Délibération SAN-2025-017 du 30 décembre 2025

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Date de publication sur Légifrance : Jeudi 22 janvier 2026
Etat juridique : En vigueur

Délibération de la formation restreinte n° SAN-2025-017 du 30 décembre 2025 concernant la société X

Certains développements de la délibération, permettant d'identifier la société ou comportant notamment des données à caractère personnel ou des secrets protégés par la loi, sont remplacés par le signe […] ou par les lettres X, Y ou Z.

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, MM. Didier KLING et Bertrand du MARAIS, 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 directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;

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° 2023-001C du 21 décembre 2022 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 des traitements mis en œuvre par la société X ou pour son compte ;

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 17 avril 2025 ;

Vu le rapport de Mme Anne DEBET, commissaire rapporteure, du 12 mai 2025, signifié à la société le 13 mai 2025 ;

Vu les observations écrites versées par la société X le 23 juin 2025 ;

Vu la réponse de la rapporteure notifiée à la société X le 16 juillet 2025 ;

Vu les nouvelles observations écrites versées par la société X le 12 septembre 2025 ;

Vu la clôture de l'instruction notifiée à la société X le 24 septembre 2025 ;

Vu les observations orales formulées lors de la séance de la formation restreinte du 16 octobre 2025 ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 16 octobre 2025 :

- Mme Anne DEBET, commissaire, entendue en son rapport ;

En qualité de représentants de la société X :

- […]

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

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. La société X (ci-après " la société ") est […] dont le siège social est situé […].

2. La société employait, en 2021, 363 salariés et l'enseigne " X " comptait plus de […] magasins sur le territoire français. En 2022, la société a réalisé un chiffre d'affaires de […] d'euros, pour un résultat net de près de […] d'euros. En 2023, elle a réalisé un chiffre d'affaires de plus de […] d'euros, pour un résultat net de près de […] d'euros. En 2024, le chiffre d'affaires de la société s'est élevé à plus de […] d'euros, pour un résultat net de plus de […] d'euros.

3. Créée […], la société est […], dont l'activité consiste en […] en magasin ainsi qu'en ligne, à partir du site web " […] " dont la société X est éditrice. Ce site permet notamment de créer un compte client, de faire des achats et d'adhérer à un programme de fidélité valable en ligne ainsi qu'à la caisse des magasins du réseau X. D'après les informations communiquées par la société le 10 février 2023, le programme de fidélité comptait à cette date près de 10,5 millions de membres en France, plus de 200 000 en Belgique, plus de 15 000 au Luxembourg ainsi que des membres dans plusieurs autres pays de l'Union européenne.

4. Par décision n° 2023-001C du 21 décembre 2022, la présidente de la Commission nationale de l'informatique et des libertés (ci-après, " la CNIL " ou " la Commission ") a chargé le secrétaire général de procéder ou de faire procéder à une mission de contrôle afin de vérifier la conformité des traitements mis en œuvre par la société au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après " RGPD ") et à la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après " loi Informatique et Libertés " ou " loi du 6 janvier 1978 modifiée ").

5. En application de cette décision, une délégation de la CNIL a réalisé un contrôle en ligne à partir du site web " […] ", le 5 janvier 2023, et un contrôle sur place dans les locaux de la société X, le 26 janvier 2023. Les procès-verbaux n° 2023-001/1 et n° 2023-001/2 dressés à l'issue de ces contrôles ont été notifiés à la société par courriers des 6 et 27 janvier 2023.

6. La société a communiqué à la délégation des éléments complémentaires les 10 et 23 février, 14 mars, 18 et 28 avril, 23 août et 26 septembre 2023.

7. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 17 avril 2025, désigné Mme Anne DEBET en qualité de rapporteure sur le fondement de l'article 22 de la loi du 6 janvier 1978 modifiée.

8. Conformément à l'article 56 du RGPD et au vu des éléments du dossier, la CNIL a, le 27 décembre 2024, informé l'ensemble des autorités de contrôle européennes de sa compétence pour agir en tant qu'autorité de contrôle cheffe de file concernant les traitements transfrontaliers mis en œuvre par la société, résultant de ce que l'établissement principal de la société se trouve en France. Après échanges entre la CNIL et les autorités de protection des données européennes dans le cadre du mécanisme de guichet unique, il apparaît que les autorités belge, luxembourgeoise, néerlandaise, espagnole, allemande, irlandaise, italienne, danoise, suédoise, portugaise, finlandaise, autrichienne, roumaine, polonaise, lituanienne et norvégienne sont concernées par les traitements mis en œuvre.

9. Le 12 mai 2025, à l'issue de son instruction, la rapporteure a fait signifier à la société un rapport détaillant les manquements aux articles 6, 13, 32 et 35 du RGPD ainsi qu'à l'article 82 de la loi Informatique et Libertés qu'elle estimait constitués en l'espèce. Ce rapport proposait à la formation restreinte de prononcer à l'encontre de la société une amende administrative, ainsi qu'une injonction de mettre en conformité ses traitements avec les dispositions susvisées, assortie d'une astreinte. Elle 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.

10. Le 23 juin 2025, la société a produit des observations en réponse au rapport de sanction.

11. La rapporteure a répondu aux observations de la société le 16 juillet 2025.

12. Le 12 septembre 2025, la société a produit de nouvelles observations en réponse.

13. Par courrier notifié le 24 septembre 2025, la rapporteure a, en application du III de l'article 40 du décret n° 2019-536 précité, informé la société que l'instruction était close.

14. Le même jour, la société a été informée que le dossier était inscrit à l'ordre du jour de la formation restreinte du 16 octobre 2025.

15. La rapporteure et la société ont présenté des observations orales lors de la séance de la formation restreinte.

II. Motifs de la décision

A. Sur la procédure de coopération européenne

16. En application de l'article 60, paragraphe 3 du RGPD, le projet de décision adopté par la formation restreinte a été transmis le 1er décembre 2025 aux autorités de contrôle européennes concernées.

17. Au 29 décembre 2025, aucune de ces autorités n'avait formulé d'objection pertinente et motivée à l'égard de ce projet de décision, de sorte que, en application de l'article 60, paragraphe 6 du RGPD, ces dernières sont réputées l'avoir approuvé.

B. Sur les traitements en cause et la qualité de responsable de traitement de la société X

18. 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 ".

19. En matière de ciblage publicitaire, le Comité européen de la protection des données (ci-après le " CEPD "), dans ses lignes directrices 8/2020 sur le ciblage des utilisateurs de médias sociaux adoptées le 13 avril 2021, indique que le cibleur agit en tant que responsable du traitement dès lors qu'il " détermine les finalités et les moyens du traitement en collectant, traitant et transmettant activement les données à caractère personnel des personnes concernées au fournisseur de médias sociaux à des fins publicitaires " (§61).

20. En premier lieu, la formation restreinte relève que les traitements en cause dans la présente procédure sont relatifs :

- d'une part, au fonctionnement du site web " [...] ", dont elle est éditrice et par le biais duquel elle collecte et traite des données techniques des utilisateurs (adresse IP, connexion Internet, type de navigateur, informations concernant le terminal utilisé) et des données recueillies à l'aide de cookies ;

- et, d'autre part, au fonctionnement des comptes clients et du programme de fidélité de l'enseigne X, la société collectant et traitant les données à caractère personnel de ses clients et des adhérents à ce programme, lors de la création d'un compte (civilité, nom, prénom, adresse électronique, mot de passe, date de naissance, numéro de téléphone, adresse postale et magasin le plus proche choisi), d'une carte de fidélité (les mêmes informations étant recueillies) et ultérieurement au travers de l'utilisation de ladite carte.

21. La formation restreinte relève que la société a indiqué à la délégation de contrôle, par courrier du 28 avril 2023, être responsable des traitements de données à caractère personnel mis en œuvre à partir du site web " [...] " ainsi que dans le cadre de son programme de fidélité. La société est également désignée comme étant responsable des traitements susvisés dans la " Politique des données personnelles " et l'article 12 des " Conditions Générales du Programme de fidélité X " figurant sur le site web " [...] ".

22. En second lieu, la formation restreinte relève que la présente procédure concerne également les traitements relatifs à la présentation de publicité ciblée sur le réseau social Z, géré par le groupe Y, afin de promouvoir les produits vendus par X. Dans ce cadre, la société X transmet l'adresse électronique et/ou le numéro de téléphone des adhérents à son programme de fidélité (lorsqu'ils ont consenti à recevoir de la prospection commerciale) au groupe Y, afin que celui-ci les fasse correspondre avec les données des utilisateurs de son réseau social. A partir de cette comparaison, Y identifie, parmi les membres du programme de fidélité X, ceux qui sont également membres de son réseau social, ainsi que les utilisateurs du réseau social ayant un profil similaire. Ce traitement permet de leur présenter des publicités dans le cadre des campagnes marketing de la société X. Il ressort de l'instruction que la transmission des données au groupe Y était réalisée depuis fin 2018, de façon hebdomadaire, et qu'elle a cessé en février 2024.

23. La formation restreinte relève que la société a indiqué à la délégation de contrôle qu'elle agissait en tant que responsable de traitement dans le cadre de la transmission des données au groupe Y et pour la mise en correspondance de ces données avec celles des utilisateurs du réseau social Z. S'agissant des traitements réalisés dans le cadre des

campagnes lancées postérieurement à cette mise en correspondance, la société X a indiqué qu'elle-même et le groupe Y agissaient en tant que responsables conjoints.

24. La formation restreinte considère en effet que la société X, en collectant et en transmettant les données à caractère personnel des adhérents de son programme de fidélité au groupe Y, en vue de leur afficher sur le réseau social Z des publicités visant à promouvoir ses produits, détermine les finalités et les moyens du traitement.

