

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

Délibération n° 4FR/2025 du 16 décembre 2025

La Commission nationale pour la protection des données siégeant en formation restreinte, composée de Madame Tine A. Larsen, présidente, Monsieur Marc Hemmerling, membre suppléant, et de Madame Romy Schaus, membre suppléant ;

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 1^{er} 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°28AD/2025 en date du 10 octobre 2025, notamment son article 10, paragraphe 2 ;

Vu le règlement de la Commission nationale pour la protection des données relatif à la procédure d'enquête adopté par décision n°08AD/2024 en date du 23 février 2024, notamment son article 9 ;

Considérant ce qui suit :

I. Faits et procédure

1. Lors de sa séance de délibération du 9 février 2024, la Commission nationale pour la protection des données (ci-après : la « CNPD » ou la « Commission nationale ») siégeant en formation plénière a décidé d'ouvrir une enquête auprès de la Société A sur base de l'article 38 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 Alain Herrmann comme chef d'enquête.

2. Ladite décision a précisé que l'enquête menée par la CNPD avait pour objet de contrôler l'application et le respect 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 : le « RGPD ») et de la loi du 1er août 2018, et « *plus particulièrement le respect des articles 30.1, 30.3 et 30.4 du RGPD relatif au registre des activités de traitement et des textes légaux prévoyant des dispositions spécifiques en matière de protection des données à caractère personnel* »¹.

3. La Société A est une société [...] inscrite au Registre de Commerce et des Sociétés de Luxembourg sous le numéro [...] et a son siège social à [...] (ci-après : le « contrôlé »). Le contrôlé a pour objet « [Activités de sécurité privée] »².

4. En date du 18 mars 2024, des agents de la CNPD ont effectué une visite sur place au siège social du contrôlé (ci-après : la « visite sur place »).

Ce moment est référencé ultérieurement dans cette décision comme « début de l'enquête ».

5. Par courriel du 19 mars 2024, c'est-à-dire avant l'envoi du procès-verbal no. [...] relatif à la visite sur place effectuée en date du 18 mars 2024 auprès du contrôlé, le contrôlé a transmis une copie numérique de son registre des activités de traitement aux agents de la CNPD en expliquant que ce registre « *a été pour la dernière fois updaté ce jour* » (ci-après le « deuxième registre des traitements »). Par un deuxième courriel du même jour, le contrôlé a fourni à la CNPD des informations complémentaires demandées lors de la visite sur place.

¹ Délibération n° [...] du 9 février 2024 de la Commission nationale pour la protection des données relative à l'ouverture d'une mission d'enquête auprès de la Société A.

² Statuts coordonnés du contrôlé du [...], article 4 ; pièce n° 6 de la communication des griefs.

6. Le procès-verbal no. [...] relatif à la visite sur place effectuée en date du 18 mars 2024 auprès du contrôlé dressé par les agents de la CNPD (ci-après : le « procès-verbal ») a été envoyé au contrôlé par courriel en date du 29 mars 2024³.

Il résulte de ce procès-verbal, entre autres, que le contrôlé a déclaré avoir mis en place un registre des activités de traitement conformément à l'article 30 du RGPD et qu'il l'a présenté aux agents de la CNPD par visioconférence sous forme d'un fichier Excel⁴ (ci-après le « premier registre des traitements »). Cependant, au jour de la visite sur place le contrôlé n'était pas en mesure de mettre le premier registre des traitements à la disposition des agents de la CNPD en expliquant « *qu'il devait l'exporter depuis une base de données du logiciel* » [...] »⁵ mais il a envoyé une version numérique dudit registre aux agents de la CNPD en date du 26 avril 2024⁶.

7. Par courriel du 26 avril 2024, le contrôlé a fait parvenir sa prise de position concernant le procès-verbal et a répondu aux questions soulevées par les agents de la CNPD dans la lettre d'accompagnement du procès-verbal. En annexe dudit courriel, le contrôlé a envoyé l'extrait du premier registre des traitements, comme demandé par les agents de la CNPD, et a expliqué les modifications faites au premier registre des traitements dans les 24h après la visite sur place. En outre, le contrôlé a envoyé une troisième version de son registre des activités de traitement (ci-après le « troisième registre des traitements ») et a précisé que cette nouvelle version a été considérablement améliorée depuis la prise de fonction de la nouvelle déléguée à la protection des données du contrôlé⁷.

8. En date du 4 novembre 2024, une demande d'information complémentaire a été envoyée au contrôlé.

9. En date du 12 novembre 2024, le contrôlé a répondu par courriel à la demande d'information complémentaire et a envoyé une nouvelle version de son registre des activités de traitement (ci-après le « quatrième registre des traitements »).

³ Le procès-verbal contenait également la décision d'ouverture d'enquête n° [...], un relevé des photos prises lors de la visite sur place et un inventaire des pièces collectées et/ou demandées par les agents de la CNPD lors de la visite sur place.

⁴ Cf. Pièces n° 07, 08, 09 et 14 de la communication des griefs ; le premier registre des traitements a été envoyé par le contrôlé à la CNPD par courriel en date du 26 avril 2024 (cf. Pièces n° 12 à 13 de la communication des griefs).

⁵ Cf. Constat 4 du procès-verbal.

⁶ Cf. Pièce n° 14 de la communication des griefs.

⁷ Cf. Courriel du contrôlé du 26 avril 2024, réponse à la (Q4).

10. En réponse au dernier courriel du contrôlé, les agents de la CNPD ont envoyé une troisième demande d'information complémentaire en date du 23 janvier 2025 à laquelle le contrôlé a répondu par courriel du 24 janvier 2025.

11. A l'issue de son instruction, le chef d'enquête a notifié au contrôlé en date du 19 février 2025 une communication des griefs (ci-après : la « communication des griefs ») détaillant les manquements qu'il estimait constitués en l'espèce par rapport aux exigences prescrites par l'article 30 (1) du RGPD (l'obligation de tenir un registre des activités de traitement).

Le chef d'enquête a proposé à la Commission nationale siégeant en formation restreinte (ci-après : la « Formation Restreinte ») d'adopter deux mesures correctrices différentes (hors amende administrative), ainsi que d'infliger au contrôlé une amende administrative d'un montant de 2.784 euros. La faculté de formuler des observations écrites sur la communication des griefs a été offerte au contrôlé.

12. Par courriel en date du 13 mars 2025, le contrôlé a formulé ses observations relatives à la communication des griefs et il a envoyé une nouvelle version de son registre des activités de traitement (ci-après le « cinquième registre des traitements »).

13. Le 24 mars 2025, le chef d'enquête a transmis le dossier à la Formation Restreinte en vue d'une prise de décision quant à l'issue de l'enquête.

14. La présidente de la Formation Restreinte a informé le contrôlé par courrier en date du 12 mai 2025, que son affaire serait inscrite à la séance de la Formation Restreinte du 26 juin 2025 et qu'il lui était offert la possibilité d'y être entendu.

15. Par courriel du 11 juin 2025, le contrôlé a confirmé sa présence à ladite séance et il a envoyé encore une version de son registre des activités de traitement (ci-après le « sixième registre des traitements »).

16. Lors de cette séance, le chef d'enquête, accompagné de [...], juriste et gestionnaire du dossier, et le contrôlé, représenté par [...], *Legal Affairs and Risk Director*, et [...], avocate externe, ont exposé leurs observations orales à l'appui de leurs observations écrites et ont répondu aux questions posées par la Formation Restreinte.

17. Par courriel du 9 juillet 2025, le contrôlé a répondu aux questions posées par la Formation Restreinte lors de la séance du 26 juin 2025 et il a envoyé une nouvelle version de son registre des activités de traitements (ci-après le « septième registre des traitements »)

18. La décision de la Formation Restreinte sur l'issue de l'enquête se basera :

- sur la tenue par le contrôlé d'un registre des activités de traitement en vertu de l'article 30 (1), (3) et (4) du RGPD ; et
- sur les dispositions légales et réglementaires en cause.

