectif 5[44] le chef d'enquête s'est attendu, entre autres, à ce que *« la politique de protection des données soit disponible dans les mêmes langues que celles proposées sur le site web, à savoir les langues de la clientèle ciblée par les services du contrôlé (cf. Test 3)*»[45].

Les agents de la CNPD ont alors inspecté *« la politique de protection des données pour identifier l'existence d'une traduction dans les mêmes langues que celles pour lesquelles le site est disponible. »*[46]

34. De la communication des griefs il ressort dans ce contexte que *« les agents de la CNPD ont constaté que la politique n'existe qu'en langue française alors que le site est disponible en allemand et en français.»*[47]

Ainsi, le chef d'enquête a retenu que les conditions de l'article 12.1 du RGPD quant au caractère compréhensible de l'information (au niveau de la traduction) n'ont pas été respectées.[48]

35. La Formation Restreinte rappelle que l'article 12.1 du RGPD exige entre autres que les informations requises doivent être fournies d'une façon compréhensible. Elle relève que les lignes directrices sur la transparence indiquent que « *l'exigence que ces informations soient « compréhensibles » signifie qu'elles devraient pouvoir être comprises par la*

[44] « *Objectif 5 - S'assurer que les informations sont concises, transparentes, compréhensibles, et transmises en des termes clairs et simples* » ; Rapport d'enquête, page 37 et s.
[45] Rapport d'enquête, page 36, Ad Objectif 5, point *« 4.4.5.1 Attentes ».*
[46] Rapport d'enquête, page 37, Ad Objectif 5, point *« 4.4.5.2.3 Test 3 Traduction ».*
[47] Communication des griefs, point 30
[48] Communication des griefs, point 32.

majorité du public visé. La compréhensibilité est étroitement liée à l'exigence d'utiliser des termes clairs et simples. Un responsable du traitement connaît les personnes au sujet desquelles il collecte des informations et peut mettre à profit ces connaissances pour déterminer ce que ce public serait susceptible de comprendre. »[49]

36. En ce qui concerne l'exigence susmentionnée de fournir les informations requises en des termes clairs et simples, les lignes directrices sur la transparence indiquent plus spécifiquement qu'une *« traduction dans une ou plusieurs langues devrait être fournie lorsque le responsable du traitement cible des personnes concernées parlant ces langues. »*[50]

37. La Formation Restreinte estime donc, comme le site internet du contrôlé était disponible en français et allemand, le contrôlé aurait dû prévoir des versions de la politique de confidentialité dans ces deux langues. Or, ladite politique n'était disponible qu'en français. Comme le contrôlé n'avait dès lors pas fourni aux utilisateurs germanophones de son site internet une politique de confidentialité en allemand, il ne leur avait pas fourni les informations requises sous une forme facilement compréhensible.

38. Au vu de ce qui précède, la Formation Restreinte se rallie à l'avis du chef d'enquête et conclut qu'au début de l'enquête de la CNPD, le contrôlé a manqué à l'obligation de transparence découlant de l'article 12.1 du RGPD, et plus précisément aux exigences de fournir les informations requises d'une façon compréhensible et en des termes clairs et simples.

2.3.2. Au niveau des destinataires

39. En ce qui concerne l'objectif 5[51] le chef d'enquête a rappelé les informations relatives aux destinataires ou catégories de destinataires qui doivent être fournies au titre des articles 13 et 14 du RGPD selon l'annexe aux lignes directrices sur la transparence.

Les agents de la CNPD ont alors inspecté la politique de confidentialité du contrôlé et ont « *noté que certaines informations décrites dans la politique de protection des données manquaient de transparence :*

[49] WP 260 rév.01, point 9.
[50] WP 260 rév.01, point 13.
[51] « Objectif 5 - S'assurer que les informations sont concises, transparentes, compréhensibles, et transmises en des termes clairs et simples » ; Rapport d'enquête, page 35 et s.

- L'identité des sous-contractants de la Société A (les destinataires des données) n'est pas précisée dans la politique de protection des données. […]. »[52]

40. Dans la communication des griefs, il est précisé par le chef d'enquête que les *« agents de la CNPD ont constaté que les informations relatives aux sous-contractants ne sont pas suffisamment précises. En effet, la politique de protection des données indique que « […]». L'identité des sous-contractants de la Société A (ou tout au moins une liste des différentes catégories de sous-contractants) n'est pas précisée dans la politique, si bien qu'il est difficile pour les personnes concernées de comprendre qui détient leurs données. »*

    Pour cette raison, le chef d'enquête était d'avis que *« les conditions de l'article 12, paragraphe 1 du RGPD quant au caractère compréhensible de l'information (au niveau des destinataires) n'ont pas été respectées ».*[53]