25. Par conséquent, et sans qu'il soit nécessaire dans le cadre de la présente procédure de se prononcer également sur la part de responsabilité incombant au groupe Y, la société X doit être regardée comme responsable du traitement de publicité ciblée affichée sur le réseau social Z, pour les besoins duquel elle transmettait au groupe Y des données à caractère personnel jusqu'en février 2024.

C. Sur le manquement à l'obligation de traiter les données de façon licite

26. En droit, l'article 6, paragraphe 1, du RGPD dispose que " le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques; b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci; c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis; d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique; e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement; f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant ".

27. L'article 4, point 11 du RGPD dispose que le consentement, tel que visé à l'article 6, paragraphe 1, a) du RGPD, doit s'entendre comme une manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

28. En outre, le considérant 32 du RGPD prévoit que cet " acte positif clair " peut par exemple se matérialiser par une case à cocher lors de la consultation d'un site internet, et qu'en tout état de cause " il ne saurait […] y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité. Le consentement donné devrait valoir pour toutes les activités de traitement ayant la ou les mêmes finalités. Lorsque le traitement a plusieurs finalités, le consentement devrait être donné pour l'ensemble d'entre elles […] ".

29. S'agissant des modalités de recueil du consentement, la Cour de justice de l'Union européenne (CJUE) a précisé, dans sa décision Planet49 GmbH de 2019, que " la manifestation de volonté visée à l'article 2, sous h), de la directive 95/46 doit, notamment, être " spécifique ", en ce sens qu'elle doit porter précisément sur le traitement de données concerné et ne saurait être déduite d'une manifestation de volonté ayant un objet distinct " (CJUE, grande chambre, 1er octobre 2019, Planet49 GmbH, C-673/17, ECLI:EU:C:2019:801, point 58).

30. Par ailleurs, à titre d'illustration, les lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 précisent " qu'un responsable du traitement qui sollicite le consentement pour diverses finalités spécifiques devrait prévoir un consentement distinct pour chaque finalité afin que les utilisateurs puissent donner un consentement spécifique à des finalités spécifiques […] Le responsable des données devrait accompagner chacune des demandes de consentement distinctes d'informations spécifiques concernant les données traitées pour chaque finalité afin que les personnes concernées soient conscientes de l'incidence de leur choix […] (§§60 et 61) ".

31. La CJUE a rappelé à cet égard que le responsable de traitement doit fournir à la personne concernée " une information au regard de toutes les circonstances entourant le traitement des données, sous une forme compréhensible et aisément accessible ainsi que formulée en des termes clairs et simples, cette personne devant notamment connaître le type de données à traiter, l'identité du responsable du traitement, la durée et les modalités de ce traitement ainsi que les finalités que celui-ci poursuit. Une telle information doit permettre à ladite personne de déterminer facilement les conséquences du consentement qu'elle pourrait donner et garantir que ce consentement soit donné en pleine connaissance de cause (voir, par analogie, arrêt du 1er octobre 2019, Planet49, C 673/17, EU:C:2019:801, point 74). " (CJUE, 11 novembre 2020, Orange România SA, C 61/19, point 40).

32. La rapporteure affirme que le traitement de publicité ciblée affichée sur le réseau social Z, pour les besoins duquel la société X transmet des données à caractère personnel des membres de son programme fidélité au groupe Y, est dépourvu de base légale, en l'absence de recueil d'un consentement valide des personnes concernées. Elle considère en effet que les modalités de recueil du consentement, ainsi que les informations fournies par la société X aux membres de son

programme de fidélité, ne permettent pas de recueillir un consentement spécifique et éclairé de ces membres au traitement susvisé.

33. En défense, la société soutient que le consentement des personnes dont les données étaient transmises, était recueilli :

- d'une part, à l'occasion de leur adhésion au programme de fidélité X, dans la mesure où ces personnes avaient consenti à recevoir de la prospection commerciale par différents canaux (par courrier électronique et/ou par SMS) ainsi qu'à la mise en correspondance de ces données avec celles de Z, un tel traitement étant selon elle mentionné dans sa " politique des données personnelles " ;

- d'autre part, à l'occasion de l'inscription de ces personnes sur Z, celles-ci ayant accepté les " conditions générales d'utilisation " et la " politique de confidentialité " du réseau social, via lesquelles elles autorisent l'affichage de publicités ciblées de la part d'annonceurs.

34. La société fait ainsi valoir que les membres du programme de fidélité qui avaient accepté de recevoir de la prospection commerciale de la part d'X et qui disposaient d'un compte Z pouvaient raisonnablement s'attendre à voir apparaître des publicités pour les produits X sur le réseau social, et qu'ils pouvaient par ailleurs retirer ou modifier leur consentement à tout moment.

35. La société relève, en outre, que les seules données transmises étaient l'adresse de courrier électronique et/ou le numéro de téléphone des personnes concernées, que ces données étaient chiffrées, d'abord par la société X avant toute transmission, au moyen de la fonction de hachage SHA256, puis par le groupe Y, " au moyen d'un pixel Javascript ", garantissant selon elle que les données transmises ne puissent être exploitées par Y en l'absence de correspondance avec un utilisateur Z. La société précise également que ces données chiffrées étaient supprimées par le groupe Y à l'issue de leur mise en correspondance positive ou non.

36. Par ailleurs, elle soutient que le nombre de personnes concernées doit être relativisé dès lors que, si les données de 10,5 millions de personnes ont bien été transmises au groupe Y, seules 1,6 million d'entre elles ont effectivement vu s'afficher une publicité entre juin 2022 et février 2024 - le taux de correspondance étant de l'ordre de 15 %. En outre, la société indique n'avoir tiré aucun avantage financier significatif de ces traitements. Elle précise, enfin, avoir cessé spontanément toute campagne de publicité ciblée avec le groupe Y en février 2024.

37. En l'espèce, la formation restreinte relève que la société a réalisé, de fin 2018 à février 2024, des opérations de publicité ciblée sur le réseau social Z. Elle a, pour ce faire, transmis au groupe Y, gestionnaire de ce réseau social, les adresses électroniques et/ou les numéros de téléphone des membres de son programme de fidélité qui avaient consenti à recevoir des messages de prospection commerciale par SMS et/ou par courrier électronique, afin que Y procède à la mise en correspondance de ces données avec celles des utilisateurs de Z et affiche de la publicité pour les produits X, d'une part, aux utilisateurs du réseau social qui sont également membres du programme de fidélité X et, d'autre part, aux utilisateurs ayant un profil similaire à ces personnes.

38. La société a indiqué, tant lors du contrôle que dans le cadre de ses observations en défense, fonder les traitements susvisés sur le consentement des personnes concernées.

39. En premier lieu, s'agissant du consentement que la société prétend recueillir via le formulaire d'adhésion au programme de fidélité X, la formation restreinte relève qu'il ressort des constatations réalisées par la délégation lors du contrôle en ligne du 5 janvier 2023 que, lorsqu'il créé un compte sur le site web " [...]", l'utilisateur se voit présenter un formulaire sur lequel il doit notamment renseigner sa civilité, ses nom, prénom, numéro de téléphone, date de naissance et adresse de courrier électronique. Ce formulaire comprend également un encart permettant à la personne concernée d'adhérer au programme de fidélité X, via un bouton poussoir (oui/non) associé à la mention " je rejoins le programme de fidélité La Team X et cagnotte immédiatement 5 € ".

40. Si l'utilisateur manifeste son souhait de rejoindre le programme de fidélité en activant le bouton poussoir, il est invité à consentir à être contacté par SMS pour " recevoir [s]es avantages fidélité " et/ou par courrier électronique pour recevoir " les meilleures offres d'X ", via des cases à cocher (oui/non). Un lien hypertexte " Détails des conditions ICI " est situé au bas du formulaire, permettant à l'utilisateur d'être redirigé vers les " Conditions Générales du Programme de fidélité X ". Un second lien hypertexte, " En savoir plus sur vos droits et sur la façon dont nous traitons vos données personnelles ", situé lui aussi au bas du formulaire, renvoie quant à lui vers la " politique des données personnelles " de la société (également accessible depuis le pied de page de chacune des pages du site), qui précise au sein de son article 3 (dans sa version en vigueur au moment du contrôle) que la société traite les données à caractère personnel des personnes notamment dans le cadre de " l'adhésion au programme de fidélité et la gestion du Programme de fidélité, notamment la mise en correspondance des données des adhérents avec celles de la société Z ". La " société Z " est également mentionnée dans les destinataires des données (article 8), puisqu'il est précisé que " Les Données Personnelles collectées par X pourront être transmises : […] à la société Z, qui s'engage, en tant que sous-traitant, à ne pas céder, à quelque titre que ce soit, les données traitées par elle, une fois le processus de mise en correspondance terminé, à des partenaires y compris

commerciaux ", ainsi qu'au stade de l'information relative à la durée de conservation des données, l'article 7 précisant que " s'agissant du programme de fidélité, la société Z s'engage à supprimer automatiquement les données transférées par X une fois le processus de mise en correspondance terminé, et à ne conserver ni copie ni sauvegarde des données personnelles concernées ".

41. De plus, les " Conditions générales de vente ", accessibles depuis le pied de page de chacune des pages du site web, prévoient en leur article 10 que " les données collectées sont réservées à l'usage de la Direction Marketing Client, Direction Stratégie Digitale & Innovation de la société X et de la société Z, agissant en qualité de sous-traitant. À ce titre, les données collectées sont susceptibles d'être transférées vers les Etats-Unis. […] Les informations nominatives collectées sont nécessaires au traitement de la commande, à son acheminement, à l'établissement de la facture, et à la mise en correspondance des données clients avec celles de la société Z ". L'article 11 prévoit quant à lui que " conformément à la règlementation en vigueur, l'adhérent est informé que l'ensemble des informations données par lui dans le questionnaire figurant sur la Demande d'adhésion sont nécessaires au traitement et à la délivrance de la Carte X, ainsi qu'au processus de mise en correspondance des données clients avec celles de la société Z ".