II. En droit

II.1. Sur les motifs de la décision

A. Sur la qualité du contrôlé

19. Selon l'article 4 (7) du RGPD, le responsable du traitement est défini comme la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

20. La Formation Restreinte note que dans le premier registre de traitements du contrôlé, présenté lors de la visite sur place, plusieurs responsables du traitement figuraient dans ce registre. Sur question posée par les agents de la CNPD, le contrôlé a déclaré faire partie d'un groupe de sociétés dirigé par la Société B⁸ mais il a clarifié dans son courriel du 12 novembre 2024 qu'il était « *la principale entité juridique et la seule entité qui a une activité opérationnelle* » parmi les sociétés mentionnées dans le premier registre de traitements et que c'était « *uniquement cette entité qui [devait] être reprise comme responsable dans le registre des traitements* »⁹. Ainsi, la Formation Restreinte partage l'avis du chef d'enquête exposé dans sa communication des griefs¹⁰ et retient que le contrôlé est à considérer comme responsable du traitement, au sens du RGPD, pour les traitements figurant dans son registre des activités de traitement.

⁸ Cf. Point 7 de la communication des griefs.

⁹ Cf. Courriel du contrôlé du 12 novembre 2024 ; Point 13 de la communication des griefs.

¹⁰ Cf. Communication des griefs, page 6, points 11 à 14.

B. Sur le manquement lié à l'obligation de tenir un registre des activités de traitement (article 30 (1), (3) et (4) du RGPD)

1. Sur les principes

21. En vertu de l'article 30 (1) du RGPD, le responsable du traitement a l'obligation de tenir un registre des activités de traitement qui sont effectués sous sa responsabilité. Ce registre doit contenir les informations suivantes :

« a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;

b) les finalités du traitement ;

c) une description des catégories de personnes concernées et des catégories de données à caractère personnel ;

d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;

e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées ;

f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;

g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1 ».

L'article 30 (3) à (4) du RGPD dispose que :

« 3. Les registres visés aux paragraphes 1 et 2 se présentent sous une forme écrite y compris la forme électronique.

4. Le responsable du traitement ou le sous-traitant et, le cas échéant, leur représentant mettent le registre à la disposition de l'autorité de contrôle sur demande. »

2. En l'espèce

22. Lors de la visite sur place en date du 18 mars 2024, le contrôlé a présenté aux agents de la CNPD le premier registre des traitements par visioconférence sous forme d'un fichier Excel¹¹ mais il n'a pas été en mesure de mettre à disposition le fichier Excel aux agents de la CNPD¹². En date du 19 mars 2024, le contrôlé a envoyé le deuxième registre des traitements et les agents de la CNPD ont constaté qu'il s'agissait d'une version modifiée par rapport à la version du premier registre des traitements présenté lors de la visite sur place¹³. Pour l'établissement de sa communication des griefs, le chef d'enquête a tenu compte du premier registre des traitements qui a été communiquée par le contrôlé aux agents de la CNPD le 26 avril 2024 et qui a été montré par le contrôlé aux agents de la CNPD lors de la visite sur place¹⁴.

23. Le premier registre des traitements est au format Excel et se compose de 51 traitements pour lesquels le contrôlé est indiqué comme responsable du traitement¹⁵.

24. Dans sa communication des griefs, le chef d'enquête a retenu que le premier registre des traitements était

- incomplet ou incorrect car certaines informations obligatoires en vertu de l'article 30 (1) du RGPD faisaient défaut ou étaient incomplètes ou incorrectes¹⁶ ; et
- imprécis car certaines informations obligatoires en vertu de l'article 30 (1) du RGPD étaient imprécises¹⁷.

¹¹ Cf. Point 15 de la communication des griefs ; Pièce n° 7 à 9 de la communication des griefs.

¹² Cf. Procès-verbal, page 3, point 4.

¹³ Cf. Point 16 de la communication des griefs.

¹⁴ Cf. Point 18 de la communication des griefs ; cependant, pour la détermination des mesures correctrices pertinentes à proposer dans sa communication des griefs, le chef d'enquête a également tenu compte du quatrième registre des traitements (cf. points 88 à 93 de la communication des griefs).

¹⁵ Cf. Point 17 de la communication des griefs ; Pièce n° 14 de la communication des griefs.

¹⁶ Cf. Points 22 à 73 de la communication des griefs.

¹⁷ Cf. Points 74 à 80 de la communication des griefs.

Il a encore souligné que « *les présentes violations ont été constatées sans préjudice quant au contrôle de l'exhaustivité et de l'exactitude de la totalité des informations contenues dans le [r]egistre des traitements, contrôle qui ne [faisait] pas l'objet de la présente enquête* »¹⁸.

a) Quant aux coordonnées du responsable du traitement ainsi qu'aux coordonnées du délégué à la protection des données (article 30 (1) a) du RGPD)

25. Il résultait du premier registre des traitements qu'il comportait uniquement le nom et l'adresse postale du contrôlé et le nom du délégué à la protection des données mais que les autres coordonnées du responsable du traitement (adresse électronique et/ou numéro de téléphone) et les coordonnées du délégué à la protection des données faisaient défaut.¹⁹

26. Or, la Formation Restreinte rappelle qu'en vertu de l'article 30 (1) a) du RGPD, le registre des activités de traitement doit comporter les coordonnées du responsable du traitement et du délégué à la protection des données et que, dans un souci d'exhaustivité et de bonne joignabilité, la mention de l'adresse postale du responsable du traitement n'est pas suffisante.

Ainsi, la Formation Restreinte se rallie à l'avis du chef d'enquête et retient que le contrôlé a manqué à son obligation découlant de l'article 30 (1) a) du RGPD.

b) Quant à la description des catégories de personnes concernées et des catégories de données à caractère personnel (article 30 (1) c) du RGPD)

27. Il résultait du premier registre des traitements et, plus précisément, de ses lignes 2, 5, 11, 15, 17, 29, 30, 46, 48 et 51 précisant des traitements spécifiques, que la colonne L intitulée « *Data Category – Personal Data* »²⁰ et la colonne M intitulée « *Data Category – Personal Data* »²¹ ne contenaient aucune information, c'est-à-dire qu'elles étaient vides pour les traitements suivants :

- *Carry out business changes_Luxembourg* (cf. ligne 2);
- *Communications between workers and external professionals for business purposes (controller)_Luxembourg* (cf. ligne 5);
- *Archiving of communication about business activities and changes_Luxembourg* (cf. ligne 11);

¹⁸ Cf. Communication des griefs, page 8, point 21.

¹⁹ Cf. Communication des griefs, page 9, points 24 à 32 ; Pièce n° 14 de la communication des griefs.

²⁰ Cf. Communication des griefs, page 10, points 33 à 36.

²¹ Cf. Communication des griefs, page 11, points 37 à 40.

- *Sharing of personal data with recipients in order to carry out business changes_Luxembourg* (cf. ligne 15);
- *Carry out analysis for increased business insights and business planning (controller)_Luxembourg* (cf. ligne 17);
- *Ensure technical functionality and security of our services (controller)_Luxembourg* (cf. ligne 29);
- *Archiving of use of IT systems and services (controller)_Luxembourg* (cf. ligne 30);
- *Sharing personal data with the employer in order to manage the contractor relationship_Luxembourg* (cf. ligne 46);
- [...] (cf. ligne 48); et
- [...] (cf. ligne 51)²².

28. En outre, le chef d'enquête a constaté dans sa communication des griefs que la colonne L intitulée « *Data Category – Personal Data* » et la colonne M intitulée « *Data Category – Personal Data* » contenaient, aux lignes 3, 4, 6, 7, 8, 9, 10, 12, 13, 14, 16, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 47, 49, 50 et 52 de son registre, une description des catégories de données traitées qui n'était pas suffisamment précise. Selon lui, il ne suffisait pas de « *fournir une liste de catégories génériques de données* », mais qu'il était « *également nécessaire de les décrire en précisant leurs caractéristiques principales et ce afin d'être en mesure de démontrer la conformité au RGPD* »²³.

29. La Formation Restreinte rappelle qu'en vertu de l'article 30 (1) c) du RGPD, le registre des activités de traitement doit comporter aussi bien une description des catégories des personnes concernées qu'une description des catégories de données à caractère personnel. Or, elle constate que le premier registre de traitement contenait ces descriptions pour certaines activités de traitement mentionnées dans ledit registre mais que les lignes 2, 5, 11, 15, 17, 29, 30, 46, 48 et 51 dudit registre ne contenaient ni l'une ni l'autre description par rapport aux activités de traitements mentionnées dans la liste ci-dessus.

