Délibération SAN-2025-014 du 11 décembre 2025

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Etat juridique : En vigueur

Date de publication sur Légifrance : Vendredi 19 décembre 2025

Délibération de la formation restreinte n° SAN – 2025-014 du 11 décembre 2025 concernant la société MOBIUS SOLUTIONS LTD

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

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

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

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

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

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

Vu la décision n° 2023-206C du 25 septembre 2023 de la présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte du 30 avril 2025 ;

Vu le rapport de M. Claude CASTELLUCCIA, commissaire rapporteur, notifié à la société le 13 juin 2025 ;

Vu les observations écrites de la société MOBIUS SOLUTIONS LTD reçues le 29 juillet 2025 après que la société se soit vue accorder un délai supplémentaire de quinze jours pour répondre;

Vu la réponse du rapporteur notifiée à la société MOBIUS SOLUTIONS LTD le 8 août 2025 ;

Vu les observations écrites de la société MOBIUS SOLUTIONS LTD reçues le 23 septembre 2025 ;

Vu la clôture de l'instruction notifiée à la société MOBIUS SOLUTIONS LTD le 13 octobre 2025 ;

Vu la demande de report de la séance formulée par la société le 16 octobre 2025, et la réponse à cette demande adressée par le président de la formation restreinte à la société le 23 octobre 2025 ;

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

Vu les autres pièces du dossier,

Étaient présents, lors de la séance de la formation restreinte du 27 novembre 2025 :

- Monsieur Claude CASTELLUCCIA, commissaire, entendu en son rapport ;

- En qualité de représentants de la société MOBIUS SOLUTIONS LTD :

- [...]

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

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

I. Faits et procédure

1. Créée en février 2009, la société MOBIUS SOLUTIONS LTD, dont le nom commercial est " Optimove ", est une société israélienne domiciliée Adgar 360 Tower 2 Hashlosha Street 33 rd Floor à Tel Aviv (6706054 – Israël).

2. La société a pour activité le développement d'outils marketing. En 2023 et 2024, elle a déclaré réaliser un chiffre d'affaires exprimé en dollars américains s'élevant respectivement à [...]et [...] dollars, soit environ et respectivement [...] euros et [...]euros. La société a déclaré employer 238 personnes en 2023.

3. La société a développé et commercialise le système SAAS Optimove qui permet à ses clients de créer et d'exécuter des campagnes marketing personnalisées à destination de leurs propres clients via l'intégration de leurs données à ce système. Dans ce cadre, la société héberge les données de ses clients.

4. En sus de la fourniture de son système SAAS Optimove, accessible en ligne, la société analyse les données de ses clients, réalise un travail de conversion dans ses propres formats et de segmentation de ces données, afin de permettre à ses clients d'optimiser leurs campagnes marketing à destination de leurs propres clients.

5. Le 10 novembre 2022, la Commission nationale de l'informatique et des libertés (CNIL) a été destinataire d'une notification de violation de données à caractère personnel émanant de la société DEEZER et qui aurait concerné plusieurs millions d'utilisateurs de la plateforme dans le monde.

6. Cette notification désignait la société MOBIUS SOLUTIONS LTD, ancien sous-traitant de la société DEEZER qui lui fournissait sa solution " Optimove ", comme source probable de la violation de données.

7. Le 31 janvier 2023, la société DEEZER a transmis à la CNIL une notification de violation de données complémentaire, confirmant que, selon son analyse, l'origine de la violation de données résidait très certainement dans les systèmes de la société MOBIUS SOLUTIONS LTD.

8. Le 23 octobre 2023, en application de la décision n° 2023-206C de la présidente de la Commission du 25 septembre 2023, une délégation de contrôle de la CNIL a adressé un questionnaire à la société afin de vérifier la conformité à la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (loi Informatique et Libertés) et au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) des traitements mis en œuvre par elle ou pour son compte. La société a répondu le 12 janvier 2024.

9. Le 29 janvier 2024, des questions complémentaires ont été posées par la délégation de contrôle à la société, qui y a répondu le 8 février suivant.

10. Le 30 avril 2025, aux fins d'instruction de l'ensemble de ces éléments, la présidente de la CNIL a désigné Monsieur Claude CASTELLUCCIA en qualité de rapporteur.

11. Le 15 mai 2025, le rapporteur a adressé une demande complémentaire à la société en application de l'article 39 du décret n° 2019-536 du 29 mai 2019, à laquelle la société a répondu par courrier du 6 juin 2025.

12. Le 13 juin 2025, à l'issue de son instruction, le rapporteur a notifié à la société un rapport détaillant les manquements aux articles 28, 29 et 30 du RGPD qu'il estimait constitués. Ce rapport proposait à la formation restreinte de prononcer à l'encontre de la société une amende administrative. Il proposait également que cette décision soit rendue publique mais qu'il ne soit plus possible d'identifier nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

13. Par courriel du 7 juillet 2025, la société a sollicité un délai complémentaire auprès du président de la formation restreinte pour produire ses observations en réponse, accordé le 10 juillet 2025, sur le fondement de l'article 40, alinéa 4, du décret du 29 mai 2019.