41. La Formation Restreinte réitère que l'article 12.1 du RGPD exige entre autres que les informations requises doivent être fournies d'une façon compréhensible. Elle relève que les lignes directrices sur la transparence indiquent que « *l'exigence que ces informations soient « compréhensibles » signifie qu'elles devraient pouvoir être comprises par la majorité du public visé. La compréhensibilité est étroitement liée à l'exigence d'utiliser des termes clairs et simples. Un responsable du traitement connaît les personnes au sujet desquelles il collecte des informations et peut mettre à profit ces connaissances pour déterminer ce que ce public serait susceptible de comprendre.* »[54]

    Elle rappelle par ailleurs que conformément à l'article 4.9) du RGPD le destinataire vise *: « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. (…) ».*

    Le WP 260 précise dans ce contexte qu'un *« destinataire n'est pas nécessairement un tiers. Par conséquent, les autres responsables du traitement, responsables conjoints du traitement et sous-traitants auxquels les données sont transférées ou communiquées sont*

[52] Rapport d'enquête, page 37, point *« 4.4.5.2.1 Test 1 : Concis et transparent ».*
[53] Communication des griefs, points 35 et 38.
[54] WP 260 rév.01, point 9.

couverts par le terme « destinataire » et des informations relatives à ces destinataires devraient être fournies en plus des informations relatives aux autres destinataires tiers. »[55]

Aux termes de l'article 13.1.e) du RGPD, le contrôlé doit par ailleurs, le cas échéant, fournir des informations sur les destinataires ou des informations sur les catégories de destinataires des données à caractère personnel, et qu'à cet égard les lignes directrices sur la transparence précisent entre autres que « *les destinataires réels (nommément désignés) des données à caractère personnel ou les catégories de destinataires doivent être indiqués. Conformément au principe d'équité, les responsables du traitement doivent fournir aux personnes concernées les informations les plus significatives sur les destinataires. En pratique, il s'agit généralement de destinataires nommément désignés afin que les personnes concernées puissent savoir exactement qui détient leurs données à caractère personnel. Si les responsables du traitement choisissent de communiquer les catégories de destinataires, les informations devraient être les plus spécifiques possible et indiquer le type de destinataire (en fonction des activités qu'il mène), l'industrie, le secteur et le sous-secteur ainsi que l'emplacement des destinataires.*»[56]

42. La Formation Restreinte constate dans ce contexte que la section […] de la politique de confidentialité du contrôlé mentionnait que chaque *« […] ».* Il ressort donc de ladite politique que des données à caractère personnel des utilisateurs pourraient être transmises à des destinataires dans le cadre des paiements et des livraisons.

Néanmoins, d'après le registre du contrôlé[57] il y avait, en sus des deux catégories de destinataires des données à caractère personnel des utilisateurs du site internet mentionnées dans la politique de confidentialité, trois autres catégories de destinataires : un prestataire d'hébergement des bases de données de la Société A dénommé [...] , les […] et un prestataire d'envoi de mailing dénommé [...].

43. Elle estime donc que le contrôlé n'avait pas fourni aux utilisateurs de son site internet une information complète sur les catégories de destinataires de leurs données à caractère personnel.

[55] WP 260 rév.01, Annexe « Informations devant être communiquées à une personne concernée au titre de l'article 13 ou de l'article 14 ».
[56] WP 260 rév.01, Annexe « *Informations devant être communiquées à une personne concernée au titre de l'article 13 ou de l'article 14* ».
[57] Pièce 9 annexée au rapport d'enquête. Voir notamment les fiches […].

44. Au vu de ce qui précède, la Formation Restreinte se rallie à l'avis du chef d'enquête et conclut qu'au début de l'enquête de la CNPD, le contrôlé a manqué à l'obligation de transparence découlant de l'article 12.1 du RGPD et au regard de l'article 13.1.e) du RGPD, et plus particulièrement aux exigences de fournir les informations requises d'une façon compréhensible et en des termes clairs et simples.

B. Sur le manquement lié à l'obligation d'informer les personnes concernées

1. Sur les principes

45. L'article 13 du RGPD prévoit ce qui suit :

« *1. Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes les informations suivantes :*

a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ;

b) le cas échéant, les coordonnées du délégué à la protection des données ;

c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;

d) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ;

e) les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent ; et

f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1, deuxième alinéa, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition ;

2. En plus des informations visées au paragraphe 1, le responsable du traitement fournit à la personne concernée, au moment où les données à caractère personnel sont obtenues,

les informations complémentaires suivantes qui sont nécessaires pour garantir un traitement équitable et transparent :

a) la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

b) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données ;

c) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point a), ou sur l'article 9, paragraphe 2, point a), l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;

d) le droit d'introduire une réclamation auprès d'une autorité de contrôle ;

e) des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données ;

f) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

3. Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au paragraphe 2.