30. Elle considère également que la description d'une catégorie de données à caractère personnel devrait, entre autres, clarifier si des catégories particulières de données à caractère personnel en vertu des articles 9 et 10 du RGPD sont traitées. Par conséquent, elle partage l'avis du chef d'enquête et retient qu'il ne suffit pas de mentionner uniquement une liste de catégorie génériques sans description. A cet égard, elle constate que la colonne

²² Cf. Communication des griefs, page 10 à 11, point 33 et 37; Pièce n° 14 de la communication des griefs.

²³ Cf. Communication des griefs, page 22, point 75.

M du premier registre des traitements contenait aux lignes 3, 4, 6, 7, 8, 9, 10, 12, 13, 14, 16, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 47, 49, 50 et 52²⁴ que des descriptions génériques de catégories de données à caractère personnel comme, par exemple, « *Employment information* » ou « *Financial information* », et qu'il s'agissait de descriptions pas suffisamment précises.

Dès lors, la Formation Restreinte se rallie à l'avis du chef d'enquête et retient que le contrôlé a manqué à son obligation découlant de l'article 30 (1) c) du RGPD.

c) Quant aux catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers (article 30 (1) d) du RGPD)

31. Il résultait du premier registre des traitements et, plus précisément, de ses lignes 4, 18, 28, 43, 51 et 52, que la colonne N intitulée « *Parties who Access/Use Data* »²⁵ ne contenait aucune information relative aux catégories de destinataires auxquels des données à caractère personnel ont été ou seront communiquées pour les traitements suivants :

- *Carry out events and other staff activities_Luxembourg* (cf. ligne 4);
- *Evaluate and follow-up on the recruitment process_Luxembourg* (cf. ligne 18);
- *Sharing of personal data with providers [...]* (cf. ligne 28);
- *Sharing of personal data [...]* (cf. ligne 43);
- [...] (cf. ligne 51); et
- [...] (cf. ligne 52)²⁶.

32. En outre, il résultait du premier registre des traitements que la colonne P intitulée « *Cross Border Transfer Mechanism(s) for the Processing Activity* » ne contenait soit pas d'information soit une information incorrecte²⁷ relative aux destinataires dans des pays tiers et ce bien que le contrôlé ait confirmé dans son courriel du 12 novembre 2024 qu'il procédait à un transfert de données à caractère personnel dans des pays tiers pour les treize traitements suivants (lignes 5, 7, 14, 16, 29, 30, 31, 33, 36, 38, 40, 51 et 52 dudit registre) :

²⁴ Cf. Communication des griefs, pages 21 à 25, points 74 à 80.

²⁵ Cf. Communication des griefs, page 12, points 41 à 44.

²⁶ Cf. Communication des griefs, page 12, point 41.

²⁷ La ligne 29 contenait notamment une information erronée dans la colonne intitulée « *Hosting Location – Assets* » selon le courriel du contrôlé du 12 novembre 2024.

- *Communication between workers and external professionals for business purposes (controller)_Luxembourg* (cf. ligne 5);
- *Ensure technical functionality and security of our services* (cf. ligne 7);
- *Manage the contractor relationship_Luxembourg* (cf. ligne 14);
- *Sharing of personal data with recipients for communication between employees and external professionals for business purposes_Luxembourg* (cf. ligne 16);
- *Ensure technical functionality and security of our services (controller)_Luxembourg* (cf. ligne 29);
- *Archiving of use of IT systems and services (controller)_Luxembourg* (cf. ligne 30);
- *Archiving of technical functionality and security of our services_Luxembourg* (cf. ligne 31);
- *Manage orders of goods and services from Customer (consumer)_Luxembourg* (cf. ligne 33);
- *Manage the contractual relationship with the customer (consumer)_Luxembourg* (cf. ligne 36);
- *Manage the client/supplier relationship_Luxembourg* (cf. ligne 38);
- *Procurement of a client/supplier_Luxembourg* (cf. ligne 40);
- [...] (cf. ligne 51); et
- [...] (cf. ligne 52)²⁸.

33. Or, la Formation Restreinte rappelle qu'en vertu de l'article 30 (1) d) du RGPD, le registre des activités de traitement doit comporter aussi bien les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées que les destinataires dans des pays tiers ou des organisations internationales. Selon l'article 4 (9) du RGPD le destinataire est « *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* » à l'exception des autorités publiques qui reçoivent « *des données à caractère personnel dans le cadre d'une mission d'enquête particulière* ». Elle souligne la différenciation faite par le RGPD dans son article 30 (1) d) en autorisant la mention des « *catégories de destinataires* » (par exemple, les sous-traitants) dans le registre des activités de traitement mais en précisant que « *les destinataires dans des pays tiers ou des organisations internationales* » (par exemple, le sous-traitant XY au [pays tiers X]) doivent être mentionnés dans ce registre. Elle se rallie à l'interprétation faite par le chef d'enquête en ce

²⁸ Cf. Communication des griefs, page 13, points 48 à 49.

qui concerne cette différenciation et retient que les destinataires doivent être précisément identifiés dès qu'un transfert de données à caractère personnel est fait vers un pays tiers.

34. Elle constate que les lignes 4, 18, 28, 43, 51 et 52 du premier registre de traitement ne contenaient aucune information relative aux catégories de destinataires auxquels des données à caractère personnel ont été ou seront communiquées (voir point 31 de la présente décision) et que les lignes 5, 7, 14, 16, 29, 30, 31, 33, 36, 38, 40, 51 et 52 dudit registre ne contenaient soit pas d'information soit une information incorrecte relative aux destinataires dans des pays tiers et ce malgré le fait que le contrôlé avait confirmé qu'il procédait à des transferts de données à caractère personnel dans des pays tiers (voir point 32 de la présente décision).

Dès lors, la Formation Restreinte se rallie à l'avis du chef d'enquête et retient que le contrôlé a manqué à son obligation découlant de l'article 30 (1) d) du RGPD.

d) Quant aux transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale (article 30 (1) e) du RGPD

35. Il résultait du premier registre des traitements que celui-ci ne comportait aucune colonne spécifique visant à indiquer, de manière affirmative ou négative, si des données à caractère personnel étaient transférées vers un pays tiers²⁹.

36. Or, le contrôlé a déclaré par courriel du 26 avril 2024³⁰ que des données à caractère personnel étaient transférées vers des pays tiers et, par courriel du 12 novembre 2024³¹, il a confirmé qu'il s'agissait concrètement des 13 traitements suivants qui étaient concernés par un transfert de données à caractère personnel vers un pays tiers :

- *Communication between workers and external professionals for business purposes (controller)_Luxembourg* (cf. ligne 5);
- *Ensure technical functionality and security of our services* (cf. ligne 7);
- *Manage the contractor relationship_Luxembourg* (cf. ligne 14);
- *Sharing of personal data with recipients for communication between employees and external professionals for business purposes_Luxembourg* (cf. ligne 16);

²⁹ Cf. Communication des griefs, page 14, points 53 à 58 ; Pièce n° 14 de la communication des griefs.

³⁰ Cf. Pièce n° 13 de la communication des griefs.

³¹ Cf. Pièce n° 17 de la communication des griefs.

- *Ensure technical functionality and security of our services (controller)_Luxembourg* (cf. ligne 29);
- *Archiving of use of IT systems and services (controller)_Luxembourg* (cf. ligne 30);
- *Archiving of technical functionality and security of our services_Luxembourg* (cf. ligne 31);
- *Manage orders of goods and services from Customer (consumer)_Luxembourg* (cf. ligne 33);
- *Manage the contractual relationship with the customer (consumer)_Luxembourg* (cf. ligne 36);
- *Manage the client/supplier relationship_Luxembourg* (cf. ligne 38);
- *Procurement of a client/supplier_Luxembourg* (cf. ligne 40) ;
- [...] (cf. ligne 51); et
- [...] (cf. ligne 52)³².

37. En outre, il résultait du premier registre des traitements que 12 des 13 traitements de données précités ne contenaient aucune identification des pays tiers concernés par un transfert de données à caractère personnel³³ et que la seule identification d'un pays tiers pour le traitement intitulé « *Ensure technical functionality and security of our services (controller)_Luxembourg* »³⁴ était erronée (selon le contrôlé dans son courriel du 12 novembre 2024)³⁵.