14. Le 29 juillet 2025, la société a produit des observations en réponse.

15. Le 8 août 2025, le rapporteur a transmis à la société sa réponse, à laquelle la société a répondu par observations du 23 septembre 2025.

16. Le 13 octobre 2025, le rapporteur a notifié à la société la clôture de l'instruction.

17. Par courrier du même jour, la société a été informée de l'inscription du dossier à l'ordre du jour de la séance de la formation restreinte du 20 novembre 2025.

18. A la suite de la demande de renvoi de la société du 16 octobre 2025, le président de la formation restreinte a informé la société de l'inscription du dossier à l'ordre du jour de la séance de la formation restreinte du 27 novembre 2025.

19. A l'issue de la procédure contradictoire écrite, le rapporteur et la société ont présenté des observations orales lors de la séance de la formation restreinte.

II. Motifs de la décision

A. Sur l'applicabilité du RGPD

20. En vertu de l'article 3, paragraphe 2 du RGPD : " Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées : […]a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union ".

21. Le considérant 24 du RGPD précise que " Le traitement de données à caractère personnel de personnes concernées qui se trouvent dans l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union devrait également être soumis au présent règlement lorsque ledit traitement est lié au suivi du comportement de ces personnes dans la mesure où il s'agit de leur comportement au sein de l'Union. Afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit ".

22. Dans ses lignes directrices 3/2018 relatives au champ d'application territorial du RGPD dans leur version du 12 novembre 2019, le Comité européen de protection des données (CEPD) a précisé que si : " le considérant 24 porte exclusivement sur le suivi d'un comportement au moyen du pistage d'une personne sur l'internet, le comité estime que le pistage par d'autres types de réseaux ou de technologies impliquant un traitement des données à caractère personnel devrait également être pris en considération pour déterminer si une activité de traitement constitue le suivi d'un comportement, par exemple au moyen de dispositifs portables ou d'autres dispositifs intelligents ".

23. Ces mêmes lignes directrices retiennent que, " contrairement à la disposition de l'article 3, paragraphe 2, point a), ni l'article 3, paragraphe 2, point b), ni le considérant 24 n'introduisent expressément un degré nécessaire d'" intention de cibler " de la part du responsable du traitement ou du sous-traitant pour déterminer si l'activité de surveillance déclencherait l'application du RGPD aux activités de traitement. Toutefois, l'utilisation du mot " suivi " implique que le responsable du traitement poursuit un objectif spécifique en vue de la collecte et de la réutilisation ultérieure des données pertinentes relatives au comportement d'une personne au sein de l'Union. Le comité n'estime pas que la collecte ou l'analyse en ligne de données à caractère personnel relatives à des personnes dans l'Union serait automatiquement considérée comme un " suivi ". Il sera nécessaire de tenir compte de la finalité du traitement des données par le responsable du traitement et, en particulier, de toute analyse comportementale ou technique de profilage ultérieure impliquant ces données. Le comité tient compte du libellé du considérant 24, qui indique que pour déterminer si le traitement implique le suivi du comportement d'une personne concernée, le suivi des personnes physiques sur l'internet, y compris l'utilisation ultérieure potentielle de techniques de profilage, constitue un facteur important ".

24. Enfin, le CEPD dans ses lignes directrices indique que l'activité décrite à l'article 3, paragraphe 2, point b, englobe un large éventail d'activités dont la publicité comportementale.

25. S'agissant plus particulièrement des sous-traitants, ces lignes directrices précisent : " Lorsqu'il s'agit d'un sous-traitant non établi dans l'Union, afin de déterminer si son traitement peut être soumis au RGPD en application de l'article 3, paragraphe 2, il est nécessaire de vérifier si les activités de traitement du sous-traitant " sont liées " aux activités de ciblage du responsable du traitement. Le comité estime que, lorsque les activités de traitement d'un responsable du traitement sont liées à l'offre de biens ou de services ou au suivi du comportement des personnes dans l'Union (" ciblage "), tout sous-traitant chargé d'effectuer cette activité de traitement pour le compte du responsable du traitement relève du champ d'application du RGPD en vertu de l'article 3, paragraphe 2, en ce qui concerne ce traitement. Le caractère de " ciblage "

d'une activité de traitement est lié aux finalités et moyens de celle-ci ; la décision de cibler des personnes dans l'Union ne peut être prise que par une entité agissant en tant que responsable du traitement. Une telle interprétation n'exclut pas la possibilité que le sous-traitant puisse participer activement aux activités de traitement liées à la réalisation des critères de ciblage (c'est-à-dire que le sous-traitant offre des biens ou des services ou qu'il effectue un suivi pour le compte et sur instruction du responsable du traitement) ".

26. A titre d'exemple d'activités de sous-traitants participant à l'activité de ciblage du responsable de traitement à destination de personnes situées sur le territoire européen et donc soumises au RGPD, le CEPD vise notamment le ciblage publicitaire (exemple n° 19) ou l'hébergement de données (exemple n° 20).

27. Le rapporteur soutient que la CNIL est compétente, tant sur le fondement de l'article 3-2-a) du RGPD que sur celui de l'article 3-2-b) du même Règlement.