42. La formation restreinte relève tout d'abord que le formulaire décrit aux paragraphes 39 et 40 ne contient pas d'information sur la transmission des données au groupe Y à des fins de publicité ciblée. Les informations contenues sur ce formulaire portent sur l'adhésion au programme de fidélité et la réception de messages de prospection commerciale par SMS et/ou courrier électronique.

43. Ainsi, sur la base des seules mentions figurant sur le formulaire, il ne saurait être considéré que l'information fournie aux adhérents est suffisante pour assurer le caractère éclairé de leur consentement à la transmission de leurs données au réseau social Z à des fins de publicité ciblée. Si ces mentions font bien référence à des traitements de prospection électronique (par SMS et/ou courrier électronique), qui visent à promouvoir des produits commercialisés par la société X tout comme la publicité ciblée effectuée sur le réseau social Z, les messages publicitaires sont adressés selon des canaux distincts et dans des environnements différents. En effet, la transmission des données au groupe Y à des fins de publicité ciblée sur le réseau social Z, c'est-à-dire une publicité par encarts affichés sur le site web, est d'une nature différente de la publicité par courriel ou SMS, qui n'implique pas nécessairement la transmission des données à un tiers. Or, cette finalité de publicité ciblée sur le réseau social Z – pour les besoins de laquelle les données sont transmises au groupe Y – n'est pas clairement mentionnée sur le formulaire. Dans ces conditions, la formation restreinte estime qu'il ne peut être considéré que, en prenant connaissance du contenu de ce formulaire, les personnes ont fourni un consentement spécifique et éclairé au traitement de leurs données à caractère personnel pour cette finalité.

44. Ensuite, en ce qui concerne les documents figurant sur le site web " [...] ", à savoir les " Conditions Générales du programme de fidélité ", la " politique des données personnelles " et les " Conditions générales de vente ", la formation restreinte relève, d'une part, que les personnes doivent prendre l'initiative de les consulter en cliquant sur plusieurs liens si elles souhaitent accéder aux informations qu'ils contiennent et, d'autre part, qu'ils comportent des informations partielles, qui ne sont pas suffisamment explicites pour permettre aux personnes concernées d'avoir une vision claire du traitement en cause et, partant, de donner un consentement éclairé et spécifique.

45. S'agissant tout d'abord des " Conditions Générales du programme de fidélité X ", qui ont pour objet d'expliquer aux membres les conséquences de leur adhésion, elles ne mentionnent pas la transmission des données au groupe Y lorsqu'ils acceptent d'être contactés par X par SMS ou courrier électronique. Quant à l'information fournie dans la " politique des données personnelles " et les " Conditions générales de vente ", selon laquelle les données des personnes sont " mise[s] en correspondance " avec " celles de la société Z ", elle n'apparait pas non plus suffisante pour recueillir un consentement éclairé des personnes concernées dans la mesure où cette simple mention ne permet pas de comprendre clairement la finalité de cette transmission, à laquelle il n'est d'ailleurs pas demandé aux personnes de consentir par un acte positif.

46. La formation restreinte observe en outre que ces informations figurent dans deux documents distincts, eux-mêmes accessibles via plusieurs liens présents au bas du formulaire de création de compte ainsi que depuis le pied de page de chacune des pages du site web, les personnes étant tenues de cliquer sur plusieurs liens situés à distance des cases à cocher et du bouton poussoir permettant le recueil du consentement en matière de prospection commerciale par SMS et/ou courrier électronique (ces cases et ce bouton portant par ailleurs, comme rappelé au paragraphe 43, sur des finalités distinctes).

47. Au vu de l'ensemble de ce qui précède, ce parcours ne permet pas vraiment aux personnes concernées de fournir un consentement explicite et éclairé par un acte positif pour le traitement en cause, comme aurait pu le permettre, par exemple, la présence d'une case à cocher sur le formulaire d'adhésion au programme de fidélité mentionnant clairement la finalité de ce traitement et offrant la possibilité aux personnes d'accepter ou non sa mise en œuvre.

48. En deuxième lieu, s'agissant du consentement fourni par les utilisateurs de Z lors de la création d'un compte sur le réseau social, la formation restreinte relève tout d'abord que les personnes dont les données sont transmises ne détiennent pas toutes un compte sur le réseau social Z. En effet, la formation restreinte relève que la société ne conteste

pas qu'elle transmettait au groupe Y les données de l'intégralité des adhérents au programme de fidélité ayant accepté la réception de messages de prospection par courrier électronique et/ou SMS, sans savoir à ce stade s'ils étaient ou non inscrits sur Z, l'objectif étant d'identifier les membres du programme de fidélité déjà utilisateurs du réseau social. A cet égard, la formation restreinte relève en outre que, d'après les informations communiquées par la société, le taux de correspondance entre les données transmises par X et celles détenues par le groupe Y s'élève seulement à 15 %.

49. La formation restreinte relève qu'en tout état de cause, le consentement donné par les utilisateurs du réseau social Z ne saurait pallier le consentement qui aurait dû être recueilli par la société X. D'une part, la formation restreinte rappelle que la société, en sa qualité de responsable de traitement, devait s'assurer, avant la mise en œuvre du traitement, et donc avant la transmission des données au groupe Y, que les personnes concernées avaient donné leur consentement, ce qui n'était pas le cas en l'espèce. D'autre part, il ressort des documents fournis par la société, dans ses observations du 23 juin 2025, que lors de leur inscription sur Z, les personnes concernées acceptent les conditions d'utilisation du réseau social et l'affichage, par le groupe Y, de publicités ciblées, à partir des données transmises par ses partenaires. Ce consentement concerne ainsi exclusivement les opérations réalisées sur le réseau social Z, et non les traitements réalisés en amont par la société X.

50. Dans ces conditions, le traitement réalisé par la société X ne saurait reposer sur le consentement recueilli par le groupe Y.

51. En troisième lieu, s'agissant du chiffrement des données au moyen de la fonction de hachage SHA256 et d'" un pixel Javascript ", dont se prévaut la société, la formation restreinte relève, d'une part, que seules les adresses électroniques transmises au groupe Y étaient hachées, alors que les numéros de téléphones étaient transmis en clair. La formation restreinte relève, d'autre part, que le hachage des données permet certes de les transmettre de manière sécurisée, ce qui est une bonne pratique, mais elle considère que cela n'a pas d'incidence sur le fait que les données sont transmises dans le cadre du traitement susvisé, objet du manquement en cause.

52. En quatrième lieu, la formation restreinte considère que la circonstance que le groupe Y supprimait certaines données à la suite de la réception et de la comparaison de celles-ci n'emporte aucune conséquence non plus sur les traitements réalisés par la société X, les données étant bien transmises par X.

53. S'agissant enfin du nombre de personnes concernées par les traitements en cause, la formation restreinte relève que, si 1,6 million de personnes ont vu s'afficher une publicité personnalisée pour les produits X sur Z entre le mois de juin 2022 et le mois de février 2024, l'ensemble des données des adhérents du programme de fidélité ayant accepté la réception de messages de prospection par SMS et/ou courriel, à savoir 10,5 millions de personnes, ont été effectivement transmises au groupe Y, si bien que ces personnes doivent bien être considérées comme étant concernées par les traitements mis en œuvre.

54. Au regard de l'ensemble de ce qui précède, la formation restreinte considère qu'un manquement à l'article 6 paragraphe 1, a) est constitué, dans la mesure où le consentement, sur lequel elle entendait fonder son traitement de ciblage publicitaire réalisé par le biais de campagnes sur le réseau social Z et pour les besoins duquel elle transmettait des données au groupe Y, n'était pas valablement recueilli.

55. Si la formation restreinte prend acte du fait que la société a cessé toute transmission de données au groupe Y en février 2024 et qu'une injonction apparait dès lors sans objet sur ce point, il n'en demeure pas moins que le manquement demeure caractérisé pour le passé.

D. Sur le manquement à l'information des personnes en application de l'article 13 du RGPD

56. L'article 13 du RGPD dresse la liste des informations devant être fournies à la personne concernée lorsque les données à caractère personnel sont collectées directement auprès d'elle. Ces informations portent notamment sur l'identité du responsable de traitement et ses coordonnées, les finalités du traitement mis en œuvre, sa base juridique, les destinataires ou les catégories de destinataires des données, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données vers un pays tiers. Cet article impose également au responsable de traitement, lorsque cela apparaît nécessaire pour garantir " un traitement équitable et transparent " des données personnelles en l'espèce, d'informer les personnes sur la durée de conservation des données, l'existence des différents droits dont elles bénéficient, l'existence du droit de retirer leur consentement à tout moment et le droit d'introduire une réclamation auprès d'une autorité de contrôle.

57. La rapporteure considère qu'au moment des opérations de contrôle, les informations figurant dans la " politique des données personnelles " de la société, accessible depuis le formulaire de création de compte (et donc au moment de l'inscription au programme de fidélité), ainsi que depuis le pied de page de chacune des pages du site, étaient incomplètes dès lors que les bases légales des traitements n'étaient pas données par finalité, que les durées de conservation dans le cadre du programme de fidélité n'étaient pas indiquées et que les informations sur les transferts de données n'étaient pas à jour au motif qu'elles renvoyaient au bouclier de protection des données " Privacy Shield ", qui ne garantit plus, depuis la

décision de la CJUE du 16 juillet 2020 (CJUE, grande chambre, 16 juillet 2020, Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems, affaire C-311/18 - arrêt dit " Schrems II "), une garantie juridique suffisante pour permettre le transfert des données personnelles de l'Union européenne vers les Etats-Unis.