38. La Formation Restreinte rappelle que l'article 30 (1) e) du RGPD exige que le registre des traitements indique clairement si des données à caractère personnel sont transférées vers un pays tiers. Cette obligation est étroitement liée aux obligations issues du chapitre V du RGPD qui encadrent les transferts de données à caractère personnel vers un pays tiers. Dans ce sens, le considérant (101) du RGPD précise qu'« *il importe que, lorsque des données à caractère personnel sont transférées de l'Union à des responsables du traitement, sous-traitants ou autres destinataires dans des pays tiers ou à des organisations internationales, le niveau de protection des personnes physiques garanti dans l'Union par le présent règlement ne soit pas compromis* » . La mention de l'existence d'un transfert et l'identification du pays tiers ou de l'organisation internationale participe à la connaissance des traitements réalisés et des risques associés.

³² Cf. Pièce n° 14 de la communication des griefs.

³³ Cf. Points 59 à 60 de la communication des griefs.

³⁴ En cinquième position dans la liste ci-dessus.

³⁵ Cf. Point 61 de la communication des griefs.

39. Elle constate qu'aucune des 52 lignes décrivant des traitements de données à caractère personnel contenus dans le premier registre des traitements ne contenait une information spécifique visant à indiquer, de manière affirmative ou négative, si des données à caractère personnel étaient transférées vers un pays tiers. En outre, elle constate que les lignes 5, 7, 14, 16, 31, 33, 36, 38, 40, 51 et 52 du premier registre des traitements concernaient des traitements concernés par un transfert de données à caractère personnel vers un pays tiers mais que l'identification du pays tiers vers lequel ces données sont transférées faisaient défaut. Finalement, elle constate que le contrôlé a clarifié que la ligne 12 du premier registre de traitement contenait l'information erronée que ces données seraient transférées vers [le pays tiers X].

Dès lors, la Formation Restreinte se rallie à l'avis du chef d'enquête et retient que le contrôlé a manqué à son obligation découlant de l'article 30 (1) e) du RGPD.

e) Quant aux délais prévus pour l'effacement des différentes catégories de données (article 30 (1) f) du RGPD)

40. Il résultait du premier registre des traitements et plus précisément, de ses lignes 2 à 29 et 32 à 34 et 36 à 50 que la colonne S intitulée « *Aggregated Data Retention description* »³⁶ ne contenait aucun délai pour l'effacement des catégories de données suivantes :

- *Carry out business changes_Luxembourg* (cf. ligne 2);
- *Carry out board meetings_Luxembourg* (cf. ligne 3);
- *Carry out events and other staff activities_Luxembourg* (cf. ligne 4);
- *Communication between workers and external professionals for business purposes (controller)_Luxembourg* (cf. ligne 5);
- *Archiving of how work was distributed and performed_Luxembourg* (cf. ligne 6);
- *Ensure technical functionality and security of our services_Luxembourg* (cf. ligne 7);
- *Archiving of camera surveillance for the purposes of preventing, exposing and investigating crime_Luxembourg* (cf. ligne 8);
- *Archiving of salary and employment benefits_Luxembourg* (cf. ligne 9);
- *Sharing of personal data with recipients in order to fulfill legal obligations_Luxembourg* (cf. ligne 10);
- *Archiving of communication about business activities and changes_Luxembourg* (cf. ligne 11);

³⁶ Cf. Communication des griefs, pages 16 à 18, points 64 à 68.

- *Manage newsletters_Luxembourg* (cf. ligne 12);
- *Document the business_Luxembourg* (cf. ligne 13);
- *Manage the contractor relationship_Luxembourg* (cf. ligne 14);
- *Sharing of personal data with recipients in order to carry out business changes_Luxembourg* (cf. ligne 15);
- *Sharing of personal data with recipients for communication between employees and external professionals for business purposes_Luxembourg* (cf. ligne 16);
- *Carry out analysis for increases business insights and business planning (controller)_Luxembourg* (cf. ligne 17);
- *Evaluate and follow-up on the recruitment process_Luxembourg* (cf. ligne 18);
- *Carry out analysis for increased business insights and business planning_Luxembourg* (cf. ligne 19);
- *Manage and defend legal claims in relation to clients/suppliers, Customer (consumer), Other external persons and Visitors_Luxembourg* (cf. ligne 20);
- *Archiving of data used to manage the employment relationship_Luxembourg* » (cf. ligne 21);
- *Manage skills development_Luxembourg* (cf. ligne 22) ;
- *Sharing of personal data with hotels, conference centers and travel agencies in order to manage an assignment_Luxembourg* (cf. ligne 23);
- *Carry out salary reviews_Luxembourg* (cf. ligne 24);
- *Fulfil legal obligations towards employees, prospective employees, consultants, board members and visitors_Luxembourg* (cf. ligne 25);
- *Sharing of personal data with recipients in order to manage and defend legal claims_Luxembourg* (cf. ligne 26);
- *Archiving of investigations made and actions taken for security in relation to employees and consultants_Luxembourg* (cf. ligne 27);
- *Sharing of personal data with providers [...] (cf. ligne 28);*
- *Ensure technical functionality and security of our services (controller)_Luxembourg* (cf. ligne 29);
- *Manage and distribute work and measurement of performance_Luxembourg* (cf. ligne 32);
- *Manage orders of goods and services from Customer (consumer)_Luxembourg* (cf. ligne 33);
- *Manage the employment relationship_Luxembourg* (cf. ligne 34);

- *Manage the contractual relationship with the customer (consumer)_Luxembourg* (cf. ligne 36);
- *External communication regarding the business and business changes_Luxembourg* (cf. ligne 37);
- *Manage the client/supplier relationship_Luxembourg* (cf. ligne 38);
- *Fulfil legal obligations in relation to clients/suppliers, Customer (consumer), Other external persons and Visitors_Luxembourg* (cf. ligne 39);
- *Procurement of a client/supplier_Luxembourg* (cf. ligne 40) ;
- *Administration to facilitate worker communication_Luxembourg* (cf. ligne 41);
- *Sharing of personal data with group internal recipients for business purposes_Luxembourg* (cf. ligne 42);
- *Sharing of personal data with [...](cf. ligne 43);*
- *Manage and defend legal claims in relation to Employees, prospective employees, Board members, Consultants_Luxembourg* (cf. ligne 44);
- *Carry out external surveys including client satisfaction_Luxembourg* (cf. ligne 45);
- *Sharing personal data with the employer in order to manage the contractor relationship_Luxembourg* (cf. ligne 46);
- *Camera surveillance for the purposes of preventing, exposing and investigating crime_Luxembourg* (cf. ligne 47);
- *Carry out investigations and for security in relation to visitor_Luxembourg* (cf. ligne 48);
- *Sharing of personal data with pension and insurance administrators and brokers in order to manage salary and employment benefits_Luxembourg* (cf. ligne 49); et
- *Archiving of data used to facilitate worker communication_Luxembourg* (cf. ligne 50).

41. La Formation Restreinte rappelle que l'article 30 (1) f) du RGPD exige que les délais prévus pour l'effacement des différentes catégories de données doivent, dans la mesure du possible, figurer dans le registre des activités de traitement. Cette obligation est liée au principe de la limitation de la conservation prévu à l'article 5 (1) e) du RGPD qui exige que les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire pour la réalisation des finalités pour lesquelles elles ont été collectées. Au-delà, ces données doivent être supprimées ou anonymisées. Dans ce sens, le considérant (39) du RGPD précise qu' « [a]fin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, des délais devraient être fixés par le responsable de traitement pour leur effacement ou pour un examen périodique ». Toutefois, le RGPD n'exige pas de délai

d'effacement déterminé pour les différentes catégories de données en vertu de l'article 30 (1) f) du RGPD mais, dans la mesure du possible, un délai d'effacement déterminable.

42. A l'instar du chef d'enquête et considérant les 46 catégories de données susmentionnées, la Formation Restreinte estime que le délai d'effacement devrait être déterminé ou au moins déterminable. En ce sens, elle constate que l'information sur le délai d'effacement faisait défaut par rapport aux 46 catégories de données susmentionnées et qu'une telle information apparaissait uniquement par rapport aux traitements précisés aux lignes 30, 31, 35, 51 et 52.