28. S'agissant de l'application de l'article 3-2-a) du RGPD, il considère que le traitement concerne des personnes, clientes de la société DEEZER, partout dans le monde, et en particulier au sein de l'Union européenne et en France. Il estime que l'activité de la société MOBIUS est liée à l'offre de services de la société DEEZER en ce qu'elle permet à cette dernière de réaliser des prestations de personnalisation et d'optimisation de campagnes marketing afin de proposer ses propres services de musique en streaming.

29. S'agissant de l'application de l'article 3-2-b) du RGPD, le rapporteur soutient que le traitement est également lié au suivi de comportement de personnes concernées se trouvant sur le territoire de l'Union européenne, en ce que l'activité de la société vise à créer des profils d'utilisateurs pour le compte de la société DEEZER, en créant des segments d'utilisateurs basés soit sur des critères socio-démographiques, soit sur des critères d'utilisation du service Deezer (par exemple, une campagne visant les utilisateurs abonnés depuis un nombre déterminé d'années ou ceux ayant sélectionné un grand nombre de favoris).

30. La société conteste la compétence de la CNIL et considère n'être qu'indirectement soumise à certaines obligations de l'article 28, paragraphe 3 du RGPD, imposées par la société DEEZER. Elle considère que les paragraphes 1 et 2 de l'article 3, ont un caractère alternatif. Enfin, elle considère que l'article 3-2-a) du RGPD ne peut qu'être appliqué à un responsable de traitement et non pas à un sous-traitant et qu'au sens de l'article 3-2-b), elle ne réalise pas de profils comportementaux des utilisateurs de la société DEEZER.

31. En l'espèce, la société ne disposant d'aucun établissement dans l'Union européenne, la formation restreinte considère que les paragraphes 1 et 2 de l'article 3, ont un caractère cumulatif au cas présent et qu'il convient de s'interroger sur son activité pour savoir si les traitements des données à caractère personnel qu'elle met en œuvre pour le compte de la société DEEZER sont ou non liés " au suivi du comportement des personnes dans la mesure où il s'agit de leur comportement au sein de l'Union ".

32. En premier lieu, la formation restreinte relève que la société MOBIUS SOLUTIONS LTD a transmis à la société DEEZER, à la suite de la violation de données dont cette dernière a été victime, la liste des différentes données concernant ses utilisateurs qu'elle traitait pour son compte et qui ont été divulguées dans le cadre de la violation de données. Apparaissent ainsi : l'identifiant ou l'identité de la personne, son pays, sa langue, son genre, son identifiant sur l'application, sa date de naissance, son inscription ou non à des newsletters de la société DEEZER, la date de création d'un compte, la date de création d'une session, le nombre d'écoutes de morceaux par jour, le nombre de playlists enregistrées, le nombre de playlists écoutées, la date du premier paiement, la totalité des paiements effectués, la moyenne d'écoutes de morceaux par jours, le cycle de vie, les indicateurs d'étapes du cycle de vie, la durée d'écoute par jour, les artistes favoris, le nombre de playlists créées, le nombre de clic de pause, le nombre de " loved " cliqué, etc.

33. Ces données constituent des données à caractère personnel des utilisateurs des services DEEZER, situés au sein de l'Union européenne et notamment en France. La société MOBIUS SOLUTIONS LTD a en effet précisé que le nombre d'utilisateurs en Europe, impactés par la violation de données, s'élevait à 21 574 775, dont 9 849 354 en France.

34. Par conséquent, la société traite des données à caractère personnel de personnes physiques situées dans l'Union européenne, et en particulier en France.

35. En second lieu, il convient de vérifier si l'activité de traitement en cause peut être considérée comme " liée au suivi du comportement " des personnes concernées au sens de l'article 3-2-b) du RGPD. Il y a lieu de relever que le RGPD n'est pas seulement applicable au traitement dont la finalité première est de suivre le comportement d'une personne résidant dans l'Union européenne, mais à tous les traitements qui sont " liés " à un tel suivi, c'est-à-dire qui sont effectués au moyen ou en lien avec des opérations de suivi des personnes résidant en Europe.

36. Il apparaît, dans la notification de violation de données auprès de la CNIL réalisée par la société DEEZER, que le traitement réalisé par la société MOBIUS SOLUTIONS LTD consistait en la création de segments " d'utilisateurs, basés soit

sur des critères socio-démographiques, soit sur des critères d'utilisation du service Deezer ". Le contrat conclu entre les sociétés mentionne explicitement son objet de " personnalisation marketing ".

37. La société MOBIUS SOLUTIONS LTD a confirmé réaliser des calculs à partir de diverses données relatives aux utilisateurs du service DEEZER et établir des segments d'utilisateurs, en fonction notamment de leurs habitudes d'écoute, en vue de permettre à DEEZER de personnaliser et adapter ses campagnes marketing afin d'optimiser l'engagement de ses clients sur ses propres services. La réalisation de ces segments implique une analyse du comportement des utilisateurs des services DEEZER, relatif à ces mêmes services, afin de leur adresser de la publicité comportementale. Contrairement à ce que soutient la société, il est dans ce contexte indifférent de savoir si les segments qu'elle réalisait étaient in fine utilisés ou non par la société DEEZER, le seul établissement de ces segments suffisant à caractériser une forme de suivi du comportement des personnes concernées.