4. Les paragraphes 1, 2 et 3 ne s'appliquent pas lorsque, et dans la mesure où, la personne concernée dispose déjà de ces informations. »

46. La communication aux personnes concernées d'informations relatives au traitement de leurs données est un élément essentiel dans le cadre du respect des obligations générales de transparence au sens du RGPD.[58] Lesdites obligations ont été explicitées par le Groupe de Travail Article 29 dans ses lignes directrices sur la transparence qui ont été reprises et réapprouvées par le CEPD.

47. Pour le surplus, la Formation Restreinte se réfère aux points 12 à 15 de la présente décision en ce qui concerne les principes à respecter en vertu de l'obligation de transparence conformément à l'article 12.1 du RGPD.

2. En l'espèce

48. Dans le cadre de l'objectif 2[59] le chef d'enquête s'est attendu, entre autres, à ce que « *les informations suivantes soient accessibles à travers la politique de protection des données, conformément à l'annexe de la guidance du Groupe de Travail Article 29 relative aux informations devant être communiquées à une personne concernée au titre de l'article 13 ou de l'article 14 du RGPD :*

[…] - La/les finalités et la base juridique du traitement (il est attendu que la base juridique spécifique du traitement soit renseignée et non pas simplement la liste des bases juridiques qui existent sous le RGPD) (cf. Test 3), […]

- Les transferts vers des pays tiers le cas échéant (cf. Tests 7 et 19), […]

- Les droits des personnes concernées : […] droit de retirer son consentement à tout moment. […]. »

49. A titre préliminaire, en ce qui concerne l'information sur les bases juridiques des cookies et leur transfert vers des pays tiers, la Formation Restreinte tient à préciser que comme le contrôle de l'application et du respect de la loi modifiée du 30 mai 2005 n'était pas dans le périmètre de l'enquête en cause, la Formation Restreinte ne statue pas dans la présente décision sur la conformité du contrôlé avec les exigences posées par cette loi.

[58] Voir notamment les articles 5.1.a) et 12 du RGPD, voir aussi le considérant (39) du RGPD.
[59] « *Objectif 2 - S'assurer que les informations sont complètes* » ; Rapport d'enquête, page 15 et s.

2.1. Quant aux bases juridiques du traitement

50. Il ressort du rapport d'enquête que même si *« les finalités de traitement soient clairement mentionnées dans la politique de protection des données, les bases juridiques ne sont pas indiquées, ni dans la politique (PIECE 1), ni dans le registre de traitements (PIECE 9). »*[60]

    Pour ces raisons, le chef d'enquête a retenu dans la communication des griefs que *« les conditions de l'article 13, paragraphe 1, lettre c) du RGPD quant aux bases juridiques des traitements n'ont pas été respectées. »*[61]

51. La Formation Restreinte constate qu'en effet les bases juridiques des traitements de données n'étaient pas indiquées dans la politique de confidentialité ou dans le registre du contrôlé.

    Le contrôlé n'a dès lors pas fourni aux utilisateurs de son site internet toutes les informations rendues obligatoires par l'article 13.1.c) du RGPD.

2.2. Quant aux transferts de données vers un pays tiers

52. Les agents de la CNPD ont constaté que dans la politique de confidentialité, le contrôlé *« n'indique pas transférer de données personnelles vers des pays tiers ou des organisations internationales (PIECE 1, pages 2 et 3).*

    Les agents de la CNPD ont toutefois constaté, au cours des entretiens menés avec la Société A, que des données étaient transférées à [...] *(prestataire de paiement en ligne, […]) et à* [...] *(prestataire d'envoi de courriels […]). […] Il existe donc bien des transferts vers des pays tiers, qui ne sont pas mentionnés dans la politique de protection des données. »*[62]

    Pour ces raisons, le chef d'enquête a retenu dans la communication des griefs que *« les conditions de l'article 13, paragraphe 1, lettre f) du RGPD quant à l'information sur les transferts de données vers des pays tiers n'ont pas été respectées. »*[63]

[60] Rapport d'enquête, page 17, point *« 4.4.2.2.3 Test 3 : Finalités et bases juridiques ».*
[61] Communication des griefs, point 47.
[62] Rapport d'enquête, page 19, point *« 4.4.2.2.7 Test 7 : Transferts vers des pays tiers - registre ».*
[63] Communication des griefs, point 51.