Dès lors, la Formation Restreinte se rallie à l'avis du chef d'enquête et retient que le contrôlé a manqué à son obligation découlant de l'article 30 (1) f) du RGPD.

f) Quant à la description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32 (1) du RGPD (article 30 (1) g) du RGPD)

43. Il résultait du premier registre des traitements que la colonne T intitulée « *Technical Security Measures - Assets* » et la colonne U intitulée « *Organizational Security Measures – Assets* » ne contenaient aucune description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32 (1) du RGPD, à l'exception des lignes 7, 12, 29, 51 et 52 qui contenaient une telle description générale pour les traitements y précisés³⁷.

44. La Formation Restreinte rappelle que l'article 30 (1) g) du RGPD exige qu'une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32 (1) du RGPD doit, dans la mesure du possible, figurer dans le registre des activités de traitement et ce pour chaque traitement mentionné dans le registre. Le chef d'enquête précise dans sa communication des griefs qu'il considère qu'au cas où aucune mesure de sécurité technique ou organisationnelle ne serait applicable pour un traitement spécifique, il serait alors nécessaire de préciser ce constat explicitement dans le registre des activités de traitement. La Formation Restreinte partage cette compréhension de l'article 30 (1) g) du RGPD car elle est d'avis que le registre des activités de traitement doit être suffisamment complet pour qu'une autorité de contrôle puisse vérifier, dans la mesure du possible, si une

³⁷ Uniquement pour les cinq traitements suivants le premier registre des traitements précisait des mesures de sécurité techniques et organisationnelles :

- *Ensure technical functionality and security of our services_Luxembourg* (cf. ligne 7);
- *Manage newsletters_Luxembourg* (cf. ligne 12);
- *Ensure technical functionality and security of our services (controller)_Luxembourg* (cf. ligne 29);
- *Protective service: Mobile Guarding – Call-out* (cf. ligne 51); et
- *Protective service: Collectieve surveillance* (cf. ligne 52).

mesure mentionnée dans le registre est appropriée pour garantir la sécurité du traitement de données en question.

Dès lors, la Formation Restreinte se rallie à l'avis du chef d'enquête et retient que le contrôlé a manqué à son obligation découlant de l'article 30 (1) g) du RGPD.

45. Au vu de ce qui précède aux points 25 à 44 de la présente décision, la Formation Restreinte conclut qu'au début de l'enquête de la CNPD, le contrôlé a manqué à son obligation découlant de l'article 30 (1) a), c), d), e), f) et g) du RGPD.

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

1. Sur les principes

46. 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 ».

47. 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.

48. L'article 83 (1) du RGPD prévoit que chaque autorité de contrôle veille à ce que les amendes administratives imposées soient, dans chaque cas, effectives, proportionnées et dissuasives.

49. L'article 83 (2) précise les critères 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 ».

50. L'imposition des amendes administratives a été explicitée par le Groupe de Travail Article 29 dans ses « Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679 » (WP 253) adoptées le 3 octobre 2017 (ci-après : les « Lignes directrices sur l'application et la fixation des amendes »). Ces lignes directrices ont été approuvées par le Comité Européen de la Protection des données (ci-après : le « CEPD »)³⁸.

La Formation Restreinte souligne que les Lignes directrices sur l'application et la fixation des amendes ont été complétées par les « Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD » du CEPD dont la version 2.1 a été adoptée le 24 mai 2023 (ci-après : les « Lignes directrices sur le calcul des amendes »). Ces lignes directrices spécifient une méthode que les autorités de contrôle peuvent appliquer afin de calculer les amendes administratives à la lumière des circonstances de chaque cas d'espèce.

³⁸ CEPD, Décision « Endorsement 1/2018 » du 25 mai 2018.

Cette méthode est composée de cinq étapes³⁹. Toutefois, les autorités de contrôle ne sont pas tenues d'appliquer toutes les étapes, si ces dernières ne sont pas pertinentes dans un cas donné, ni d'exposer des motivations relatives aux aspects des lignes directrices qui sont sans objet⁴⁰.

51. La Formation Restreinte tient à préciser que les faits et éléments pris en compte dans le cadre de la présente décision sont ceux existants au début de l'enquête, tels qu'ultérieurement commentés par le contrôlé. Les éventuelles modifications effectuées par le contrôlé au cours de l'enquête et avant la prise de décision de la Formation Restreinte, même si elles permettent d'établir entièrement ou partiellement la conformité, ne permettent pas d'annuler rétroactivement un manquement constaté (cf. Tribunal administratif, jugement du 14 mai 2024, N° 46401 du rôle, ECLI:LU:TADM:2024:46401, p.26/27).

52. 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, peuvent être prises en compte par la Formation Restreinte dans le cadre des éventuelles mesures correctrices à prononcer et/ou d'une éventuelle amende administrative à prononcer.

2. En l'espèce

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

53. Dans la communication des griefs, le chef d'enquête a proposé à la Formation Restreinte de prononcer à l'encontre du contrôlé une amende administrative d'un montant de 2.784 euros.

54. Quant au degré de gravité des violations commises, le chef d'enquête a évalué les critères de l'article 83 (2) et il a précisé que « *la classification du degré de gravité des violations est à considérer comme faible* »⁴¹.

55. Le contrôlé, dans ses observations écrites en réponse à la communication des griefs, a remercié le chef d'enquête d'avoir tenu compte de son quatrième registre des traitements (i.e. la version du 12 novembre 2024) pour déterminer les mesures correctrices pertinentes dans sa communication des griefs. Il a également envoyé le cinquième registre

³⁹ Lignes directrices sur le calcul des amendes, page 10 ; pour une vue d'ensemble de la méthode, voir point 17 des lignes directrices.

⁴⁰ Lignes directrices sur le calcul des amendes, point 6.

⁴¹ Cf. Communication des griefs, page 32, point 108.

des traitements (une version modifiée par rapport à son quatrième registre des traitements) pour démontrer son « *engagement en matière de conformité* » et sa « *coopération continue avec la CNPD* ». ⁴²

56. Dans sa réponse à l'invitation à la séance de délibération de la Formation Restreinte du 26 juin 2025, le contrôlé a envoyé le sixième registre des traitements (la version du 11 juin 2025).

57. Lors de la séance de la Formation Restreinte du 26 juin 2025, le contrôlé a réitéré ses propos et il a souligné l'importance qu'il donne à la protection des données à caractère personnel. Son représentant légal a remarqué que, selon elle, les griefs contenus dans la communication des griefs, étaient des griefs basics et que son client avait fait beaucoup d'efforts tout au long de la procédure d'enquête pour améliorer son registre des activités de traitement. Selon elle, le chef d'enquête n'avait pas uniquement mais surtout soulevé des défauts et des facteurs aggravants et que l'appréciation des facteurs atténuants avait été négligée et qu'elle aurait souhaité recevoir d'abord une mise en demeure avant qu'une décision soit prise par la Formation Restreinte.

58. La Formation Restreinte se focalisera ci-dessous sur l'analyse des critères qui sont nécessaires pour décider s'il y a lieu d'imposer une amende administrative et, le cas échéant, du montant de l'amende administrative en vertu de l'article 83 du RGPD. La Formation Restreinte appliquera dans ce contexte la méthode composée de cinq étapes qui est spécifiée dans les Lignes directrices sur le calcul des amendes.

2.1.1. Étape 1 : Recenser les opérations de traitement en l'espèce

59. Conformément aux Lignes directrices sur le calcul des amendes, il est essentiel que l'autorité de contrôle détermine, en premier lieu, si un seul ou plusieurs comportements du contrôlé sont passables de sanctions et si ces derniers donnent lieu à une ou plusieurs violations imputables au contrôlé compte tenu des circonstances de l'espèce ⁴³.

60. Lesdites lignes directrices précisent que lorsqu'il est question d'évaluer une même opération de traitement ou des opérations de traitement liées, l'autorité de contrôle peut prendre en considération, dans le cadre de son appréciation des violations, toutes les obligations nécessaires sur le plan juridique pour que les opérations de traitement soient

⁴² Cf. Courrier du contrôlé du 13 mars 2025 en réponse à la communication des griefs.

⁴³ Lignes directrices sur le calcul des amendes, Chapitre 3 ; point 25 et s.

réalisées dans le respect des lois, y compris, par exemple, les obligations en matière de transparence (par exemple, l'article 13 du RGPD)⁴⁴.