38. La formation restreinte considère que le travail d'analyse et de segmentation réalisé par la société MOBIUS SOLUTIONS LTD à partir des données transmises par la société DEEZER doit être qualifié de profilage comportemental, lié au comportement des personnes au sein de l'Union, même si le périmètre du profil obtenu est limité à l'écoute de musique sur la plateforme DEEZER. Le traitement en cause amène en effet à la création d'un profil comportemental des personnes concernées.

39. La formation restreinte rappelle, en outre, que la seule activité d'hébergement des données de la société DEEZER par la société, en vue de la réalisation de l'activité de ciblage publicitaire, suffit à caractériser une activité de sous-traitance en lien avec le suivi du comportement des personnes selon les lignes directrices du CEPD.

40. Les traitements ainsi mis en œuvre sont bien liés au suivi du comportement des personnes concernées au sens des dispositions de l'article 3-2-b) du RGPD et relèvent du champ d'application territorial du RGPD, sans qu'il soit besoin de se prononcer sur l'applicabilité de l'article 3-2-a) du RGPD.

B. Sur la compétence de la CNIL et la non application du mécanisme du guichet unique

41. L'article 55, paragraphe 1, du RGPD prévoit que " chaque autorité de contrôle est compétente pour exercer les missions et les pouvoirs dont elle est investie conformément au présent règlement sur le territoire de l'État membre dont elle relève ".

42. L'article 56, paragraphe 1, du RGPD dispose que " sans préjudice de l'article 55, l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant, conformément à la procédure prévue à l'article 60 ".

43. Le considérant 122 du RGPD précise que " Chaque autorité de contrôle devrait être compétente sur le territoire de l'État membre dont elle relève pour exercer les missions et les pouvoirs dont elle est investie conformément au présent règlement. Cela devrait couvrir, notamment, […] le traitement effectué par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union lorsque ce traitement vise des personnes concernées résidant sur le territoire de l'État membre dont elle relève. […] ".

44. Il ressort d'une lecture combinée des articles 55 et 56 du RGPD que, dans l'hypothèse où un responsable de traitement ou un sous-traitant, implanté en dehors de l'Union européenne met en œuvre au sein de l'Union européenne, un traitement transfrontalier soumis au RGPD sans y disposer d'un établissement principal ni d'un établissement unique, le mécanisme du guichet unique prévu à l'article 56 du RGPD n'est pas applicable. Chaque autorité de contrôle nationale est donc compétente pour contrôler le respect du RGPD sur le territoire de l'Etat membre dont elle relève.

45. En l'espèce, la formation restreinte relève que la société est établie en Israël et ne dispose d'aucun établissement sur le territoire d'un État membre de l'Union européenne. Le mécanisme du guichet unique n'est donc pas applicable, et la CNIL est compétente pour contrôler la conformité des traitements mis en œuvre par la société MOBIUS SOLUTIONS LTD pour le compte de la société DEEZER sur le territoire français, conformément à l'article 55, paragraphe 1 du RGPD.

C. Sur le principe de courtoisie internationale invoqué par la société

46. La société soutient qu'étant établie en Israël, pays bénéficiant d'une décision d'adéquation de la Commission européenne n° C (2011)332 du 31 janvier 2011, la CNIL devrait renoncer à sa compétence en application du principe de courtoisie internationale.

47. En l'espèce, la formation restreinte relève tout d'abord que la décision d'adéquation de la Commission européenne n° 332 du 31 janvier 2011 ne s'applique que dans le cadre d'un transfert des données à caractère personnel de l'Union européenne vers un pays hors Union européenne, pour déterminer si le pays de transfert offre des garanties suffisantes en matière de protection des données. Dans le cadre de la présente procédure, aucun manquement n'est reproché à la

société au titre de transferts de données à caractère personnel, et seuls des manquements aux articles 28, 29 et 30 du RGPD sont allégués par le rapporteur.

48. Ensuite, elle note que le principe de courtoisie internationale consiste en un ensemble d'usages, non obligatoires, particulièrement usités dans le cadre des relations diplomatiques entre États. La formation restreinte rappelle que ses attributions lui sont conférées par le RGPD, dont les règles sont d'ordre public. Elle ne saurait donc écarter la mise en œuvre de ses compétences au regard du principe de courtoisie internationale.

49. Il résulte de l'ensemble de ces éléments que la CNIL est compétente pour contrôler la conformité des traitements mis en œuvre par la société MOBIUS SOLUTIONS LTD sur le territoire français.

D. Sur la qualité de la société vis-à-vis du traitement en cause

50. Aux termes de l'article 4, point 2, du RGPD, le traitement de données à caractère personnel s'entend comme " toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ".

51. L'article 4, point 7 du RGDP définit le responsable de traitement 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 ".

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

53. La formation restreinte relève que la société propose une solution d'analyse, de communication et de marketing, permettant de personnaliser et d'optimiser les campagnes marketing de ses clients, notamment d'emailing.