53. La Formation Restreinte constate en effet que la politique de confidentialité indiquait que le contrôlé *« ne transfère pas de données personnelles vers un pays tiers, ni vers une organisation internationale »*[64], alors qu'il ressort du Compte-rendu[65], tout comme du registre du contrôlé que des données à caractère personnels étaient transférées [vers des pays tiers] à ses prestataires de paiement en ligne ([...]) et d'envoi de courriels ([...]).

    Le contrôlé n'a dès lors pas fourni aux utilisateurs de son site internet toutes les informations rendues obligatoires par l'article 13.1.f) du RGPD.

2.3. Quant au droit de retirer son consentement

54. Les agents de la CNPD ont inspecté la politique de confidentialité du contrôlé pour identifier la présence d'informations relatives aux droits des personnes concernées incluant un résumé de ce que comprennent les droits en question et les mesures pouvant être prises par la personne concernée pour les exercer ainsi que toute limitation auxdits droits.[66]

    Ils ont constaté dans ce contexte *« qu'un consentement était demandé pour l'envoi de newsletters au moment de l'inscription d'un nouveau client. A ce niveau, il existe un lien vers la politique de protection des données, mais la politique ne mentionne pas le droit pour un utilisateur de retirer son consentement à tout moment. »*[67]

55. Le chef d'enquête a pris en compte dans la communication des griefs *« que l'utilisateur peut modifier son consentement relatif à l'envoi de newsletters à tout moment en changeant les paramètres de son compte. Il peut également se désinscrire de la newsletters en cliquant sur le lien de désinscription se trouvant en bas de l'email. »*

    Il a néanmoins retenu dans que *« les conditions de l'article 13, paragraphe 2, lettre c) du RGPD quant à l'information sur le droit de retirer son consentement n'ont pas été respectées. »*[68]

56. La Formation Restreinte rappelle que l'obligation de mentionner l'existence du droit de retirer son consentement à tout moment s'impose uniquement lorsque le traitement par le

[64] Politique de confidentialité, page 3.
[65] Voir page 5 qui indique ce qui suit : *« La Société A a recours aux sous-traitants suivants : […]* - […] *(paiements en ligne, […]) ;* - […] *(prestataire d'envoi de courriels, […]) […]. »*
[66] Rapport d'enquête, page 20, point *« 4.4.2.2.9 Test 9 : Droits des personnes concernées (utilisateurs)».*
[67] Communication des griefs, point 54.
[68] Communication des griefs, points 55 et 56.

responsable du traitement est fondé sur l'article 6.1.a) ou 9.2.a) du RGPD, c'est-à-dire si la base juridique du traitement est le consentement de la personne concernée.

En l'espèce, comme indiqué au point 51 de la présente décision, ni la politique de confidentialité, ni le registre du contrôlé ne mentionnait les bases juridiques des différents traitements opérés. La Formation Restreinte constate néanmoins qu'il était documenté par une capture d'écran envoyée par le contrôlé que lorsqu'un utilisateur souhaitait créer un compte, il devait activement cocher une case s'il voulait recevoir la newsletter.[69] Par ailleurs, d'autres captures d'écrans envoyés par le contrôlé ont montré la possibilité pour un utilisateur de s'abonner activement sur le site internet du contrôlé à sa newsletter et que dans ce cas, un mail de confirmation d'inscription sur la liste d'envoi de la newsletter lui a été envoyé.[70]

Sur base de ce qui précède, la Formation Restreinte conclut que la base juridique du traitement de données à caractère personnel opéré dans le cadre de l'envoi de la newsletter était le consentement de l'utilisateur et que dès lors, le contrôlé était obligé d'informer ledit utilisateur sur l'existence du droit de retirer son consentement à tout moment.

57. En l'espèce, la Formation Restreinte prend note qu'au moment de la création d'un compte par un utilisateur, un lien vers la politique de confidentialité était disponible. Par contre, même si un utilisateur pouvait toujours modifier son consentement relatif à l'envoi de la newsletter en changeant les paramètres de son compte[71], ladite politique ne mentionnait pas l'existence du droit de retirer son consentement à tout moment.

Par ailleurs, au cas où un utilisateur s'abonnait activement sur le site internet du contrôlé à sa newsletter, aucune information sur l'existence du droit de retirer son consentement à tout moment lui était disponible, ni au moment de l'inscription sur le site internet, ni lorsqu'il recevait l'email de confirmation d'inscription sur la liste d'envoi de la newsletter. Il pouvait néanmoins se désinscrire de la newsletter en cliquant sur le lien de désinscription se trouvant en bas de l'email d'envoi de ladite newsletter.

[69] Voir pièce 5 annexée au rapport d'enquête.
[70] Voir pièce 7 annexée au rapport d'enquête.
[71] Voir communication des griefs, point 55.