61. En l'espèce, le contrôlé est à considérer comme responsable du traitement au sens du RGPD pour la mise en place du registre des traitements et pour les traitements y figurant au sens de l'article 30 (1) du RGPD (cf. point 20 de la présente décision). La mise en place d'un registre des activités de traitement est effectuée dans le cadre d'une volonté unitaire qui est étroitement liée sur le plan contextuel, spatial et temporel. En l'espèce, la Formation Restreinte estime donc qu'il s'agit de sanctionner un comportement unique au sens du chapitre 3.1 des Lignes directrices sur le calcul des amendes.

2.1.2. Étape 2 : Fixer le montant de départ pour le calcul ultérieur de l'amende

62. Conformément aux Lignes directrices sur le calcul des amendes, l'autorité de contrôle doit, en deuxième lieu, fixer le montant de départ pour le calcul ultérieur de l'amende eu égard aux circonstances en l'espèce⁴⁵ et ce sur base de l'évaluation de trois éléments :

- la classification de la violation en vertu de l'article 83 (4) à (6) du RGPD ;
- la gravité de la violation ; et
- le chiffre d'affaires de l'entreprise⁴⁶.

2.1.2.1. La classification des violations en vertu de l'article 83 (4) à (6) du RGPD

63. S'agissant de la classification des violations, le RGPD prévoit deux catégories, à savoir les violations punissables en vertu de l'article 83 (4) du RGPD et les violations punissables en vertu de l'article 83 (5) et (6) du RGPD. En ce qui concerne la première catégorie de violations, le montant maximal de l'amende pouvant être retenu s'élève à 10 millions d'euros ou à 2% du chiffre d'affaires annuel de l'entreprise, le montant le plus élevé étant retenu. En ce qui concerne la deuxième catégorie de violations, le montant maximal de l'amende pouvant être retenu s'élève à 20 millions d'euros ou à 4% du chiffre d'affaires annuel de l'entreprise, le montant le plus élevé étant retenu.

⁴⁴ Lignes directrices sur le calcul des amendes, point 27.

⁴⁵ Lignes directrices sur le calcul des amendes, Chapitre 4.

⁴⁶ Lignes directrices sur le calcul des amendes, point 48.

64. Par cette catégorisation, le législateur européen a donné une première indication (abstraite) de la gravité de la violation. En effet, plus la violation est grave, plus l'amende est susceptible d'être élevée⁴⁷.

65. La Formation Restreinte constate que le manquement reproché au contrôlé, notamment le manquement à l'article 30 (1) a), c), d), e), f) et g) du RGPD, est classé dans la disposition de l'article 83 (4) du RGPD, c'est-à-dire que ce manquement appartient à la première catégorie de violations et donc des violations moins graves.

2.1.2.2. La gravité de la violation

66. S'agissant de la détermination de la gravité de la violation, il convient d'examiner la nature, la gravité et la durée de la violation (article 83 (2) a) du RGPD), ainsi que son caractère délibéré ou négligent (article 83 (2) b) du RGPD) et les catégories de données à caractère personnel concernées par la violation (article 83 (2) g) du RGPD)⁴⁸.

67. Quant à la nature de la violation (article 83 (2) a) du RGPD), la Formation Restreinte retient en ce qui concerne le manquement à l'article 30 (1) a), c), d), e), f) et g) du RGPD que le législateur européen a entendu renforcer les obligations de documentation du responsable de traitement en les obligeant à documenter tous leurs traitements de données dans un registre des activités de traitement. Ledit registre est censé faciliter l'analyse et le recensement de l'ensemble des traitements de données du responsable du traitement et, partant, la démonstration de sa conformité au RGPD.

68. Quant à la gravité de la violation (article 83 (2) a) du RGPD), la Formation Restreinte tient compte du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi.

69. En ce qui concerne le nombre de personnes concernées affectées, la Formation Restreinte note que le contrôlé emploie [plus que 250] employés⁴⁹ et que le nombre de personnes tierces éventuellement concernées est indéfini.

70. En ce qui concerne le niveau de dommage subi par les personnes concernées affectées, elle estime que les personnes concernées n'ont pas subi un dommage en raison du registre des traitements incomplet.

⁴⁷ Lignes directrices sur le calcul des amendes, points 49. et 50.

⁴⁸ Lignes directrices sur le calcul des amendes, point 51 et s.

⁴⁹ Cf. Courrier du contrôlé du 26 avril 2024 ; Pièces n° 13 et 16 de la communication des griefs.

71. Quant au critère de la durée de la violation (article 83 (2) a) du RGPD), la Formation Restreinte note que le RGPD étant entré en vigueur en mai 2018, la durée de la violation au jour de la visite sur place du 18 mars 2024 était au moins de 5 ans et 10 mois.

72. Quant à la question de savoir si la violation a été commise délibérément ou par négligence (article 83 (2) b) du RGPD), la Formation Restreinte rappelle qu'une amende administrative en application de l'article 83 du RGPD peut être imposée uniquement s'il est établi que le responsable du traitement a commis, délibérément ou par négligence, une violation visée aux paragraphes (4) et (6) de cet article⁵⁰.

73. L'« *intention* », c'est-à-dire une infraction commise délibérément, comprend à la fois la connaissance et la volonté en rapport avec les caractéristiques d'une infraction, tandis que « *non délibérément* » (par négligence) 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 législation⁵¹.

74. La Formation Restreinte considère que le contrôlé ne pouvait pas ignorer l'existence de l'obligation violée⁵². Elle se rallie au chef d'enquête qui a estimé que la violation résulte « *d'une mauvaise exécution de cette obligation ainsi que d'un manque de vérification adéquate par le [c]ontrôlé* »⁵³.

75. Au vu de ce qui précède, la Formation Restreinte est d'avis que les faits et le manquement constaté ne traduisent pas une intention délibérée de violer le RGPD dans le chef du contrôlé. Néanmoins, elle retient que le manquement a été commis par négligence.

76. Quant aux catégories de données à caractère personnel concernées (article 83 (2) g) du RGPD), la Formation Restreinte retient que le registre des traitements ne contient que peu de données à caractère personnel⁵⁴.

⁵⁰ Dans un arrêt du 5 décembre 2023, la CJUE (grande chambre) a jugé qu'une amende administrative en application de l'article 83 du RGPD peut être imposée « *uniquement s'il est établi que le responsable du traitement, qui est à la fois une personne morale et une entreprise, a commis, délibérément ou par négligence, une violation visée aux paragraphes 4 à 6 de cet article* ». A cet égard, la CJUE a précisé « *qu'un responsable du traitement peut être sanctionné pour un comportement entrant dans le champ d'application du RGPD dès lors que ce responsable du traitement ne pouvait ignorer le caractère infractionnel de son comportement, qu'il ait eu ou non conscience d'enfreindre les dispositions du RGPD [...]* » (Arrêts du 5 décembre 2023 (grande chambre), *Deutsche Wohnen*, C-807/21, ECLI:EU:C:2023:950, point 76).

⁵¹ Lignes directrices sur l'application et la fixation des amendes, pages 11 à 12.

⁵² Arrêts du 5 décembre 2023 (grande chambre), *Deutsche Wohnen*, C-807/21, ECLI:EU:C:2023:950, point 76 et *Nacionalinis visuomenės sveikatos centras*, C-683/21, ECLI:EU:C:2023:949, point 81.

⁵³ Communication des griefs, point 96.

⁵⁴ Uniquement le nom et les coordonnées du délégué à la protection des données.

77. Compte tenu de son évaluation des critères pertinents de l'article 83 (2) a), b) et g) du RGPD ci-dessus, la Formation Restreinte estime que la classification du degré de gravité de la violation est à considérer comme faible.

2.1.2.3. Le chiffre d'affaires de l'entreprise

78. Pour finir l'étape 2, la Formation Restreinte prend en compte le chiffre d'affaires de l'entreprise conformément aux Lignes directrices sur le calcul des amendes⁵⁵.

79. La Formation Restreinte rappelle que conformément au droit de l'Union européenne et à la jurisprudence de la CJUE, c'est dans le contexte spécifique du calcul des amendes administratives qu'il y a lieu d'appréhender le renvoi, effectué au considérant (150) du RGPD, à la notion d'« entreprise » au sens des articles 101 et 102 du TFUE⁵⁶. Dès lors, la notion « entreprise » est définie comme l'« unité économique », qui consiste en une organisation unitaire d'éléments personnels, matériels et immatériels poursuivant de façon durable un but économique déterminé, même si, du point de vue juridique, cette unité économique est constituée de plusieurs personnes physiques ou morales⁵⁷.