54. Il ressort de l'instruction que la société DEEZER, qui propose la mise à disposition de sa plateforme de musique accessible en streaming (sans enregistrement préalable) pour tous ses utilisateurs, a conclu un contrat avec la société MOBIUS SOLUTIONS LTD, qui a été exécuté du 1er décembre 2016 au 1er décembre 2020. Il ressort de ce contrat que la société MOBIUS SOLUTIONS LTD, désignée comme " fournisseur de services ", mettait à la disposition de la société DEEZER sa plateforme dite " Optimove, pour la personnalisation de campagnes marketing (…), qui analyse les données fournies par le client concernant ses clients et recommande certaines actions marketing. ". Le contrat précise qu'avant de permettre l'accès à cette plateforme, la société MOBIUS SOLUTIONS LTD devait recevoir des informations concernant les utilisateurs de la société DEEZER afin d'analyser ces données.

55. La formation restreinte considère qu'il résulte de l'ensemble de ces éléments que la société MOBIUS SOLUTIONS LTD agissait pour le compte de la société DEEZER, en qualité de sous-traitant, dans le cadre de l'exécution du contrat qui les liait, la société DEEZER définissant les finalités et les moyens du traitement.

56. Dans ces conditions, la formation restreinte considère que la société doit être regardée comme sous-traitante de la société DEEZER au sens de l'article 4, point 8, du RGPD dans la cadre de sa relation contractuelle avec cette dernière.

E. Sur le manquement à l'article 28.3 g) du RGPD

57. En droit, l'article 28.3 g) du RGPD dispose que le sous-traitant : " selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel ".

58. A titre d'éclairage, le considérant 81 du RGPD relève que : " […] Après la réalisation du traitement pour le compte du responsable de traitement, le sous-traitant devrait, selon le choix du responsable de traitement, renvoyer ou supprimer les données à caractère personnel, à moins que le droit de l'Union ou le droit d'Etat membre auquel le sous-traitant est soumis n'exige la conservation des données à caractère personnel ".

59. Aux termes de l'article 5.1 e) du RGPD, " Les données à caractère personnel doivent être : […] e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées […] ".

60. Il résulte de la lecture combinée de ces textes que les données d'un responsable de traitement ne doivent pas être conservées par un sous-traitant, au terme de la prestation que ce dernier réalisait et qui impliquait le traitement de ces données.

61. La CNIL a déjà sanctionné un sous-traitant pour une violation de l'article 28 du RGPD (en ce sens, CNIL, FR, 15 avril 2022, Sanction, SAN 2022-009, publié).

62. Le rapporteur soutient que la société aurait dû supprimer les données à caractère personnel des utilisateurs fournies par DEEZER à la fin de leur relation contractuelle le 1er décembre 2020, comme elle y était tenue par les dispositions contractuelles.

63. En défense, la société soutient que les données qui ont fait l'objet de la violation de données sont issues d'une copie non autorisée de données non anonymisées des utilisateurs de la société DEEZER, réalisée par trois de ses salariés dans le but d'améliorer les performances des services offerts à la société DEEZER. Elle indique n'avoir découvert cette copie qu'après avoir été informée par la société DEEZER de la violation de données, et avoir lancé une enquête interne en matière de cybersécurité de son environnement " cloud ", mettant à jour qu'entre le 31 octobre et le 5 novembre 2022, elle avait subi des coûts liés au trafic (coûts de bande passante) sur le compte stockant les données issues de cette copie alors que le mois précédent, aucun coût journalier ne lui avait été facturé. Elle ajoute ne pas avoir agi intentionnellement et avoir supprimé, au moment de la fin du contrat avec la société DEEZER, l'ensemble des données dont elle avait connaissance.

64. En l'espèce, la formation restreinte relève qu'il ressort de l'article 6.1.5 du contrat conclu entre la société MOBIUS SOLUTIONS LTD et la société DEEZER que toutes les données des clients devaient être supprimées des serveurs MOBIUS SOLUTIONS LTD à la résiliation du contrat. Celle-ci est intervenue le 1er décembre 2020. Si la société MOBIUS SOLUTIONS LTD indique avoir supprimé de ses systèmes toutes les données DEEZER dont elle avait connaissance, il n'en reste pas moins qu'en novembre 2022, elle a fait l'objet d'une violation de données concernant 46 millions de données non anonymisées d'utilisateurs DEEZER dans le monde, dont plus de 9 millions en France. Cette violation a eu lieu depuis un environnement de non-production appartenant à la société MOBIUS SOLUTIONS LTD. La société indique avoir supprimé la copie des données DEEZER le 1er octobre 2023, sur instruction de cette dernière.

65. La société fait valoir que les données ont été copiées à son insu par ses salariés et qu'elle n'en avait pas connaissance, ce qui justifierait selon elle qu'elle n'ait pu procéder à leur suppression à la fin de sa relation contractuelle avec la société DEEZER, le 1er décembre 2020. Toutefois, la formation restreinte observe que ces données ont été copiées en 2019, dans le cadre du contrat liant les deux sociétés, et stockées jusqu'au 1er octobre 2023, sur un environnement de non-production appartenant à la société MOBIUS SOLUTIONS LTD, dans le cadre de ses activités et dans son propre intérêt (l'amélioration de la performance des services offerts à DEEZER mais aussi de ses propres services liés à l'utilisation de sa plateforme Optimove). La formation restreinte considère qu'en ne supprimant pas la copie des données d'utilisateurs DEEZER à la fin de la relation contractuelle, comme elle y était tenue, elle a manqué à ses obligations en tant que sous-traitant et conservé ces données pour une durée excédant celle qui était nécessaire au regard des finalités pour lesquelles elles étaient traitées. La circonstance que la copie des données ait été réalisée par ses salariés, sans que la direction de MOBIUS SOLUTIONS LTD n'en ait eu connaissance, n'a aucune incidence sur ses obligations en tant que sous-traitant dès lors qu'il lui incombait de vérifier les opérations réalisées par les salariés placés sous sa responsabilité. La société ne saurait invoquer l'absence de maîtrise de ses outils ou l'absence de contrôle et de direction de l'activité de ses salariés pour éluder sa responsabilité, alors qu'il lui revenait de s'assurer des conditions du traitement qu'elle mettait en œuvre.