58. Le contrôlé n'a dès lors pas fourni aux utilisateurs de son site internet toutes les informations rendues obligatoires par l'article 13.2.c) du RGPD.

59. Au vu de ce qui précède aux points 50 à 58, la Formation Restreinte se rallie à l'avis du chef d'enquête et conclut qu'au début de l'enquête de la CNPD, le contrôlé a manqué à son obligation d'informer les personnes concernées découlant de l'article 13.1.c), f) et 13.2.c) du RGPD, et plus précisément de les informer sur les bases juridiques du traitement, sur les transferts de données personnelles vers des pays tiers ou des organisations internationales, ainsi que sur l'existence du droit de retirer leur consentement à tout moment.

II. 2. Sur l'amende et les mesures correctrices

1. Sur les principes

60. Conformément à l'article 12 de la loi du 1er août 2018, la Commission nationale dispose des pouvoirs prévus 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. »

61. 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.

62. 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 œuvre 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 ».

63. 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.

64. Néanmoins, les démarches effectuées par le contrôlé pour se mettre en conformité avec le RGPD en 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 à prononcer 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

65. Dans la communication des griefs, le chef d'enquête propose à la Formation Restreinte de prononcer à l'encontre du contrôlé une amende administrative portant sur le montant de 1.700 euros.

66. 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 analyse les critères posés par l'article 83.2 du RGPD :

- Quant à la nature et la gravité de la violation (article 83.2 a) du RGPD), en ce qui concerne les manquements aux articles 12 et 13 du RGPD, elle rappelle que l'information et la transparence relative aux traitements de données à caractère personnel sont des obligations essentielles pesant sur les responsables de traitement afin que les personnes soient pleinement conscientes de l'utilisation qui sera faite de leurs données à caractère personnel, une fois celles-ci collectées. Un manquement aux articles 12.1 et 13 du RGPD est ainsi constitutif d'une atteinte aux droits des personnes concernées. Le droit à la transparence et le droit à l'information ont par ailleurs été renforcés aux termes du RGPD, ce qui témoigne de leur importance toute particulière.

- Quant au critère de durée (article 83.2.a) du RGPD), la Formation Restreinte constate que ces manquements ont duré dans le temps, à tout le moins depuis le début de l'enquête de la CNPD et jusqu'à, le cas échéant, une modification éventuelle de la politique de protection des données. Elle rappelle que de la guidance relative aux principes et obligations prévus dans le RGPD était disponible auprès de la CNPD, notamment sur son site internet.

- Quant au nombre de personnes concernées (article 83.2. a) du RGPD), la Formation Restreinte constate qu'il s'agit […]. Le contrôlé a précisé qu'en 2020 environ […] commandes ont été réalisées par […].[72]

- 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

[72] Voir compte-rendu, pages 4 et 6.

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.

- Quant au degré de coopération établi avec l'autorité de contrôle (article 83.2. f) du RGPD), la Formation Restreinte tient compte de l'affirmation du chef d'enquête selon laquelle le contrôlé a fait preuve d'une participation constructive tout au long de l'enquête.[73]

- Quant aux mesures prises par le contrôlé pour atténuer le dommage subi par les personnes concernées (article 83.2.c), 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.

67. 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.

68. Elle 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 lancement de l'enquête par les agents de la CNPD en date du 26 août 2020 (voir aussi le point 63 de la présente décision).

69. 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 12.1 et 13 du RGPD.

70. 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 aux articles 12.1 et 13 du RGPD est reproché au contrôlé, le montant maximum de l'amende pouvant être retenu

[73] Communication des griefs, point 60.c).

s'élève à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

71. Au regard des critères pertinents de l'article 83.2 du RGPD évoqués ci-avant, la Formation Restreinte considère que le prononcé d'une amende de mille quatre cents (1.400) 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

72. Dans la communication des griefs le chef d'enquête propose à la Formation Restreinte d'adopter les mesures correctrices suivantes : « *endéans un délai de **1 mois** à compter de la notification au Contrôlé de la décision prise par la Formation Restreinte :*

Ordonner, en vertu de l'article 58 (2) d) du RGPD, la mise en conformité du Contrôlé à l'article 12 (1) du RGPD en procédant aux modifications suivantes :

a) Mettre à jour la politique de protection des données et la politique cookies de la Société A en s'assurant que les informations contenues dans ces politiques reflètent la réalité, notamment au niveau de l'utilisation de la technique de profilage, de l'existence d'un DPD et des durées de rétention pour les cookies et les commandes des clients ;

b) Adapter dans la politique de protection des données l'information relative à sa mise à jour ;

c) Traduire la politique de protection des données dans les mêmes langues que celles proposées pour le site internet;

d) Préciser dans la politique de protection des données l'information sur les destinataires des données.