58. La rapporteure relève également que l'ensemble des documents d'information de la société, à savoir les " conditions générales du programme de fidélité ", la " politique des données personnelles " et les " conditions générales de vente ", ne faisait apparaître à aucun moment la finalité de publicité ciblée sur le réseau social Z ni la base légale correspondante, et ne contenait pas non plus d'information relative à l'existence d'une responsabilité conjointe entre le groupe Y et la société X, dont se prévaut la société, s'agissant des campagnes lancées sur le réseau social Z.

59. En défense, si la société reconnaît que sa " politique de données personnelles " de 2023 aurait pu être plus claire, elle soutient qu'elle contenait bien la liste des traitements mis en œuvre, notamment la mise en correspondance des données des adhérents avec la société Z, et que chaque traitement mentionnait sa finalité et était rattaché à sa base légale. Elle précise qu'en tout état de cause, la mention d'information relative à cette mise en correspondance a été retirée dès lors que la transmission des données vers le groupe Y a cessé en 2024. Elle fournit, pour le démontrer, sa nouvelle " politique des données personnelles " de septembre 2025, permettant, selon elle, de clarifier les différents traitements mis en œuvre et d'expliciter, pour chaque finalité de traitement, la base légale correspondante. Elle explique également avoir mis à jour, le 20 juin 2025, les informations relatives aux transferts internationaux de données, en supprimant les références au bouclier de protection des données " Privacy Shield ". Enfin, elle indique avoir modifié, en septembre 2025, les " conditions générales du programme de fidélité " afin d'indiquer que les données des adhérents au programme de fidélité sont conservées deux ans.

60. Premièrement, la formation restreinte relève qu'il ressort des constats réalisés lors du contrôle en ligne du 5 janvier 2023 que la " politique des données personnelles " accessible depuis le site web " […] " contenait à cette date un article 3 intitulé " Pourquoi X collecte et utilise vos données ", au sein duquel la société informait d'abord les utilisateurs qu'elle " peut être amenée à traiter [leurs] données personnelles sur plusieurs fondements ", avant de lister plusieurs bases légales prévues par le RGPD, telles que l'exécution d'un contrat ou de mesures précontractuelles, le consentement, l'intérêt légitime ou encore une obligation légale. Au paragraphe suivant, la société indiquait " les raisons " pour lesquelles elle traitait les données et fournissait une liste de finalités poursuivies par les traitements mis en œuvre, par exemple, la gestion et l'administration du site, le traitement des demandes d'exercice des droits, l'adhésion au programme de fidélité et la gestion de celui-ci, ou encore l'analyse des données de connexion et de navigation à des fins de publicité ciblée sur les services offerts par le site. La formation restreinte considère qu'une telle présentation des bases légales et des finalités, sans correspondance entre ces deux éléments, était imprécise. Celle-ci ne permettait pas aux utilisateurs d'appréhender pleinement les traitements mis en œuvre ni de comprendre que certains traitements étaient fondés sur leur consentement et qu'ils pouvaient par conséquent le retirer s'ils le souhaitaient.

61. La formation restreinte observe que la " politique des données personnelles " transmise par la société à l'occasion de ses secondes observations en défense, en septembre 2025, comprend désormais, en son article 4, un tableau présentant les différentes finalités des traitements, associées aux bases légales correspondantes et aux traitements concernés. Une telle présentation permet aux utilisateurs d'être désormais clairement informés, pour chaque traitement, de sa finalité et de sa base légale.

62. Deuxièmement, s'agissant de l'information relative à la publicité ciblée sur le réseau social Z, la formation restreinte relève que l'article 3 de la " politique des données personnelles " de la société, dans sa version en vigueur au moment des contrôles, précisait que les données collectées par la société étaient traitées " pour l'adhésion au programme de fidélité, et la gestion du programme de fidélité, notamment la mise en correspondance des données des adhérents avec celles de la société Z ". Il était également précisé à l'article 10 des " conditions générales de vente sur internet ", accessibles depuis le pied de page de chacune des pages du site web, que les données collectées auprès de l'internaute étaient réservées " à l'usage de la Direction Marketing Client, Direction Stratégie Digitale & Innovation de la société X et de la société Z, agissant en qualité de sous-traitant " et que " les informations nominatives [étaient] nécessaires […]à la mise en correspondance des données clients avec celles de la société Z ". L'article 11, quant à lui, prévoyait que " conformément à la règlementation en vigueur, l'adhérent est informé que l'ensemble des informations données par lui dans le questionnaire figurant sur la Demande d'adhésion [étaient] nécessaires au traitement et à la délivrance de la Carte X, ainsi qu'au processus de mise en correspondance des données clients avec celles de la société Z ".

63. La formation restreinte relève que si ces mentions font état de la mise en correspondance des données des adhérents au programme de fidélité avec celles " de la société Z ", ni les " conditions générales de vente ", ni la " politique des données personnelles ", ni aucun autre document d'information élaboré par la société X ne mentionne la finalité de cette mise en correspondance, à savoir la réalisation de publicité ciblée sur le réseau social Z. La base légale d'un tel traitement n'est pas davantage mentionnée.

64. La formation restreinte prend acte que, dès lors que la société a cessé toute transmission de données au groupe Y depuis le mois de février 2024, de telles mentions d'information apparaissent aujourd'hui sans objet.

65. Troisièmement, la formation restreinte relève que l'information fournie par la société à ses clients au moment du contrôle en ligne du 5 janvier 2023, selon laquelle le transfert des données à des partenaires situés en dehors de l'Espace économique européen reposait sur le bouclier de protection des données (ou " Privacy Shield ") constituait une information erronée dans la mesure où, comme le relève la rapporteure, ce texte ne garantit plus, depuis la décision de la CJUE de juillet 2020 citée précédemment, une garantie juridique suffisante pour permettre le transfert des données personnelles de l'Union européenne vers les Etats-Unis.

66. La formation restreinte prend acte de la modification réalisée par la société, le 20 juin 2025, la politique des données personnelles indiquant désormais que de tels transferts sont régis par le " Data Privacy Framework " (cadre de protection des données Union européenne-Etats-Unis, considéré par la Commission européenne, dans une décision du 10 juillet 2023, comme offrant un niveau de protection substantiellement équivalent à celui de l'Union européenne).

67. Quatrièmement, la formation restreinte observe que la " politique des données personnelles ", accessible depuis le site web " [...] ", ne comportait, à la date du contrôle en ligne du 5 janvier 2023, aucune information relative aux durées de conservation des données des adhérents dans le cadre du programme de fidélité.

68. Elle relève que la nouvelle " politique des données personnelles ", datée de septembre 2025, précise que les données " relatives au compte client ainsi qu'à l'utilisation du n° de fidélité sont conservées pendant deux (2) ans à compter de la dernière connexion au compte ou utilisation du n° de fidélité ". La formation restreinte considère qu'une telle précision permet désormais aux personnes d'être pleinement informées de la durée de conservation de leurs données collectées dans le cadre de l'adhésion au programme de fidélité et prend acte de la mise en conformité de la société sur ce point.

69. Au vu de ce qui précède, la formation restreinte considère qu'au moment du contrôle en ligne du 5 janvier 2023, les documents d'information présentés sur le site web " […] " et destinés notamment à informer les personnes sur les traitements de leurs données à caractère personnel, ne permettaient pas de fournir une information complète, claire et précise, ce qui constitue un manquement aux dispositions de l'article 13 du RGPD.

70. La formation restreinte observe que la société s'est mise en conformité au cours de l'instruction et que, dès lors, le prononcé d'une injonction, tel que proposé par la rapporteure, apparait sans objet. Néanmoins, les mesures adoptées ne remettent pas en cause l'existence du manquement pour les faits passés.

E. Sur le manquement à l'obligation d'assurer la sécurité des données en application de l'article 32 du RGPD

71. En droit, l'article 32 du RGPD impose au responsable de traitement, " compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, [de mettre] en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ".

72. Il résulte de ces dispositions que le responsable de traitement est tenu de s'assurer que le traitement automatisé de données qu'il met en œuvre est suffisamment sécurisé. Le caractère suffisant des mesures de sécurité s'apprécie, d'une part, au regard des caractéristiques du traitement et des risques qu'il induit, d'autre part, en tenant compte de l'état de connaissances et du coût des mesures.

1) Sur la robustesse des mots de passe des comptes utilisateurs

73. En matière de mots de passe, des règles de complexité trop permissives, qui autorisent l'utilisation de mots de passe insuffisamment robustes, peuvent conduire à des attaques par des tiers non autorisés, telles que des attaques par " force brute " ou " par dictionnaire ", qui consistent à tester successivement et de façon systématique de nombreux mots de passe et conduisent ainsi à une compromission des comptes associés et des données à caractère personnel qu'ils contiennent.

74. La nécessité d'un mot de passe fort est ainsi recommandée tant par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), notamment dans son guide " recommandations relatives à l'authentification multifacteur et aux autres mots de passe " du 8 octobre 2021, que par la Commission.

75. En effet, dans sa délibération n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés – qui n'a certes pas un caractère impératif mais qui fournit un éclairage pertinent sur les mesures qu'il convient de prendre en matière de sécurité – la CNIL rappelle que, pour assurer un niveau de sécurité et de confidentialité suffisant, il convient d'adopter une politique de mots de passe présentant un niveau d'entropie suffisamment fort. La Commission précise à cet égard qu'" on appelle "entropie" la quantité de hasard contenue dans un système. Pour un mot de passe ou une clé cryptographique, cela correspond à son degré d'imprédictibilité, et donc à sa capacité de résistance à une attaque par force brute. "

76. Ainsi, dans l'hypothèse où l'authentification repose uniquement sur un identifiant et un mot de passe, la Commission recommande que la complexité fixée dans la politique de mots de passe permette d'assurer l'équivalent d'une entropie d'au moins 80 bits, ce qui correspond, par exemple, à un minimum de 12 caractères comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux à choisir dans une liste d'au moins 37 caractères spéciaux possibles, ou à un minimum de 14 caractères comprenant des majuscules, des minuscules et des chiffres sans caractère spécial obligatoire, ou encore à une phrase de passe composée de minimum 7 mots de la langue française.