66. Il résulte de ces éléments que la société a conservé de manière injustifiée des données relatives aux utilisateurs de la société DEEZER après la fin de leur relation contractuelle, alors que ces données auraient dû être supprimées.

67. Par conséquent, la formation restreinte considère que la société a commis un manquement à l'article 28.3 g) du RGPD.

F. Sur le manquement à l'article 29 du RGPD

68. En droit, l'article 29 du RGPD dispose que " Le sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peut pas traiter ces données, excepté sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre ".

69. Le rapporteur relève que la société MOBIUS SOLUTIONS LTD a utilisé les données à caractère personnel des utilisateurs de la société DEEZER en dehors de toute instruction de cette dernière afin d'améliorer les performances de ses propres services.

70. En défense, la société considère que les données des utilisateurs de la société DEEZER ont fait l'objet d'une copie non autorisée par des salariés. Elle indique que cette copie avait pour finalité l'amélioration des performances des services

fournis à ses clients, dont DEEZER et que par conséquent, elle rentrait dans le cadre de la relation contractuelle. Elle estime donc ne pas avoir agi en dehors des instructions de la société DEEZER.

71. En l'espèce, la formation restreinte relève que, selon le contrat conclu entre la société DEEZER et la société MOBIUS SOLUTIONS LTD, cette dernière proposait sa plateforme Optimove (dit aussi " le système ") basée sur l'internet, qui analyse les données fournies par ses clients et recommandait certaines actions marketing. Les services proposés par la société MOBIUS SOLUTIONS LTD concernaient la fourniture et l'intégration des données de la société DEEZER à la plateforme " Optimove ".

72. La formation restreinte souligne que l'article 6 du contrat, portant sur la confidentialité des données transmises par la société DEEZER, insistait sur la nécessité de les protéger. En ce sens, des engagements successifs étaient pris par la société MOBIUS SOLUTIONS LTD pour protéger ces données. Il était ainsi précisé que la société n'avait " aucun droit sur ces données " et que la société DEEZER " rest[ait] le seul propriétaire des données " (article 6.1.3) ; que la société MOBIUS SOLUTIONS LDT " n'utilisera[it] pas les données à d'autres fins que celles de fournir au client les services prévus par le contrat " (6.1.4) et qu'à la résiliation du contrat, la société MOBIUS SOLUTIONS LTD supprimerait les données (6.1.5).

73. La formation restreinte note également que si le contrat, de façon incidente et en vue d'assurer la réparation de la plateforme " Optimove " ou sa mise à jour (articles 4.1 ou 7.2 par exemple), mentionne une coopération de la société DEEZER, il ne prévoit pas que la société MOBIUS puisse faire usage des données des utilisateurs de la société DEEZER en vue d'améliorer la performance des services proposés à la société DEEZER ni de manière générale la performance de ses propres services.

74. La formation restreinte relève que la société hébergeait les données de la société DEEZER sur ses serveurs. La société MOBIUS SOLUTIONS LTD a indiqué avoir, en cours d'exécution du contrat en avril 2019, copié des données à caractère personnel non anonymisées d'utilisateurs de la société DEEZER d'un environnement de production vers un environnement de non-production qui lui appartenait, afin de développer et tester des améliorations possibles de son système Optimove. Il résulte de ce qui précède que la copie des données réalisée à cette fin n'entrait pas dans le champ du contrat conclu avec la société DEEZER.

75. La société MOBIUS SOLUTIONS LTD reconnait que cet espace de stockage était accessible à des tiers et n'était pas sécurisé au moment de la violation de données. Ultérieurement, la société a indiqué ne pas avoir eu connaissance de la copie réalisée par ses salariés et que celle-ci aurait eu d'après ses salariés pour seule finalité d'améliorer les performances des services proposés à la société DEEZER.

76. La formation restreinte rappelle que la société est responsable de l'action de ses salariés et qu'elle aurait dû être vigilante, au regard de ses obligations en qualité de sous-traitant, s'agissant de la copie des données de plus de 46 millions d'utilisateurs DEEZER dans le monde dont 9 millions en France, d'un environnement de production à un environnement externe dont les flux lui étaient facturés. La formation restreinte note que les données des utilisateurs DEEZER transmises à MOBIUS SOLUTIONS LTD avaient pour seule finalité la réalisation de campagnes marketing personnalisées par la société DEEZER. La formation restreinte relève que la copie des données des utilisateurs DEEZER a été réalisée pour un usage propre à la société MOBIUS SOLUTIONS LTD, afin d'améliorer la performance de ses services, que ces services soient destinés à la société DEEZER ou non.