Ordonner, en vertu de l'article 58 (2) d) du RGPD, la mise en conformité du Contrôlé à l'article 13 paragraphes (1) et (2) du RGPD, en renseignant, dans la politique de protection des données, les informations suivantes :

- les bases juridiques des traitements de données et des cookies ;

- l'information relative aux transferts de données vers des pays tiers ;

- l'information relative au droit de retirer son consentement à tout moment.»[74]

73. A titre préliminaire, en ce qui concerne les mesures correctrices proposées par le chef d'enquête concernant les cookies déposés par le contrôlé, la Formation Restreinte tient à réitérer que comme le contrôle de l'application et du respect de la loi modifiée du 30 mai 2005 n'était pas dans le périmètre de l'enquête en cause, la Formation Restreinte ne statue pas dans la présente décision sur les mesures correctrices proposées par le chef d'enquête concernant les cookies déposés par le contrôlé.

74. Quant aux autres mesures correctrices proposées par le chef d'enquête et par référence au point 64 de la présente décision, la Formation Restreinte prend en compte les démarches effectuées par le contrôlé afin de se conformer aux dispositions des articles 12.1 et 13 du RGPD, telles que détaillées notamment dans son courrier du 10 février 2022. Plus particulièrement, elle prend note des faits suivants :

- Quant à la mesure correctrice proposée par le chef d'enquête reprise sous a) du point 72 de la présente décision concernant la mise à jour de la politique de confidentialité en s'assurant que les informations reflètent la réalité, notamment au niveau de l'utilisation de la technique de profilage, de l'existence d'un DPD et des durées de rétention des commandes des clients, la Formation Restreinte prend en compte la précision du contrôlé lors de la séance du 13 juillet 2022 que la politique de confidentialité a été mise à jour le 17 février 2022 (ci-après : « la politique de confidentialité mise à jour ») et qu'elle a déjà été mise sur son site internet.

  Dans son courrier du 10 février 2022, le contrôlé a précisé avoir mis à jour sa politique de confidentialité en *« supprimant les références à des techniques de profilage que nous n'appliquons pas. »* Dans la partie […][75] de la politique de confidentialité mise à jour il n'est en effet plus fait mention d'une technique de profilage. Par contre, elle constate que la politique de confidentialité mise à jour mentionne toujours dans la partie […] que *« la Société A collecte et traite notamment les […] préférences et centres d'intérêts […] des Utilisateurs. »* La Formation Restreinte estime donc que la collecte des données précitées fait toujours, de manière implicite, référence à l'utilisation d'une technique de profilage.

[74] Communication des griefs, point 58.
[75] Partie […] dans l'ancienne politique de confidentialité.

Par ailleurs, dans ledit courrier du 10 février 2022, le contrôlé a précisé avoir mis à jour les « *informations, y compris les coordonnées de contact, relatives au DPD, poste que nous avons introduit en 2021.* » La politique de confidentialité mise à jour mentionne donc que le contrôlé *« a nommé un Délégué à la Protection des Données (DPO) pouvant être contacté à l'adresse email suivante :* [...] *».* Durant l'audience de la Formation Restreinte du 13 juillet 2022, le contrôlé a confirmé la nomination d'un DPD interne qui occupe aussi d'autres tâches.

Finalement, en ce qui concerne les durées de rétention des commandes des clients, la Formation Restreinte note que la politique de confidentialité mise à jour contient une partie spécifique sur les durées de conservation des données[76] indiquant que si [un client demande la fermeture de son compte, ses données personnelles sont supprimées ou rendues anonymes]. Dans ladite partie l'utilisateur est par ailleurs invité à consulter la durée de conservation de données personnelles par traitement dans les tableaux décrits à la partie […] de sa politique. En passant en revue les durées de rétention des différentes données traitées dans le cadre du traitement « […] » indiquées dans ces tableaux, la Formation Restreinte constate que les « données personnelles » et les « données de la commande »[77] sont sauvegardées pendant dix ans. Il n'y est pas indiqué que les données personnelles seront supprimées ou rendues anonymes si l'utilisateur demande la fermeture de son compte.

Il y a donc une incohérence entre la partie […] de la politique de confidentialité mise à jour et les durées de conservation indiquées dans la partie […].

En considération des mesures de mise en conformité insuffisantes prises par le contrôlé en l'espèce et du point 64 de la présente décision, la Formation Restreinte considère dès lors qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête à cet égard et reprise au point 72 de la présente décision sous a) concernant la durée de rétention des commandes des clients, ainsi que la référence à l'utilisation de la technique de profilage.