77. À défaut, la Commission considère que permet également d'assurer un niveau de sécurité et de confidentialité suffisant une authentification reposant sur un mot de passe présentant une entropie d'au moins 50 bits, soit par exemple un mot de passe d'une longueur minimum de huit caractères, composé de trois des quatre catégories de caractères (majuscules, minuscules, chiffres et caractères spéciaux, ces derniers devant être pris dans un ensemble d'au moins 11 caractères), si elle s'accompagne d'un mécanisme de restriction d'accès au compte comme, par exemple, la temporisation d'accès au compte après plusieurs échecs (suspension temporaire de l'accès dont la durée augmente à mesure des tentatives), la mise en place d'un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (ex : " captcha ") et/ou le blocage du compte après plusieurs tentatives d'authentification infructueuses (au maximum dix). La CNIL a à cet égard mis à la disposition des acteurs un outil en ligne permettant de calculer, de manière simple, l'entropie des mots de passe.

78. La Commission précise également, dans la délibération susvisée, que les acteurs peuvent mettre en œuvre d'autres mesures de sécurité que celles décrites dans cette recommandation s'ils sont en capacité de montrer qu'elles garantissent un niveau de sécurité au moins équivalent, et précise qu'au regard de l'état de l'art, tout responsable de traitement utilisant des mots de passe doit garantir un niveau minimal de sécurité reposant, d'une part, sur un niveau d'entropie suffisant, le cas échéant avec un mécanisme de restriction d'accès au compte, et d'autre part, sur des règles de mise en œuvre et de gouvernance permettant de préserver la sécurité du mot de passe tout au long de son cycle de vie.

79. La rapporteure relève que, lors du contrôle en ligne du 5 janvier 2023, la délégation a constaté que lors de la création d'un compte utilisateur sur le site web " [...] ", un mot de passe composé de huit caractères, avec la seule contrainte de devoir contenir au moins un chiffre, était accepté. Elle note également que la société a confirmé les constatations effectuées par la délégation de contrôle et a ajouté qu'elle utilisait un outil nommé " […] ", permettant le blocage des tentatives d'attaque par force brute des mots de passe, ce blocage s'effectuant soit par l'affichage d'un captcha, soit par le blocage des appels à la page de login depuis l'adresse IP appelante. La rapporteure considère que de tels mots de passe, sans critère de complexité suffisante, ne permettaient pas d'assurer la sécurité des données à caractère personnel traitées par la société et d'empêcher que des tiers non autorisés y aient accès.

80. La société ne conteste pas l'insuffisante robustesse des mots de passe constatée lors du contrôle en ligne de la CNIL, mais déclare avoir mis en place des actions correctives dès le 6 novembre 2024. Elle précise ainsi avoir renforcé les exigences de complexité des mots de passe en imposant une combinaison de huit caractères incluant un caractère spécial, un chiffre, des lettres majuscules et minuscules afin d'atteindre une entropie minimale de 50 bits. Elle fait également valoir qu'elle a procédé, en juin 2025, à un nouveau renforcement des mots de passe en imposant qu'ils soient composés de douze caractères minimum et en étendant le panel de caractères spéciaux, celui-ci étant désormais fixé à 37, afin d'atteindre une entropie de 80 bits.

81. La formation restreinte relève qu'il ressort de l'instruction que les mots de passe des personnes créant un compte sur le site web " […] " (lequel contient les nom, prénom, date de naissance, numéro de téléphone, adresse électronique et adresse postale des personnes concernées) pouvaient être, à l'époque du contrôle en ligne du 5 janvier 2023, composés de huit caractères, le seul critère de complexité imposé aux utilisateurs étant d'intégrer un chiffre à leur mot de passe. Ainsi, les mots de passe générés selon les critères définis par la société présentaient une entropie de 26 bits, alors pourtant que la CNIL recommande une entropie d'au moins 50 bits quand l'authentification prévoit un mécanisme de restriction de l'accès au compte.

82. La formation restreinte considère qu'une telle construction des mots de passe ne permettait pas d'assurer la sécurité des données et d'empêcher que des tiers non autorisés y aient accès. Si, à la suite des contrôles, la société a modifié sa politique de mots de passe pour exiger une combinaison de huit caractères incluant un caractère spécial, un chiffre, des lettres majuscules et minuscules, puis douze caractères avec une extension du panel de caractères spéciaux, la formation restreinte relève que de tels mots de passe (qui présentaient une entropie de 26 bits au moment des contrôles) étaient insuffisants à assurer la sécurité des données traitées au regard de l'état de l'art.

83. Elle rappelle, comme l'a souligné la rapporteure, que la société traitait un volume important de données à caractère personnel puisque, d'après les informations communiquées, elle traitait les données de plus de 10,8 millions de membres du programme de fidélité, accessibles depuis les comptes client, telles les noms, prénoms, dates de naissance, numéros de téléphone, adresses électronique et adresses postales des personnes concernées.

84. Au vu de ce qui précède, la formation restreinte considère qu'au jour des contrôles, la politique de mots de passe de la société X ne permettait pas d'assurer la sécurité des données à caractère personnel traitées, ce qui constitue un manquement aux dispositions de l'article 32 du RGPD.

85. La formation note qu'en cours de procédure, la société s'est mise en conformité sur ce point en adoptant une nouvelle politique de mots de passe permettant désormais d'assurer un niveau de sécurité conforme à l'état de l'art. Dans ces conditions, le prononcé d'une injonction, tel que proposé par la rapporteure, n'apparait plus opportun.

2) Sur le stockage des mots de passe

86. La conservation des mots de passe de manière sécurisée constitue une précaution élémentaire en matière de protection des données à caractère personnel. Dès 2013, l'ANSSI alertait et rappelait les bonnes pratiques s'agissant de la conservation des mots de passe en indiquant que ces derniers doivent " être stockés sous une forme transformée par une fonction cryptographique à sens unique (fonction de hachage) et lente à calculer telle que PBKDF2 " et que " la transformation des mots de passe doit faire intervenir un sel aléatoire pour empêcher une attaque par tables précalculées " (ANSSI, " Bulletin d'actualité CERTA-2013-ACT-046 ", 15 novembre 2013, https://www.cert.ssi.gouv.fr/actualite/CERTA-2013-ACT-046/). L'ANSSI précisait également dans ses recommandations relatives à l'authentification multifacteur et aux mots de passe que " les fonctions de hachage cryptographique recommandées, comme la famille SHA2, sont des fonctions très rapides à exécuter, ce qui, dans le contexte du stockage des mots de passe, est un avantage pour les attaquants, leur permettant de tester de nombreux mots de passe " (https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe).

87. De même, dans sa délibération n° 2017-012 du 19 janvier 2017, la CNIL indiquait déjà qu'elle " recommande [que le mot de passe] soit transformé au moyen d'une fonction cryptographique non réversible et sûre (c'est-à-dire utilisant un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue), intégrant l'utilisation d'un sel ou d'une clé ", recommandation confirmée dans sa délibération n° 2022-100 du 21 juillet 2022. En effet, les fonctions de hachage non robustes présentent des vulnérabilités connues qui ne permettent pas de garantir l'intégrité et la confidentialité des mots de passe en cas d'attaque par force brute après compromission des serveurs qui les hébergent. La CNIL recommande également, dans son " Guide RGPD du développeur " publié le 27 janvier 2020, que le stockage d'un mot de passe se fasse " au moyen d'une librairie éprouvée, comme Argon2, yescrypt, scrypt, balloon, bcrypt et, dans une moindre mesure, PBKDF2 ".

88. Ainsi, le stockage des mots de passe des utilisateurs doit être réalisé de façon sécurisée. A cet égard, il est recommandé de stocker les empreintes de mots de passe plutôt que les mots de passe en clair. Pour obtenir une telle empreinte de mot de passe, il est en principe nécessaire de recourir à une fonction de hachage cryptographique mathématiquement éprouvée et lente à exécuter, tout en utilisant un sel aléatoire et long pour chaque mot de passe (d'une longueur d'au moins 128 bits), et ce, afin de se prémunir contre des attaquants qui auraient précalculé des tables de correspondance entre les mots de passe et leurs empreintes respectives.

89. La rapporteure relève que les mots de passe des comptes utilisateurs du site web de la société étaient stockés hachés avec la fonction de hachage SHA256 et l'ajout d'un sel. Elle considère que de telles modalités de stockage constituent un manquement à l'article 32 du RGPD, dans la mesure où cette fonction n'est pas conçue pour permettre le stockage sécurisé des mots de passe puisque sa rapidité de calcul pourrait permettre à un attaquant ayant accès aux mots de passe hachés de procéder à la création d'une table de correspondance entre tous les mots de passe les plus courants et leur dérivé résultant de l'exécution de la fonction SHA256, afin de retrouver les mots de passe originaux à partir de leur version hachée dans la base de données.