77. Il en résulte qu'en copiant les données de plus de 9 millions d'utilisateurs DEEZER en France et en les transférant sur son environnement de non-production, la société MOBIUS SOLUTIONS LTD a traité ces données en dehors des instructions de la société DEEZER.

78. Par conséquent, la formation restreinte considère qu'un manquement à l'article 29 du RGPD est caractérisé.

G. Sur le manquement à l'article 30 du RGPD

79. En droit, l'article 30-2 du Règlement dispose que : " Chaque sous-traitant et, le cas échéant, le représentant du sous-traitant tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant :

a) le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données ;

b) les catégories de traitements effectués pour le compte de chaque responsable du traitement ;

c) 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 ;

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

80. L'article 30-5 du Règlement précise que cette obligation ne s'impose pas aux entreprises de moins de 250 salariés, sauf si le traitement comporte un risque pour les droits et les libertés des personnes, n'est pas occasionnel ou porte sur des catégories particulières de données.

81. Le rapporteur considère que la société a commis un manquement à l'article 30-2 du RGPD en ne tenant pas de registre des activités de traitement alors que le traitement des données qu'il réalisait en sa qualité de sous-traitant de la société DEEZER n'était pas occasionnel.

82. En défense, la société considère que le " data processing addendum " (DPA) contient l'ensemble des informations requises dans le cadre de la mise en œuvre d'un registre des activités de traitement.

83. En l'espèce, la formation restreinte relève que, si l'ensemble des documents présentés (contrat et addendum) contiennent des informations requises au titre de l'article 30 du RGPD, il n'en reste pas moins que la société n'a pas tenu de registre d'activités de traitement en tant que sous-traitant, ce qu'elle ne conteste pas, l'information relative au nom et coordonnées du délégué à la protection des données du responsable de traitement étant d'ailleurs manquante.

84. Il en résulte qu'un manquement formel à l'article 30 du RGPD est caractérisé à l'encontre de la société.

III. Sur les mesures correctrices

85. L'article 20 de la loi n° 78-17 du 6 janvier 1978 modifiée prévoit que : " lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut […] saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : […]

86. 7° À l'exception des cas où le traitement est mis en œuvre par l'État, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du 27 avril 2016, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83 ".

87. L'article 83 du RGPD, tel que visé par l'article 20, paragraphe III, de la loi Informatique et Libertés, prévoit quant à lui que : " Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives ", avant de préciser les éléments devant être pris en compte pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de cette amende.

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

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

90. En outre, la formation restreinte souligne que, si l'imposition d'une amende administrative est conditionnée à l'établissement d'une violation fautive de la part de l'organisme poursuivi, cette faute peut découler d'un comportement délibéré mais également d'une négligence, en application de l'alinéa b) de l'article 83, paragraphe 2 du RGPD (CJUE, Grande Chambre, 5 décembre 2023, Deutsche Wohnen SE e.a., C-807/21 ; CJUE, Grande Chambre, 5 décembre 2023, Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos e.a., C- 683/21).

91. Enfin, elle rappelle qu'en vertu de l'article 83 du RGPD, les amendes administratives doivent être dissuasives et proportionnées.

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

1. Sur le prononcé d'une amende administrative

92. En défense, la société fait valoir que la copie non autorisée des données des utilisateurs de la société DEEZER présente un caractère accidentel et isolé, ne résultant ni d'une intention ni d'une négligence de sa part. La société ajoute avoir subi des pertes financières nettes à hauteur de […] dollars américains, soit environ […] euros en 2024, et avoir toujours pleinement coopéré avec la CNIL, en dépit de la contestation de sa compétence.

93. En premier lieu, la formation restreinte considère qu'il convient de faire application du critère prévu à l'article 83, paragraphe 2, a) relatif à la gravité du manquement compte tenu de la nature, de la portée ou de la finalité du traitement, ainsi que du nombre de personnes concernées affectées et du niveau de dommage qu'elles ont subi.

94. La formation restreinte relève que la société a manqué à plusieurs de ses obligations en qualité de sous-traitant, ayant conduit à une violation de données à caractère personnel présentant un caractère massif puisque selon la déclaration de violation de données dont la CNIL a été destinataire, plus de 200 millions de personnes dans le monde auraient été concernées, ces données concernant des utilisateurs de DEEZER et des données d'autres clients de MOBIUS. La société a estimé quant à elle que 46,9 millions d'utilisateurs DEEZER étaient concernés dans le monde, entre 12,7 et 21,6 millions au sein de l'Union européenne et 9,8 millions en France, soit un nombre considérable de personnes concernées.

95. La formation restreinte estime que le fait que la société n'ait pas supprimé les données transmises par la société DEEZER au terme de leur relation contractuelle, en violation de l'article 28 du RGPD, et ait traité ces données à caractère personnel au-delà des instructions données par le responsable de traitement, en violation de l'article 29 du RGPD, caractérise des manquements aux obligations du sous-traitant au regard des exigences du RGPD et de la protection des données à caractère personnel. En outre, ces manquements ont contribué à créer les conditions propices à la violation de données, en stockant un grand nombre de données à caractère personnel en dehors des instructions du responsable de traitement. En outre, la société devait tenir un registre des activités de traitement, ce qu'elle n'a pas formellement fait.