- Quant à la mesure correctrice proposée par le chef d'enquête reprise sous b) du point 72 de la présente décision concernant l'information relative à la mise à jour de la politique de confidentialité, le contrôlé a confirmé dans son courrier du 10 février 2022

[76] Voir partie […]
[77] Par « Données personnelles: » sont visées […] et par « Données de la commande » […].

avoir adapté la politique de confidentialité et plus précisément *« l'information relative à sa mise à jour en précisant que les utilisateurs enregistrés sont informés de tout changement par e-mail. »*

La Formation Restreinte note que la politique de confidentialité mise à jour mentionne dans la partie […] que les [clients enregistrés sont informés de tout changement de la Politique de Confidentialité par e-mail].

En considération des mesures de mise en conformité suffisantes prises par le contrôlé en l'espèce et du point 64 de la présente décision, la Formation Restreinte considère dès lors qu'il n'y a pas lieu de prononcer la mesure correctrice proposée par le chef d'enquête à cet égard et reprise au point 72 de la présente décision sous b).

- Quant à la mesure correctrice proposée par le chef d'enquête reprise sous c) du point 72 de la présente décision concernant la traduction de la politique de confidentialité dans les mêmes langues que celles proposées pour le site internet, le contrôlé a indiqué dans son courrier du 10 février 2022 qu'en *« date du […] 2022, nous avons publié la politique de protection des données en allemand. »*

  En effet, la Formation Restreinte constate que la politique de confidentialité est désormais disponible dans les mêmes langues que le site internet du contrôlé, c'est-à-dire en français et allemand.

  En considération des mesures de mise en conformité suffisantes prises par le contrôlé en l'espèce et du point 64 de la présente décision, la Formation Restreinte considère dès lors qu'il n'y a pas lieu de prononcer la mesure correctrice proposée par le chef d'enquête à cet égard et reprise au point 72 de la présente décision sous c).

- Quant à la mesure correctrice proposée par le chef d'enquête reprise sous d) du point 72 de la présente décision concernant la précision dans la politique de confidentialité de l'information sur les destinataires des données, le contrôlé a indiqué dans son courrier du 10 février 2022 qu'en *« date du […] 2022, nous avons mis à jour la politique de protection des données en précisant l'information sur les destinataires des données et plus particulièrement la catégorie des destinataires. »*

- En lisant la politique de confidentialité mise à jour, la Formation Restreinte constate que dans la partie […] les destinataires des données, nommément désignés en fonction des

différents traitements, sont précisés, tandis que la partie […] contient [une liste des entités autorisées à recevoir des données personnelles relatives au client].[78]

En considération des mesures de mise en conformité suffisantes prises par le contrôlé en l'espèce et du point 64 de la présente décision, la Formation Restreinte considère dès lors qu'il n'y a pas lieu de prononcer la mesure correctrice proposée par le chef d'enquête à cet égard et reprise au point 72 de la présente décision sous d).

- Quant aux mesures correctrices proposées par le chef d'enquête reprises au deuxième alinéa du point 72 de la présente décision concernant l'insertion dans la politique de confidentialité d'informations sur les bases juridiques des traitements de données, sur les transferts de données vers des pays tiers, ainsi que l'information relative au droit de retirer son consentement à tout moment, le contrôlé a indiqué dans son courrier du 10 février 2022 ce qui suit *: […] en date du […] 2021 :*
- nous avons ajouté les bases juridiques des traitements des données ;
[…]
- nous avons ajouté l'information relative au droit de retirer son consentement à tout moment.

Veuillez noter qu'une mise à jour additionnelle est prévue prochainement afin de :
[…]
- préciser davantage les transferts vers des pays tiers, notamment en relation avec la plateforme de paiement […] et la solution de gestion des newsletter […]*. »*

En ce qui concerne les bases juridiques des traitements des données, la Formation Restreinte note que dans la partie […] de la politique de confidentialité, les bases juridiques sont mentionnées par traitement de données. En ce qui concerne le traitement dénommé « […] », elle constate néanmoins que deux différentes bases juridiques sont indiquées,[79] alors que le responsable du traitement ne peut se baser que sur une des six bases juridiques prévues à l'article 6 du RGPD. Le CEPD a précisé dans ce contexte dans ses lignes directrices sur le consentement ce qui suit : *« L'article 6*

[78] Et plus précisément […] (Prestataire du service de paiement électronique), […] (Editeur […] de la Société A), […] (Prestataire du service de livraison), […] (Prestataire d'hébergement des bases de données), […] (Partenaire […]).
[79] Et plus précisément : *« […]».*

établit les conditions d'un traitement des données à caractère personnel licite et décrit six bases juridiques sur lesquelles un responsable du traitement peut se fonder. L'application de l'une de ces six bases juridiques doit être établie avant l'activité de traitement et en lien avec une finalité spécifique. »[80]

En ce qui concerne l'information relative au droit de retirer son consentement à tout moment, la Formation Restreinte tient à renvoyer au point 56 de la présente décision en réitérant que l'obligation de mentionner l'existence du droit de retirer son consentement à tout moment s'impose uniquement si la base juridique du traitement est le consentement de la personne concernée, c'est-à-dire en l'espèce l'envoi de la newsletter par le contrôlé.