90. En défense, si la société ne conteste pas les modalités de stockage des mots de passe relevées lors des opérations de contrôle, elle précise néanmoins que le sel utilisé était composé d'une chaîne alphanumérique de 60 caractères, soit 480 bits, de l'adresse de courriel, du mot de passe de l'utilisateur ainsi que d'un composant aléatoire. Elle soutient que cette solution répondait aux recommandations de l'ANSSI, qui suggère " un sel aléatoire long d'au moins 128 bits ", ainsi qu'aux recommandations de la CNIL. Elle fait valoir qu'elle était dès lors convaincue agir en conformité avec les exigences réglementaires et conformément à l'état de l'art, et que les recommandations de l'ANSSI étaient ambivalentes dès lors qu'elle relevait que les " fonctions de hachage cryptographique (comme les familles SHA2 ou SHA3) semblaient au premier abord de bons outils pour stocker les mots de passe ".

91. Dans ses observations en réponse du 23 juin 2025, la société précise avoir procédé à la refonte de son système de stockage et avoir remplacé la fonction SHA256 par Argon2.

92. La formation restreinte rappelle que la fonction de hachage SHA256 appartenant à la famille SHA2 n'est pas considérée comme adaptée pour un stockage sécurisé des mots de passe, comme le relève également l'ANSSI dans sa recommandation R29 du 8 octobre 2021 relatives à l'authentification multifacteur et aux mots de passe. Elle considère qu'il existe un risque substantiel qu'un attaquant, qui accède au système d'information de la société et aux empreintes des

mots de passe de ses utilisateurs, trouve très rapidement le mot de passe correspondant à chaque empreinte conservée par la société dans la mesure où l'algorithme de hachage est très rapide et ne peut ralentir l'attaquant.

93. Elle relève que si l'ajout d'un sel permet d'augmenter le nombre d'empreintes de mots de passe possibles et de se prémunir contre des attaquants utilisant des tables précalculées, celui-ci n'a aucune incidence sur le temps de recherche des empreintes stockées. Si l'ANSSI indique, dans ses recommandations précitées, qu'il est recommandé d'utiliser un sel choisi aléatoirement pour chaque compte, d'une longueur d'au moins 128 bits, elle n'en déduit pas que les mots de passe peuvent être stockées avec la fonction de hachage SHA256, fonction qu'elle considère comme étant très rapide à exécuter et constituant, dans le contexte du stockage des mots de passe, un avantage pour les attaquants. De même, la CNIL indiquait dans sa délibération du 21 juillet 2022, que tout mot de passe doit être, avant d'être stocké, préalablement transformé au moyen d'une fonction cryptographique spécialisée, non réversible et sûre, intégrant un sel.

94. En l'espèce, la formation restreinte considère que, si la société avait mis en place, avec le recours à un sel aléatoire d'une longueur de 128 bits, une mesure de sécurité recommandée, celle-ci demeurait insuffisante dès lors que les mots de passe étaient chiffrés avec une fonction de hachage qui demeurait trop rapide à exécuter pour un attaquant.

95. La formation restreinte considère par conséquent qu'il revenait à la société X d'utiliser une fonction de hachage lente à calculer pour le stockage des mots de passe, tel qu'il ressort clairement des recommandations de l'ANSSI et de la CNIL précitées, afin de permettre en cas d'attaque, par exemple par force brute ou par dictionnaire, de ralentir un attaquant dans son identification des mots de passe.

96. Au vu de ce qui précède, la formation restreinte considère qu'au jour des contrôles, les modalités de stockage des mots de passe de la société X ne permettaient pas d'assurer leur confidentialité, ce qui constitue un manquement aux dispositions de l'article 32 du RGPD.

97. La formation note qu'en cours de procédure, la société s'est mise en conformité sur ce point en modifiant son système de stockage des mots de passe, celui-ci permettant désormais d'assurer la sécurité et la confidentialité des données. Dans ces conditions, le prononcé d'une injonction, tel que proposé par le rapporteur, n'apparait plus opportun.

F. Sur le manquement à l'obligation d'effectuer une analyse d'impact relative à la protection des données en application de l'article 35 du RGPD

98. En droit, l'article 35, paragraphe 1 du RGPD dispose que " lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires ".

99. Aux termes du paragraphe 4 de cet article, " l'autorité de contrôle établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise […] ".

100. Selon le considérant 91 du RGPD, une analyse d'impact " devrait s'appliquer, en particulier, aux opérations de traitement à grande échelle qui visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées […] ".

101. À titre d'éclairage, les lignes directrices du Groupe de travail de l'article 29 (dit " G29 " devenu le Comité Européen de Protection des Données) concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est " susceptible d'engendrer un risque élevé " aux fins du règlement (UE) 2016/679, modifiées et adoptées en dernier lieu le 4 octobre 2017, ont fixé une liste de neuf critères à prendre en compte pour donner une vision plus concrète des opérations de traitement qui nécessitent une analyse d'impact du fait d'un risque inhérent élevé. Parmi ces critères figurent notamment la collecte de données à caractère personnel à grande échelle et le croisement ou la combinaison d'ensembles de données.

102. Ces lignes directrices ajoutent que, " dans la plupart des cas, le responsable du traitement peut considérer qu'un traitement satisfaisant à deux critères nécessite une AIPD ".

103. Dans le sillage du CEPD, la CNIL a établi, dans sa délibération n° 2018-326 du 11 octobre 2018, des lignes directrices sur les analyses d'impact relatives à la protection des données. La délibération rappelle les hypothèses dans lesquelles une AIPD est nécessaire et se réfère notamment aux critères identifiés par le CEPD.

104. En outre, la CNIL rappelle, dans cette délibération, que " de manière générale, un traitement qui rencontre au moins deux des critères mentionnés ci-dessus doit faire l'objet d'une AIPD ".

105. Enfin, dans les lignes directrices 8/2020 sur le ciblage des utilisateurs de médias sociaux précitées, le CEPD précise qu'en cas de responsabilité conjointe, " les responsables conjoints du traitement doivent évaluer si une AIPD est nécessaire. Si une AIPD est nécessaire, ils sont tous deux responsables de satisfaire cette obligation " (§108).

106. La rapporteure relève que la société n'avait pas réalisé d'analyse d'impact avant de mettre en œuvre le traitement de publicité ciblée mené sur le réseau social Z. Elle estime que, dès lors qu'il impliquait un traitement de données à grande échelle et un croisement de données entre les sociétés X et Y, il était susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques et qu'une analyse d'impact aurait dès lors dû être menée.

107. En défense, la société reconnait qu'elle n'avait pas effectué d'analyse d'impact avant la mise en œuvre du traitement susvisé, mais qu'une telle analyse est devenue sans objet, le traitement en cause ayant cessé. Elle précise par ailleurs avoir mis en place un suivi régulier de ses traitements, afin d'identifier ceux nécessitant à l'avenir la réalisation d'une AIPD.

108. La formation restreinte relève qu'en traitant les données de plus de 10,8 millions de personnes dans l'Union européenne, la société mettait en œuvre un traitement de données à caractère personnel à grande échelle et, qu'en outre, le traitement en cause impliquait un croisement de données entre celles détenues par la société X et celles détenues par le groupe Y. Ces éléments ne sont pas contestés par la société.

109. Dès lors, dans la mesure où le traitement en cause concerne un volume important de données, qu'il est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes et que deux des critères définis par le CEPD étaient réunis, la formation restreinte estime que la société aurait dû mener une analyse d'impact préalablement à la mise en œuvre des traitements relatifs aux opérations de publicité ciblée menées sur le réseau social Z, pour les besoins desquels elle transmettait des données au groupe Y.

110. La formation restreinte considère ainsi qu'en s'abstenant de procéder à telle analyse, la société X a commis un manquement aux dispositions de l'article 35 du RGPD.

111. La formation restreinte relève que dans la mesure où la société a cessé toute transmission de données au groupe Y, la réalisation d'une AIPD relative aux traitements susvisés est aujourd'hui sans objet. Dans ces conditions, le prononcé d'une injonction, tel que proposé par le rapporteur, n'apparait plus opportun.

G. Sur le manquement à l'obligation d'informer les personnes concernées et d'obtenir leur consentement avant d'inscrire des informations (cookies) sur leur terminal de communications électroniques ou d'accéder à celles-ci (lecture des cookies) en application de l'article 82 de la loi Informatique et Libertés

112. En droit, l'article 82 de la loi Informatique et Libertés, transposant l'article 5, paragraphe 3 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (ci-après, " la directive vie privée et communications électroniques " ou " la directive ePrivacy "), dispose que " tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant :

1° De la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ;

2° Des moyens dont il dispose pour s'y opposer.

Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son consentement qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.

Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :

1° Soit, a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;

2° Soit, est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur ".

113. Cet article prévoit ainsi expressément que les opérations d'accès ou d'inscription d'informations dans le terminal d'un utilisateur ne peuvent avoir lieu qu'après que ce dernier a exprimé son consentement. De manière corrélative, cet article offre nécessairement à l'utilisateur la possibilité de refuser ce dépôt, ou de revenir sur son choix d'accepter que des cookies et/ou traceurs soient déposés sur son terminal en retirant son consentement.

114. Depuis l'entrée en application du RGPD, le " consentement " prévu à l'article 82 précité doit s'entendre au sens de l'article 4, paragraphe 11 du RGPD, c'est-à-dire qu'il doit être donné de manière libre, spécifique, éclairée et univoque et se manifester par un acte positif clair.

115. La formation restreinte rappelle également que seuls les traceurs strictement nécessaires à la fourniture d'un service de communication en ligne expressément demandé par l'utilisateur, et les traceurs ayant pour finalité exclusive de permettre ou de faciliter la communication par voie électronique, sont exemptés de cette obligation de recueil préalable du consentement pour leur dépôt ou leur lecture.

