RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Légifrance
Le service public de la diffusion du droit

Délibération du 31 mars 2022

Commission Nationale de l'Informatique et des Libertés Etat juridique : En vigueur

Date de publication sur Légifrance : Mercredi 06 avril 2022

Délibération de la formation restreinte n°SAN-2022-008 du 31 mars 2022 relative à l'injonction prononcée à l'encontre de la société SPARTOO par la délibération n°SAN-2020-003 du 28 juillet 2020

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de Messieurs Alexandre LINDEN, président, Philippe-Pierre CABOURDIN, vice-président, de Mesdames Anne DEBET et Christine MAUGÜE, et de Monsieur Alain DRU, membres ;

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

Vu la loi no 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 20 et suivants ;

Vu le décret no 2019-536 du 29 mai 2019 pris pour l'application de la loi

no 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération no 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la délibération no SAN-2020-003 du 28 juillet 2020 prononçant une sanction à l'encontre de la société SPARTOO ;

Vu les éléments transmis par la société SPARTOO le 5 novembre 2020, les 7 avril et 16 décembre 2021 et le 2 février 2022 ;

Vu les autres pièces du dossier ;

Après en avoir délibéré lors de sa séance du 10 février 2022, a adopté la décision suivante :

I. Faits et procédure

1. La société SPARTOO SAS (ci-après "la société"), est spécialisée dans le secteur de la vente à distance de chaussures. Par sa délibération no 2020-003 du 28 juillet 2020, notifiée le 4 août 2020, la formation restreinte a, entre autres dispositions, prononcé une injonction de mettre en conformité le traitement avec les obligations résultant des articles 5-1 c), 5- 1 e), 13 et 32 du règlement no 2016/679 du 27 avril 2016 relatif à la protection des données (ci-après RGPD)

2. L'injonction était formulée en ces termes :

"prononcer à l'encontre de la société SPARTOO SAS une injonction de mettre en conformité les traitements avec les obligations résultant des articles 5-1 c), article 5- 1 e), 13 et 32 du règlement no 2016/679 du 27 avril 2016 relatif à la protection des données, et en particulier :

• s'agissant du manquement au principe de minimisation des données à caractère personnel :

o justifier de la fin des enregistrements non ponctuels et non aléaloires des conversations téléphoniques des conseillers lorsque la finalité poursuivie est leur formation ou leur évaluation ;

• s'agissant du manquement au principe de limitation de la durée de conservation des données, définir et mettre en œuvre une politique de durée de conservation des données relatives aux clients et aux prospects qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées, et notamment :

o justifier de la procédure d'archivage intermédiaire des données à caractère personnel des clients mise en place, après avoir opéré un tri des données pertinentes à archiver et une suppression des données non pertinentes, ainsi que du point de départ de cet archivage ;

o justifier de la restriction des accès des salariés aux données à caractère personnel présentes en base active aux seules personnes ayant à en connaître;

o cesser de traiter les données des prospects au-delà du délai à l'issue duquel la société ne les contacte plus (en l'espèce deux ans) et cesser de prendre en compte, comme dernier point de contact émanant de ces derniers, la simple ouverture d'un

courriel ;

o cesser de conserver les adresses électroniques et mots de passes hachés des anciens clients à l'issue de la période d'inactivité fixée et procéder à la purge de telles données conservées par la société jusqu'à la date de la délibération de la formation restreinte ;

o justifier de la suppression des données concernant les clients au-delà de la période d'inactivité définie, dont il appartiendra à la société de justifier, et concernant les prospects au-delà de deux ans d'inactivité ;

• s'agissant du manquement à l'obligation d'informer les personnes :

o procéder à l'information des salariés relative à la mise en place d'un dispositif d'enregistrement des conversations téléphoniques concernant notamment les finalités poursuivies, la base légale du dispositif, les destinataires des données issues du dispositif, la durée de conservation des données, les droits des salariés notamment d'accès aux données les concernant, la possibilité d'introduire une réclamation auprès de la CNIL ;

o procéder à l'information complète des clients, en fournissant une information relative aux différentes bases légales des traitements mis en œuvre par la société;

• s'agissant du manquement à l'obligation d'assurer la sécurité des données personnelles, prendre toute mesure, pour l'ensemble des traitements de données à caractère personnel mis en œuvre, permettant de préserver la sécurité de ces données et d'empêcher que des tiers non autorisés y aient accès en application de l'article 32 du RGPD, notamment :

o mettre en œuvre une politique de gestion des mots de passe contraignante, s'agissant des comptes clients selon l'une des modalités suivantes ;

les mots de passe sont composés d'au minimum douze caractères, contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial ;

les mots de passe sont composés d'au moins huit caractères, contenant trois des quatre catégories de caractères (lettres majuscules, lettres minuscules, chiffres et caractères spéciaux) et s'accompagnent d'une mesure complémentaire comme 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) ;

3. Cette injonction était assortie d'une astreinte de 250 euros par jour de retard à l'issue d'un délai de trois mois suivant la notification de la délibération, les justificatifs de la mise en conformité devant être adressés à la formation restreinte dans ce délai.