Elle note que dans la partie […] est mentionné ce qui suit : « *[…].*» La Formation Restreinte estime dans ce contexte que le contrôlé a fait un amalgame de deux bases juridiques et de deux différents traitements de données : le consentement de l'utilisateur pour l'envoi de la newsletter, un consentement que la personne concernée doit pouvoir retirer à tout moment, d'une part, et l'exécution du contrat entre le contrôlé et les utilisateurs pour ce qui concerne la gestion des commandes […], un contrat que les utilisateurs peuvent résilier en clôturant leur compte, d'autre part. Il est important de noter dans ce contexte que *« le consentement ne peut être obtenu moyennant la même action que lorsqu'une personne concernée accepte un contrat ou les conditions générales d'un service. L'acceptation globale des conditions générales ne peut être considérée comme un acte positif clair visant à donner son consentement à l'utilisation de données à caractère personnel. »*[81]

La politique de confidentialité doit dès lors mentionner plus précisément que l'utilisateur a le droit de retirer à tout moment son consentement donné pour l'envoi de la newsletter.

En ce qui concerne les transferts vers des pays tiers, la Formation Restreinte note que la politique de confidentialité mise à jour indique dans la partie […] ce qui suit : *« Pour les sous-traitants/outils* [...] *et* [...]*, un transfert de données a lieu vers des pays tiers. […] ».*

[80] Lignes directrices 5/2020 du CEPD sur le consentement au sens du règlement (UE) 2016/679, Version 1.1, Adoptées le 4 mai 2020, point 121.
[81] Lignes directrices 5/2020 du CEPD sur le consentement au sens du règlement (UE) 2016/679, Version 1.1, Adoptées le 4 mai 2020, point 81.

Néanmoins, comme l'article 13.1.f) du RGPD exige du responsable du traitement de mentionner *« l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1, deuxième alinéa, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition »*, la Formation Restreinte estime que les informations fournies par le contrôlé ne sont pas suffisantes […].

En considération des mesures de mise en conformité insuffisantes prises par le contrôlé en l'espèce et du point 64 de la présente décision, la Formation Restreinte considère dès lors qu'il y a lieu de prononcer les mesures correctrices proposées par le chef d'enquête à cet égard et reprises au deuxième alinéa du point 72 de la présente décision concernant l'insertion dans la politique de confidentialité d'informations sur les bases juridiques des traitements de données, sur les transferts de données vers des pays tiers, ainsi que l'information relative au droit de retirer son consentement à tout moment.

Compte tenu des développements qui précèdent, la Commission nationale siégeant en formation restreinte et après en avoir délibéré, décide :

- de retenir les manquements aux articles 12.1 et 13 du RGPD ;
- de prononcer à l'encontre de la Société A une amende administrative d'un montant de mille quatre cents (1.400) euros, au regard des manquements constitués aux articles 12.1 et 13 du RGPD ;
- de prononcer à l'encontre de la Société A une injonction de mettre en conformité les traitements avec les obligations résultant de l'article 12.1 du RGPD, dans un délai de 2 (deux) mois suivant la notification de la décision de la Formation Restreinte, et, en particulier :
    - mettre à jour dans la politique de confidentialité les durées de conservation des données à caractère personnel collectées dans le cadre des commandes des clients en s'assurant que leur indication est cohérente dans les différentes parties de ladite politique ;

- s’assurer que les informations contenues dans la politique de confidentialité reflètent la réalité au niveau de l'utilisation de techniques de profilage ;

- de prononcer à l'encontre de la Société A» une injonction de mettre en conformité les traitements avec les obligations résultant de l’article 13 du RGPD, dans un délai de 2 (deux) mois suivant la notification de la décision de la Formation Restreinte, et, en particulier :

  - mettre à jour dans la politique de confidentialité les bases juridiques des différents traitements de données en s’assurant qu’une seule base juridique par traitement est mentionnée ;

  - mettre à jour la politique de confidentialité en mentionnant le droit pour un utilisateur de retirer à tout moment son consentement donné pour l’envoi de la newsletter ;

  - mettre à jour dans la politique de confidentialité les informations sur les transferts de données vers des pays tiers.

Belvaux, le 13 décembre 2022.

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

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Alain Herrmann 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.