116. La rapporteure relève que les constatations réalisées par la délégation lors du contrôle en ligne du 5 janvier 2023 ont permis de mettre en évidence le dépôt, sur le terminal de l'utilisateur et avant que le consentement de ce dernier soit recueilli, de plusieurs cookies. Parmi ces cookies, figure le cookie " IADVIZE ", outil de tchat en ligne (" chatbox ") avec un conseiller expert qui permet une reconnaissance unique de l'utilisateur et un enregistrement de l'historique de conversation. Elle relève également que sept autres cookies permettent la personnalisation de contenus à partir de l'historique de navigation de l'utilisateur et l'analyse de sa navigation. Elle considère par conséquent que ces cookies sont soumis à l'exigence de recueil du consentement. Elle relève également que ces cookies n'étaient pas supprimés du navigateur après que l'utilisateur a refusé les cookies " non essentiels ", et qu'ils continuaient ainsi à être lus malgré ce refus. Elle considère que ces faits constituent un manquement à l'article 82 de la loi Informatique et Libertés.

117. En défense, la société admet que les cookies en cause étaient bien déposés avant tout recueil du consentement de l'utilisateur. Elle précise que, pour certains d'entre eux, elle avait considéré qu'ils pouvaient relever de son intérêt légitime et insiste sur le fait que les cookies concernés n'ont pas pour finalité de collecter ou de transmettre des données à des tiers à des fins de profilage ou de prospection commerciale, mais ont pour seule finalité d'optimiser l'expérience utilisateur sur le site. Elle ajoute avoir, depuis les contrôles, pris des mesures permettant de garantir que ces cookies ne sont plus déposés en l'absence de consentement de l'utilisateur.

118. La formation restreinte relève qu'il ressort des constatations réalisées lors du contrôle en ligne du 5 janvier 2023 que, lors de son arrivée sur le site web " [...] ", l'utilisateur voit s'afficher une fenêtre surgissante relative aux cookies, au bas de laquelle figurent deux boutons intitulés respectivement " En savoir plus " et " Accepter et fermer ", ainsi qu'un lien en haut à gauche de la fenêtre intitulé " continuer sans accepter ".

119. La délégation a constaté qu'avant même que l'utilisateur ait exprimé un choix quant au dépôt et à la lecture de cookies sur son terminal, et alors que la fenêtre surgissante était toujours affichée, onze cookies étaient déposés sur son terminal.

120. La formation restreinte relève en outre qu'il ressort de ces constats qu'après avoir cliqué sur le lien " continuer sans accepter " (et après avoir donc refusé le dépôt et la lecture de cookies non essentiels), les onze cookies précités n'étaient pas supprimés du navigateur et continuaient ainsi à être lus.

121. La formation restreinte note que, parmi ces onze cookies, était déposé le cookie " iadvize-5593-vuid ". La société a précisé que " IADVIZE " est " un outil de tchat en ligne (" chatbox ") avec un conseiller expert afin d'aider l'utilisateur dans ses achats. Le cookie [en question] permet d'identifier de manière unique l'utilisateur et de personnaliser l'affichage et la conversation avec l'utilisateur en fonction de sa navigation sur le site. Il permet également de reconnaître l'utilisateur à chaque visite afin de conserver son historique de conversation ". Elle relève que la société a précisé au cours de l'instruction que, depuis le 17 janvier 2023, ce tchat en ligne n'apparaissait plus sur l'ensemble des pages du site mais uniquement sur les pages de contact et certaines fiches de produits où son utilité est la plus pertinente pour l'utilisateur – le consentement étant désormais systématiquement demandé préalablement au dépôt de tout cookie lié à ce service.

122. La formation restreinte considère que ce cookie, en permettant une reconnaissance unique des utilisateurs et un enregistrement de l'historique de conversation, n'avait pas pour finalité exclusive de permettre ou de faciliter la communication par voie électronique et n'était pas non plus strictement nécessaire à la fourniture d'un service expressément demandé par les utilisateurs du site web de la société. La formation restreinte relève à cet égard que la société a reconnu que le dépôt d'un tel cookie requérait le consentement des personnes et que celui-ci n'était pas recueilli en l'espèce.

123. La formation restreinte observe que la société a fourni, dans le cadre de l'instruction, une capture écran indiquant que le consentement des personnes est recueilli depuis le 17 janvier 2023, à l'issue du contrôle en ligne du 5 janvier 2023.

124. Par ailleurs, la formation restreinte relève qu'étaient également déposés, parmi les onze cookies susvisés, les cookies " t2s-p ", " t2s-analytics " et " t2s-rank ", ayant pour finalité la personnalisation de contenus éditoriaux en fonction de l'historique de navigation de l'utilisateur afin de lui proposer des produits adaptés, ainsi que les cookies " wizville_cookie_page_load ", " wizville_cookie_session_start_at ", " wizville_cookie_first_visit " et " wizville_cookie_page_count ", ayant pour finalité la mémorisation des informations de navigation sur le site web " [...]" visité par l'utilisateur, afin d'afficher ou non un questionnaire de satisfaction destiné à recueillir l'avis de l'utilisateur sur le

site web. Elle considère que de tels cookies, qui permettent de réaliser une personnalisation du contenu du site web en fonction d'informations obtenues sur les utilisateurs, telles que leur historique de navigation, afin d'afficher un questionnaire de satisfaction ou des produits adaptés, n'ont pas pour finalité de permettre ou faciliter la communication par voie électronique, et ne sont pas strictement nécessaires à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

125. Elle relève que la société a fourni, dans le cadre de l'instruction, une capture écran de gestion du cookie " wizville " démontrant que le consentement des personnes est recueilli depuis le 1er mars 2023. Elle a, en outre, fourni une capture écran de gestion du cookie " t2s ", ainsi que des captures écrans du site web " [...] ", permettant de démontrer que, depuis le 3 juin 2025, les cookies " t2s " ne sont plus déposés en l'absence de consentement de l'utilisateur.

126. Au vu de ce qui précède, la formation restreinte considère qu'en procédant au dépôt et à la lecture des cookies susvisés sur le terminal de l'utilisateur sans recueillir préalablement son consentement, la société X a méconnu les dispositions de l'article 82 de la loi Informatique et Libertés.

127. La formation restreinte note que, postérieurement aux opérations de contrôle, la société X s'est mise en conformité en démontrant que les cookies susvisés n'étaient plus déposés sur le terminal des utilisateurs avant que leur consentement ne soit recueilli. Elle rappelle néanmoins que les mesures de mise en conformité adoptées ne sauraient exonérer la société de sa responsabilité pour les faits passés.

III. Sur les mesures correctrices

128. L'article 20-IV 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 : […]

2° Une injonction de mettre en conformité le traitement avec les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans les cas où le traitement est mis en œuvre par l'Etat, d'une astreinte dont le montant ne peut excéder 100 000 euros par jour de retard à compter de la date fixée par la formation restreinte ;

[…]

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 ".

129. L'article 83 du RGPD, tel que visé par l'article 20, paragraphe IV, 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.

130. La CJUE a rappelé à cet égard que " seule une amende administrative dont le montant est déterminé en fonction de la capacité économique réelle ou matérielle de son destinataire […] est susceptible de réunir les trois conditions énoncées à l'article 83, paragraphe 1, du RGPD, à savoir d'être à la fois effective, proportionnée et dissuasive " (CJUE, grande chambre, 5 décembre 2023, C-807/21, " Deutsche Wohnen " ; CJUE, cinquième chambre, 13 février 2025, C-383/23, " Ilva A/S "),

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

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

132. La formation restreinte rappelle qu'il convient d'examiner les critères pertinents de l'article 83 du RGPD pour décider s'il y a lieu d'imposer une amende administrative à la société et, le cas échéant, pour déterminer son montant.

1. Sur le prononcé d'une amende administrative

133. La rapporteure propose à la formation restreinte de prononcer à l'encontre de la société une amende administrative au regard des manquements constitués aux articles 6, 13, 32 et 35 du RGPD, ainsi qu'à l'article 82 de la loi Informatique et

Libertés.

134. En défense, la société fait valoir que les manquements constatés ne présentent aucun caractère de gravité, que les personnes concernées n'ont subi aucun préjudice et qu'aucune donnée à caractère personnel sensible n'a été concernée par les manquements. Elle souligne également sa pleine coopération avec les services de la CNIL et la rapidité avec laquelle elle a apporté les mesures correctives nécessaires, avant même qu'elle n'ait été informée de l'ouverture d'une procédure de sanction. Elle conteste enfin s'être montrée négligente ou avoir agi de manière délibérée et soutient qu'elle ne disposait d'aucune décision antérieure de la CNIL susceptible de lui servir de référence dans le cadre du traitement mis en œuvre avec le groupe Y.

135. 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 ait 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.

136. En premier lieu, la formation restreinte considère qu'il y a lieu de faire application du critère prévu à l'article 83, paragraphe 2, a) du RGPD relatif à la nature, à la gravité et à la durée de la violation, compte tenu de la nature, de la portée ou de la finalité des traitements concernés ainsi que du nombre de personnes concernées.