80. Ainsi, elle considère qu'en l'espèce l'unité économique à prendre en compte, au regard de la violation en cause, est le groupe de sociétés dirigé par la Société B, une société de droit [...], qui détient de façon indirecte 99,9% du capital du contrôlé⁵⁸.

81. Elle note que le chiffre d'affaires net consolidé de la Société B pour l'année 2024 s'élevait à [...] ⁵⁹ [...] (soit EUR [entreprise dont le chiffre d'affaire est supérieur à 500 millions d'euros] ⁶⁰)⁶¹.

82. Par ailleurs, le chiffre d'affaires net du contrôlé pour l'année 2023 s'élevait à EUR [...] avec un bénéfice net de EUR [...] selon les comptes annuels de l'année 2023⁶². Par courriel du 9 juillet 2025, le contrôlé a précisé que ses comptes annuels de l'année 2024 ne sont pas encore finalisés.

⁵⁵ Cf. Lignes directrices sur le calcul des amendes, chapitre 4.3, points 63 à 69.

⁵⁶ Le traité sur le fonctionnement de l'Union européenne (TFUE).

⁵⁷ Arrêt du 5 décembre 2023, *Deutsche Wohnen*, C-807/21, ECLI:EU:C:2023:950, points 56 et 57 ; voir également Lignes directrices sur l'application et la fixation des amendes, page 6 et Lignes directrices sur le calcul des amendes, point 118. et s.

⁵⁸ Cf. Communication des griefs, point 7 et Pièces n° 2 et 5.

⁵⁹ [...].

⁶⁰ Conversion effectuée le 16 décembre 2025 sur xe.com.

⁶¹ Cf. Courriel du contrôlé envoyé à la Formation Restreinte en date du 9 juillet 2025.

⁶² Cf. Pièce n° 2 de la communication des griefs.

2.1.3. Étape 3 : Apprécier les circonstances aggravantes et atténuantes

83. Conformément aux Lignes directrices sur le calcul des amendes, l'autorité de contrôle doit, en troisième lieu, apprécier si des circonstances aggravantes ou atténuantes sont applicables aux circonstances de l'espèce⁶³. Les lignes directrices précisent que l'autorité de contrôle doit prendre qu'une seule fois en considération chaque critère prévu à l'article 83 (2) du RGPD. Ainsi, après avoir évalué, à l'étape 2, la nature, la gravité, et la durée de la violation (article 83 (2) a) du RGPD), de même que son caractère délibéré ou négligent (article 83 (2) b) du RGPD), et les catégories de données à caractère personnel concernées (article 83 (2) g) du RGPD), la Formation Restreinte va évaluer les autres circonstances aggravantes et atténuantes au titre de l'article 83 (2) du RGPD (article 83 (2) points c), d), e), f), h), i), j) et k) du RGPD)⁶⁴.

84. 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 estime, dans un premier temps, que les personnes concernées n'ont subi aucun dommage (cf. point 70 de la présente décision). Ensuite, elle note, sans préjuger du caractère satisfaisant des mesures prises par le contrôlé, que le contrôlé a modifié le premier registre des traitements à plusieurs reprises depuis le début de l'enquête. Elle note également que le chef d'enquête a tenu compte du quatrième registre des traitements (dernière version du registre envoyé avant l'envoi de la communication des griefs) pour déterminer les mesures correctrices dans sa communication des griefs. En outre, elle considère notamment les trois versions modifiées de son registre que le contrôlé a envoyé après la réception de la communication des griefs en vue de remédier aux manquements y soulevés par le chef d'enquête. Ces mesures seront analysées au chapitre II.2., section 2.2. de la présente décision. En résumé, elle constate qu'il s'agit de mesures qui ont été mises en place pendant la procédure d'enquête et après l'envoi de la communication des griefs mais que toutes les mesures prises par le contrôlé n'ont été prises qu'après le début de l'enquête. Dès lors, la Formation Restreinte est d'avis que ces circonstances sont à considérer comme neutres.

85. Quant au degré de coopération établi avec la CNPD, en vue de remédier à la violation, et d'en atténuer les éventuels effets négatifs (article 83 (2) f) du RGPD), la Formation Restreinte note qu'au vu du dossier d'enquête et, notamment, des réponses délivrées par le contrôlé pendant la procédure d'enquête, il y a lieu de retenir que la coopération du contrôlé

⁶³ Lignes directrices sur le calcul des amendes, Chapitre 5.

⁶⁴ Lignes directrices sur le calcul des amendes, points 70 à 72.

était bonne. Toutefois, elle rappelle que le contrôlé est soumis à une obligation générale de coopération en vertu de l'article 31 du RGPD. Dès lors, elle est d'avis que ces circonstances sont à considérer comme neutres.

86. Quant à toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce (article 83 (2) k) du RGPD), le chef d'enquête a relevé « *à titre de circonstances aggravantes, qu'en l'espèce, il pouvait raisonnablement être attendu du [c]ontrôlé, compte tenu de sa taille et de ses ressources, qu'il mette en place un [r]egistre des traitements conforme aux prescrits du RGPD et que ce dernier présente toutes les informations requises au titre de l'article 30.1 du RGPD* ». ⁶⁵

87. A titre de circonstances atténuantes, le chef d'enquête a relevé que le contrôlé aurait complété et mise à jour son registre des activités de traitement suite à la visite sur place et aux questions subséquentes posées par les agents de la CNPD et qu'il ressortait de l'analyse du quatrième registre de traitement « *qu'une partie des violations établies dans la partie D supra de la [communication des griefs avaient] d'ores et déjà été corrigées* » ⁶⁶.

88. La Formation Restreinte tient compte des éléments susmentionnés et se rallie à l'avis du chef d'enquête.

89. 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 et que, partant, elle ne les analysera pas ⁶⁷.

90. Dès lors, compte tenu de l'évaluation des critères pertinents de l'article 83 (2) du RGPD, la Formation Restreinte considère que l'imposition d'une amende administrative se justifie pour le manquement retenu à l'article 30 (1) a), c), d), e), f) et g) du RGPD.

2.1.4. Étape 4 : Déterminer le montant maximal légal applicable

91. Conformément aux Lignes directrices sur le calcul des amendes, l'autorité de contrôle doit, en quatrième lieu, déterminer les montants maximaux légaux applicables ⁶⁸. Les lignes directrices rappellent que le RGPD n'attribue pas de montants fixes à des violations

⁶⁵ Communication des griefs, page 32, point 102..

⁶⁶ Communication des griefs, page 32, point 103.

⁶⁷ Lignes directrices sur le calcul des amendes, point 6.

⁶⁸ Lignes directrices sur le calcul des amendes, Chapitre 6.

spécifiques, mais que le RGPD prévoit des montants maximaux généraux. Dès lors, il y a lieu de s'assurer que ces montants maximaux ne sont pas dépassés⁶⁹.

92. La Formation Restreinte a déjà relevé que le chiffre d'affaires net consolidé de la Société B pour l'année 2024 s'élevait à [...] (soit [EUR [entreprise dont le chiffre d'affaire est supérieur à 500 millions d'euros]]) (cf. point 81 de la présente décision).

93. La Formation Restreinte constate que dans la mesure où le manquement unique reproché au contrôlé (notamment le manquement à l'article 30 (1) a), c), d), e), f) et g) du RGPD) est classé dans la disposition de l'article 83 (4) du RGPD, le montant maximal de l'amende pouvant être retenu s'élève à 10 millions d'euros ou à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent⁷⁰ de l'entreprise, « *le montant le plus élevé étant retenu* », conformément à l'article 83 (4) du RGPD. Dès lors, la Formation retient qu'en l'espèce le montant maximal d'une amende administrative s'élève à [...] (c'est-à-dire, 2% du chiffre d'affaires annuel de l'entreprise)⁷¹.

94. En l'espèce, compte tenu des étapes 1 à 4 de la présente décision (cf. points 59 à 93), et plus particulièrement du fait qu'un manquement unique a été retenu en l'espèce, de la classification du manquement retenu au titre de l'article 83 (4) du RGPD, de sa gravité faible et de l'appréciation des circonstances aggravantes et atténuantes en l'espèce, la Formation Restreinte considère que l'amende administrative à imposer devrait s'élever à un montant de 2.784 (deux mille sept cent quatre-vingt-quatre) euros.