96. La formation restreinte considère que la copie irrégulière des données par la société a eu un caractère dommageable pour les personnes concernées, dans la mesure où de nombreuses données ont été divulguées sur le darknet concernant non seulement leur identité (nom, prénom, âge), leurs coordonnées (adresse électronique) mais aussi leurs habitudes d'écoute sur la plateforme DEEZER.

97. La formation restreinte rappelle que les données en cause présentent un risque pour les droits et libertés des personnes, en ce que les personnes dont les données figurent dans les fichiers mis en ligne sur le darknet sont des cibles de choix pour un hameçonnage (" phishing ") personnalisé (envoi de faux messages ou de faux documents pour récupérer des informations personnelles ou de l'argent). Si ces données datent de 2019, elles restent d'actualité puisque certaines d'entre elles présentent un caractère constant (l'identité) ou pérenne (les adresses électroniques ne font pas non l'objet d'un changement régulier).

98. En deuxième lieu, la formation restreinte considère qu'il convient de faire application du critère

prévu à l'article 83, paragraphe 2, b) relatif à l'intentionnalité ou non des manquements commis.

99. La formation restreinte considère que la société a fait preuve d'une négligence certaine en copiant, en dehors du cadre contractuel avec la société DEEZER, des données non anonymisées de millions de ses utilisateurs et en ne les supprimant pas à l'issue de la relation contractuelle. A supposer que ces données aient été copiées par des salariés en dehors des instructions des dirigeants de la société MOBIUS SOLUTIONS LTD, il n'en reste pas moins que MOBIUS SOLUTIONS LTD est responsable de l'action de ses salariés et aurait dû être vigilante sur les flux de son stockage.

100. La formation restreinte souligne de surcroît que dans le cadre de ses observations en réponse, la société considère que la copie des données des utilisateurs de la société DEEZER, réalisée par ses salariés, pourrait relever de l'exécution normale du contrat avec la société DEEZER, ce qui laisse à penser que la société a pu commettre de manière délibérée le manquement à l'article 29 du RGPD.

101. La formation restreinte note en outre que la société a, dans un premier temps, contesté toute responsabilité avant de reconnaître être à l'origine de la copie non autorisée des données de la société, ne facilitant pas la notification de violation de données par la société DEEZER.

102. La formation restreinte considère dès lors que la société s'est montrée, à tout le moins, très négligente.

103. En troisième lieu, la formation restreinte considère qu'il y a lieu de prendre en compte le critère relatif aux mesures prises par le responsable de traitement pour atténuer le dommage subi par les personnes concernées en application de l'article 83, paragraphe 2, c) du RGPD.

104. La société a indiqué n'avoir que le 1er octobre 2023, supprimé les données issues de la copie non autorisée des utilisateurs de la société DEEZER.

105. La formation restreinte relève que cette suppression est intervenue tardivement après que la société DEEZER eut notifié le 10 novembre 2022 à la CNIL la violation de données dont elle avait été victime, et n'a pas permis d'éviter la mise en vente des données de plus de 46 millions de personnes utilisatrices des services de la société DEEZER sur le darknet.

106. En conséquence, la formation restreinte estime, au vu de l'ensemble de ces éléments et au regard des critères fixés à l'article 83 du RGPD, qu'il y a lieu de prononcer une amende administrative au titre des manquements en cause.

2. Sur le montant de l'amende administrative

107. En défense, la société soutient que la société a enregistré des pertes nettes chaque année et en particulier à hauteur de […] dollars américains, soit environ […] euros en 2024, et conteste la proportionnalité du montant de l'amende proposée.

108. La formation restreinte relève qu'en application des dispositions de l'article 20-IV-7° de la loi Informatique et Libertés, elle peut prononcer à l'encontre d'un responsable du traitement ayant commis les manquements constatés, une " amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu ".

109. La formation restreinte relève que dans le cadre de la prise en compte de l'activité de la société et de sa situation financière pour la détermination de l'amende, la société justifie d'un chiffre d'affaires pour 2024 de […] dollars américains. Pour 2023, ce chiffre s'élevait à […] de dollars américains. Ce chiffre est en constante progression.

110. Dès lors, au regard de la responsabilité de la société MOBIUS SOLUTIONS LTD, de ses capacités financières et des critères pertinents de l'article 83 du RGPD évoqués ci-avant, la formation restreinte estime qu'une amende administrative d'un montant d'un million (1 000 000) d'euros, au regard des manquements constitués aux articles 28, 29 et 30 du RGPD apparaît justifiée.

IV. Sur la publicité de la sanction

111. En défense, la société soutient que la publicité de la sanction n'est pas justifiée.

112. La formation restreinte considère qu'une telle mesure se justifie compte tenu de l'important retentissement de la violation de données en cause, de la gravité des manquements constitués et du nombre de personnes concernées, lesquelles doivent être informées.

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

PAR CES MOTIFS

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

- prononcer à l'encontre de la société MOBIUS SOLUTIONS LTD, une amende administrative d'un montant d'un million (1 000 000) d'euros pour les manquements aux articles 28, 29 et 30 du RGPD ;

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

Le Président

Philippe-Pierre CABOURDIN

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