137. La formation restreinte note tout d'abord que plusieurs manquements relevés sont relatifs aux opérations de publicité ciblée réalisées sur le réseau social Z, pour les besoins desquelles la société transmettait au groupe Y les données à caractère personnel des adhérents à son programme de fidélité. Il a en effet été démontré qu'un tel traitement était mis en œuvre sans que les personnes concernées y aient consenti de manière éclairée et spécifique, sans qu'elles en aient été clairement informées et sans qu'une analyse d'impact ait été menée préalablement. La formation restreinte relève, premièrement, que deux de ces manquements concernent des principes fondamentaux de la protection des données, relatifs à la licéité du traitement et l'information des personnes. Elle observe à cet égard que ces manquements entrent dans les prévisions de l'article 83, paragraphe 5 du RGPD, et sont ainsi susceptibles d'être sanctionnés par l'amende la plus élevée prévue par le législateur européen. Deuxièmement, la formation restreinte insiste sur le nombre particulièrement élevé de personnes concernées, la société ayant reconnu que les données de l'ensemble des adhérents à son programme de fidélité, à savoir plus de 10,5 millions de personnes, avaient été transmises au groupe Y. Troisièmement, s'agissant de la durée des violations, la formation restreinte relève que la société transmettait les données au groupe Y depuis fin 2018, de façon hebdomadaire, et qu'une telle transmission a duré plus de cinq années, à savoir jusqu'en février 2024. Si la société a procédé de sa propre initiative à la cessation du traitement en cause, ce qui doit être mis à son crédit, la formation restreinte relève néanmoins qu'elle ne l'a fait qu'après avoir été confrontée à un contrôle de la CNIL qui, selon ses propres déclarations, a soulevé de nombreuses interrogations.

138. Ensuite, s'agissant du manquement à l'obligation d'assurer la sécurité des données à caractère personnel, la formation restreinte relève qu'il concerne des obligations élémentaires en matière de sécurité, à savoir la robustesse des mots de passe utilisés ainsi que le stockage sécurisé de ces derniers. Elle note également qu'un tel manquement concerne l'ensemble des clients de la société et adhérents à son programme de fidélité, les règles de complexité des mots de passe et les modalités de stockage étant les mêmes pour tous.

139. Enfin, s'agissant du manquement relatif aux cookies déposés sur le terminal de l'utilisateur lors de la visite du site web " [...] ", la formation restreinte rappelle qu'au jour du contrôle en ligne, la société traitait les données de ses utilisateurs sans avoir recueilli préalablement leur consentement, en déposant sur leurs terminaux des cookies pourtant soumis au recueil préalable d'un consentement. Elle considère qu'un tel manquement constitue une atteinte substantielle au droit au respect de la vie privée des personnes concernées.

140. En deuxième lieu, la formation restreinte estime qu'il convient de tenir compte du critère prévu à l'article 83, paragraphe 2, b) du RGPD, relatif au fait que la violation ait été commise délibérément ou par négligence.

141. La formation restreinte souligne que le nombre de manquements constatés révèle une particulière négligence de la part de la société. Plus particulièrement, concernant le manquement à l'article 6 paragraphe 1, a) du RGPD, la formation restreinte considère que la société aurait dû, compte tenu du caractère massif du traitement en cause, faire preuve d'une vigilance accrue.

142. En outre, s'agissant du manquement à l'article 32 du RGPD, il y a lieu de rappeler que la Commission communique régulièrement sur l'importance que revêtent les mesures d'authentification en matière de sécurité, que ses recommandations relatives à la politique de mots de passe étaient déjà très connues au moment des contrôles, et que depuis le mois de décembre 2022, elle a de surcroit mis à disposition des organismes, sur son site web, un outil permettant de vérifier de manière simple la robustesse d'un mot de passe. Elle rappelle en outre avoir régulièrement adopté des

sanctions pécuniaires pour manquement à l'article 32 du RGPD en raison de mesures insuffisantes pour garantir la sécurité des données traitées, notamment dans ses délibérations n° SAN-2019-007 du 18 juillet 2019, n° SAN-2022-018 du 8 septembre 2022, n° SAN-2023-023 du 29 décembre 2023 et n° SAN-2024-002 du 31 janvier 2024.

143. Par ailleurs, s'agissant du manquement à l'article 82 de la loi Informatique et Libertés, la formation restreinte rappelle que la Commission a accompagné les acteurs du numérique dès 2013, en publiant une recommandation et des lignes directrices rappelant les principes qu'il convient de respecter pour permettre l'utilisation des cookies et autres traceurs. De nouvelles recommandations et lignes directrices ont été adoptées en 2020 et ont, elles aussi, fait l'objet d'une large diffusion. La formation restreinte rappelle également avoir déjà sanctionné à de nombreuses reprises des organismes pour non-respect de l'obligation de recueillir le consentement de l'utilisateur avant toute opération de lecture et/ou d'écriture (délibération n° SAN-2020-012 du 7 décembre 2020 validée par le Conseil d'État dans sa décision n° 44209 du 28 janvier 2022 ; délibération n° SAN-2020-013 du 7 décembre 2020 validée par le Conseil d'État dans sa décision n° 451423 du 27 juin 2022).

144. Enfin, tout en tenant compte de ce que la société a mis en place des mesures permettant d'assurer sa mise en conformité, dont certaines ont été prises avant même la notification du rapport de sanction, la formation restreinte relève que ces actions n'exonèrent pas la société de sa responsabilité pour les faits passés.

145. En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative pour les manquements aux articles 6, 13, 32 et 35 du RGPD et 82 de la loi Informatique et Libertés.

2. Sur le montant de l'amende administrative

146. En défense, la société soutient que le montant proposé par la rapporteure est disproportionné et excessif au regard de la réalité de l'atteinte portée aux droits des personnes. Elle invoque également sa situation économique qui s'est dégradée en 2024, ainsi que les conséquences que pourraient avoir une sanction financière élevée sur son activité. Elle fait valoir que son résultat net a baissé, passant de […] euros en 2023 à […] euros en 2024, et illustre les spécificités de son modèle économique ainsi que la faible marge caractéristique de son secteur d'activité.

147. La formation restreinte relève tout d'abord que les manquements relatifs aux articles 6 et 13 du RGPD sont des manquements à des principes fondamentaux du RGPD, susceptibles de faire l'objet, en vertu de l'article 83 du RGPD, d'une amende administrative pouvant s'élever jusqu'à 20 000 000 euros ou jusqu'à 4 % du chiffre d'affaires annuel, le montant le plus élevé étant retenu. Elle rappelle en outre que les amendes administratives doivent être dissuasives et proportionnées.

148. Ensuite, la formation restreinte considère que l'activité de la société et sa situation financière doivent également être prises en compte. Elle relève tout d'abord que le chiffre d'affaires réalisé en 2023 était de […] d'euros, son résultat net s'élevant à […] d'euros.

149. La formation restreinte rappelle ensuite, comme cela est détaillé au paragraphe 130, que pour s'assurer du caractère effectif, dissuasif et proportionné de l'amende prononcée, il convient de prendre en compte la capacité économique réelle ou matérielle de son destinataire. Une telle capacité économique ne saurait s'apprécier exclusivement au regard du résultat net dégagé par l'entreprise (qui peut être affecté par des éléments exceptionnels), mais doit tenir compte d'un ensemble d'éléments d'analyse financière, tels que le chiffre d'affaires, mentionné par l'article 83 du RGPD, le compte de résultat, l'endettement, la trésorerie, etc. En l'espèce, la formation restreinte considère que si le résultat net de la société a en effet subi une baisse entre l'année 2023 et l'année 2024, l'analyse de l'ensemble des éléments financiers de la société démontre que celle-ci n'est pas, contrairement à ce qu'elle affirme, dans une situation économique dégradée, comme en attestent notamment la trésorerie disponible et les réserves dont disposait la société en 2023.

150. Ainsi, au regard de la responsabilité de la société, de ses capacités financières et des critères pertinents de l'article 83, paragraphe 2 du RGPD évoqués ci-avant, la formation restreinte considère qu'une amende administrative, d'une part, d'un montant de deux millions cinq cent mille (2 500 000) euros pour sanctionner les manquements aux articles 6 paragraphe 1, a), 13, 32 et 35 du RGPD et d'autre part, d'un montant de un million (1 000 000) d'euros pour sanctionner le manquement à l'article 82 de la loi Informatique et Libertés apparait dissuasive et proportionnée.

B. Sur le prononcé d'une injonction

151. Dans son rapport initial, la rapporteure proposait à la formation restreinte de prononcer à l'encontre de la société une injonction de mettre en conformité le traitement avec les dispositions des articles 6, 13, 32 et 35 du RGPD et 82 de la loi Informatique et Libertés, assortie d'une astreinte.

152. En défense, la société soutient que le prononcé d'une injonction est sans objet, dès lors qu'elle a déployé des mesures de mise en conformité en cours de procédure.

153. Compte tenu des éléments développés ci-avant et de la mise en conformité de la société s'agissant de l'ensemble des manquements relevés, la formation restreinte considère qu'il n'y a pas lieu de prononcer d'injonction.

C. Sur la publicité de la sanction

154. La société conteste la proposition de la rapporteure de rendre publique la présente délibération, au motif notamment qu'une telle publicité risque de fragiliser son équilibre commercial ainsi que la confiance de ses adhérents, sans pour autant apporter de bénéfice à l'intérêt général et tout en favorisant ses concurrents.

155. La formation restreinte considère que la publicité de la présente décision est justifiée au regard des manquements en cause et du nombre de personnes concernées, le recours à la publicité ciblée sur le réseau social Z étant, notamment, une pratique répandue parmi les acteurs économiques. Dans ce contexte, il importe d'informer les personnes concernées sur les règles applicables en matière de consentement. La formation restreinte considère toutefois que, dans cette perspective, une publication de la décision sans que la société y soit nommément identifiée est suffisante.

PAR CES MOTIFS

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

- de prononcer à l'encontre de la société X une amende administrative d'un montant de trois millions cinq cent mille (3 500 000) euros pour l'ensemble des manquements constatés, qui se décompose comme suit :

-

o deux millions cinq cent mille (2 500 000) euros au regard des manquements constitués aux articles 6 paragraphe 1, a), 13, 32 et 35 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ;

o un million (1 000 000) d'euros au regard du manquement constitué à l'article 82 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

- **de rendre publique, sur le site de la CNIL et sur le site de Légifrance, sa délibération,** qui n'identifiera pas nommément la société dès la publication.

Le Président

Philippe-Pierre CABOURDIN

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