4. Le 5 novembre 2020, la société a adressé à la Commission nationale de l'informatique et des libertés (ci-après "la Commission" ou "la CNIL") un courrier par lequel elle présentait les mesures mises en place afin de se conformer à l'injonction. Par courrier du 2 février 2021, le président de la formation restreinte a demandé à la société des éléments complémentaires concernant notamment les modalités de conservation par la société des données relatives à ses clients. La société a répondu à cette demande le 7 avril 2021 puis a complété sa réponse par des envois supplémentaires les 16 décembre 2021 et 2 février 2022.

II. Motifs de la décision

A. Sur les mesures prises en lien avec la minimisation des données

5. La formation restreinte relève que les réponses et justificatifs fournis par la société font apparaître que celle-ci a cessé d'enregistrer, à des fins de formation de ses salariés, la totalité des appels téléphoniques reçus par les salariés de son service clients et qu'elle a réduit de façon substantielle la proportion des enregistrements auxquels elle procède.

6. Par conséquent, la formation restreinte considère que la société s'est conformée à ce volet de l'injonction.

B. Sur les mesures prises en lien avec la conservation des données

7. En premier lieu, s'agissant de la gestion des accès des salariés aux seules données à caractère personnel nécessaires pour l'exercice de leurs fonctions, il ressort des réponses et justificatifs fournis par la société que seules trois personnes, dont les fonctions au sein de la société le justifient, ont désormais accès aux données (par exemple, pour effectuer des recherches et analyses en cas de fraude, de plainte ou de réquisition judiciaire).

8. La formation restreinte considère que ces mesures satisfont à ce volet de l'injonction.

9. En deuxième lieu, s'agissant de la conservation des données à des fins de prospection, la formation restreinte relève que dans sa réponse à l'injonction, la société a indiqué avoir modifié le point de départ à partir duquel le délai permettant de déterminer l'inactivité d'un prospect était calculé, pour ne plus prendre en compte la simple ouverture d'un courriel mais par exemple la dernière commande ou la dernière connexion au compte. En outre, la société a justifié avoir supprimé les données qui étaient conservées en application de son ancienne politique de durée de conservation.

10. La formation restreinte considère que, dans ces conditions, les mesures adéquates ont été mises en place pour se conformer à l'injonction et elle observe qu'une conservation des données des prospects durant trois ans à partir de ces points de départ identifiés pour calculer la durée d'inactivité des prospects, n'est pas excessive au sens de l'article 5(1)(e) du RGPD.

11. En troisième lieu, s'agissant de la conservation des données au-delà d'une durée de trois ans à compter de l'inactivité des utilisateurs sous une forme ne permettant plus l'identification des personnes auxquelles elles se rapportent, la formation restreinte relève qu'au cours de l'instruction des suites apportées à l'injonction, la société a progressivement fait évoluer les modalités de conservation envisagées afin que les données conservées ne permettent plus de réidentifier les personnes. En ce sens, la société a notamment:

- réduit le nombre de champs conservés dans sa base de données ;

- cessé de conserver l'identifiant interne attribué à chaque client ;

- réparti les données conservées en trois tables distinctes, dans lesquels les données se rapportant à une même personne sont versées à des moments différents, de façon à ce qu'il ne soit pas possible de faire le lien entre les données se rapportant à une même personne entre les trois tables.

12. La formation restreinte considère que les mesures prises par la société sont de nature à ne plus permettre la réidentification des personnes.

13. En dernier lieu, s'agissant de la conservation des adresses électroniques et des mots de passe des anciens clients sous forme hachée afin de leur permettre de se reconnecter à leur compte, la société a indiqué cesser de proposer cette fonctionnalité et donc mettre fin à la conservation de ces informations pour cette finalité.

14. Par conséquent, la formation restreinte considère la société a satisfait à ce volet de l'injonction.

C. Sur les mesures prises en matière d'information des personnes

15. En premier lieu, s'agissant de l'information des salariés quant à l'enregistrement des appels téléphoniques, il ressort des réponses et justificatifs fournis par la société que cette dernière a fait signer une note d'information à chacun de ses salariés, comportant l'ensemble des informations visées par l'article 13 du RGPD.

16. En second lieu, la formation restreinte constate que la société a complété la politique de confidentialité accessible sur son site web afin d'y faire figurer une description des bases juridiques sur lesquelles reposent ses traitements.

17. Par conséquent, la formation restreinte considère que la société s'est conformée à ce volet de l'injonction.

D. Sur les mesures prises en lien avec la sécurité du traitement

18. La société a produit des justificatifs dont il ressort que les mots de passe permettant d'accéder aux comptes clients doivent désormais être composés d'au moins 8 caractères, dont au moins une minuscule, une majuscule, un chiffre ou un caractère spécial. Elle explique avoir également mis en œuvre une mesure de temporisation d'accès aux comptes.

19. La formation restreinte considère que ces mesures satisfont à ce volet de l'injonction.

20. Par conséquent, la formation restreinte considère que la société SPARTOO a satisfait à l'ensemble de l'injonction.

21. Cette décision sera rendue publique comme l'avait été la délibération no SAN 2020-003 du 28 juillet 2020.

PAR CES MOTIFS

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

- qu'il n'y a pas lieu à liquidation d'astreinte ;

- de rendre publique, sur le site de la CNIL et sur le site de Légifrance, sa délibération, qui n'identifiera plus nommément la société SPARTOO à compter du 5 août 2022.

Le président

Alexandre LINDEN