2.1.5. Étape 5 : Déterminer si le montant final de l'amende calculée est bien effectif, proportionné et dissuasif

95. Conformément aux Lignes directrices sur le calcul des amendes, l'autorité de contrôle doit, en cinquième lieu, veiller à ce que l'amende administrative imposée pour la ou les violations du RGPD visées à l'article 83 (4) à (6) soit, dans chaque cas, effective, proportionnée et dissuasive, tel que l'exige l'article 83 (1) du RGPD⁷². Selon le CEPD, il revient à l'autorité de contrôle de vérifier si le montant de l'amende retenue répond à ces exigences ou si d'autres ajustements du montant sont nécessaires⁷³.

⁶⁹ Lignes directrices sur le calcul des amendes, points 112. et 113.

⁷⁰ Le terme « précédent » se rapporte à l'année précédant la prise de décision d'infliger une amende émise par l'autorité de contrôle (cf. Lignes directrices sur le calcul des amendes, point 131).

⁷¹ Selon la fourchette évolutive précisée au point 115 et s. des Lignes directrices sur le calcul des amendes.

⁷² Lignes directrices sur le calcul des amendes, Chapitre 7.

⁷³ Lignes directrices sur le calcul des amendes, point 132.

96. La Formation Restreinte considère que le montant de l'amende 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

97. Dans la communication des griefs, le chef d'enquête a également proposé à la Formation Restreinte d'adopter les mesures correctrices suivantes (hors amende administrative) et il a confirmé avoir tenu compte du quatrième registre des traitements (version envoyée le 12 novembre 2024) pour la détermination de ces mesures⁷⁴ :

- *« rappeler à l'ordre le [c]ontrôlé quant à la nécessité d'inclure, de manière complète, correcte et précise, dans le [r]egistre des traitements les informations requises au titre de l'article 30.1 a), c), d), e), f) et g) du RGPD ;*
- *prononcer à l'encontre du [c]ontrôlé, et lui donner pour s'y conformer un délai de **1 (un) mois** à compter de la notification de la décision sur l'issue de l'enquête, une injonction de mettre en conformité la Version modifiée du Registre des traitements [version modifiée le 12 novembre 2024] avec les dispositions de l'article 30.1 c), e), f) et g) du RGPD et plus précisément de compléter la Version modifiée du Registre des traitements [version modifiée le 12 novembre 2024] comme suit :*
 - *en renseignant les descriptions de chaque catégorie de données traitées, par exemple, en listant, pour chaque catégorie, des exemples des types de données traitées,*
 - *en renseignant, pour chaque traitement, de manière affirmative ou négative, l'existence de transferts de données à caractère personnel vers des pays tiers,*
 - *en indiquant, de façon déterminée ou déterminable, les délais prévus pour l'effacement des différentes catégories de données traitées,*
 - *en fournissant pour chaque traitement, dans la mesure où il en existe, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32.1 du RGPD, sinon en indiquant de*

⁷⁴ Cf. Communication des griefs, page 27, point 92.

manière expresse l'absence de mesures de sécurité techniques et organisationnelles,

et de communiquer tout justificatif à même de rapporter la preuve du respect de la présente injonction ; [...] »⁷⁵.

98. Quant aux mesures correctrices proposées par le chef d'enquête et par référence au point 52 de la présente décision, la Formation Restreinte tient compte des démarches effectués par le contrôlé afin de se conformer aux dispositions du RGPD, telles que détaillées i) dans son courriel du 19 mars 2024 (y inclus le deuxième registre des traitements), ii) dans son courriel du 26 avril 2024 (y inclus le troisième registre des traitements), iii) dans son courriel du 12 novembre 2024 (y inclus le quatrième registre des traitements), iv) dans son courriel du 24 janvier 2025, v) dans son courriel du 13 mars 2025 (y inclus le cinquième registre des traitements), vi) dans son courriel du 11 juin 2025 (y inclus le sixième registre des traitements) et vii) dans son courriel du 9 juillet 2025 (y inclus le septième registre des traitements).

99. Quant au rappel à l'ordre (cf. point 97 premier point de la présente décision) proposé par le chef d'enquête pour le manquement retenu en vertu de l'article 30 (1) a), c), d), e), f) et g) du RGPD, la Formation Restreinte considère les mesures de mise en conformité prises par le contrôlé en l'espèce et estime qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête à cet égard.

100. Quant à l'ordre de mise en conformité du traitement (cf. point 97 deuxième point de la présente décision) proposé par le chef d'enquête pour le manquement retenu en vertu de l'article 30 (1) c), e), f) et g) du RGPD, la Formation Restreinte note

- en ce qui concerne l'article 30 (1) c) du RGPD, que le septième registre des traitements (la dernière version transmise) contient désormais dans ses colonnes H « Data Subject – Personal Data », I « *Data Category – Personal Data* » et J « Data Element, Personal Data » des descriptions suffisamment précises de catégories de personnes concernées et de catégories de données traités ;
- en ce qui concerne l'article 30 (1) e) du RGPD, que le septième registre des traitements (la dernière version transmise) renseigne désormais dans ses colonnes M « *Cross-Border Transfer (EU/EEA to Third Country)* » et N « *Cross-Border Transfer*

⁷⁵ Communication des griefs, page 33 à 34, point 114.

Mechanism(s) for the Processing Activity » pour chaque traitement, de manière affirmative ou négative, l'existence de transferts de données à caractère personnel vers des pays tiers et l'identification des pays tiers et si les transferts vers ces derniers sont couverts par une décision d'adéquation ou des garanties appropriées ;

- en ce qui concerne l'article 30 (1) f) du RGPD, que le septième registre des traitements (la dernière version transmise) contient désormais dans sa colonne L « *Data Retention* » des délais déterminée ou déterminable pour l'effacement de l'ensemble des catégories de données traitées ; et

- en ce qui concerne l'article 30 (1) g) du RGPD, que le septième registre des traitements (la dernière version transmise) contient désormais dans ses colonnes P « *Technical Security Measures – Storage/Processing (Assets)* » et Q « *Organisational Security Measures – Storage/Processing (Assets)* » une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32.1 du RGPD pour chaque traitement, à l'exception du traitement intitulé « *HSE : Whistleblowing handling* » (ligne 33) qui ne contient aucune information aux colonnes P et Q et qui n'indique pas non plus de manière explicite que des mesures de sécurité techniques et organisationnelles ne seraient pas applicable pour ledit traitement de données.

En considération des mesures de mise en conformité insuffisantes prises par le contrôlé en l'espèce, la Formation Restreinte estime dès lors qu'il y a lieu de prononcer la mesure correctrice proposée par le chef d'enquête mais uniquement par rapport à la mesure correctrice proposée concernant l'article 30 (1) g) du RGPD et dans ce cadre uniquement pour le traitement « *HSE : Whistleblowing handling* » (ligne 33 du septième registre des traitements).

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

- de retenir le manquement à l'article 30 (1) a), c), d), e), f) et g) du RGPD ;
- de prononcer à l'encontre de la Société A un rappel à l'ordre pour avoir manqué à l'article 30 (1) a), c), d), e), f) et g) du RGPD ;
- de prononcer à l'encontre de la Société A une injonction de mettre en conformité un seul traitement de données dans sa dernière version de son registre des activités de traitement

avec l'article 30 (1) g) du RGPD, dans un délai de 1 (un) mois suivant la notification de la décision de la Formation Restreinte, et, plus précisément, d'inclure pour le traitement « *HSE : Whistleblowing handling* » (ligne 33) une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32.1 du RGPD ou d'indiquer de manière explicite l'absence de mesures de sécurité techniques et organisationnelles pour ce traitement de données ;

- de prononcer à l'encontre de la Société A une amende administrative d'un montant de 2.784 (deux mille sept cent quatre-vingt-quatre) euros au regard du manquement à l'article 30 (1) a), c), d), e), f) et g) du RGPD.

Belvaux, le 16 décembre 2025.

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

Tine A. Larsen
Présidente

Marc Hemmerling
Membre suppléant

Romy Schaus
Membre suppléant

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.