Lire cet article en ligne

CNIL : SPARTOO est sanctionnée d'une amende de 250 000 euros

La Commission nationale de l'informatique et des libertés (CNIL) vient d'infliger une sanction de 250 000 euros à SPARTOO, une entreprise spécialisée dans la vente en ligne de chaussures. La CNIL lui reproche plusieurs infractions au RGPD, le règlement général sur la protection des données applicable depuis le 25 mai 2018.

Il s'agit de la première décision de sanction adoptée par la CNIL en tant que « chef de file » en coopération avec d'autres autorités de contrôle européennes car les clients de Spartoo dont le siège social est à Grenoble (et leurs données personnelles) dépassent le cadre français.

En mai 2018, une délégation de la CNIL a procédé à une mission de contrôle dans les locaux de la société SPARTOO. Si la mission était de vérifier le respect par la société du RGPD, le contrôle a plus particulièrement porté sur les fichiers clients/prospects et l'enregistrement des conversations téléphoniques entre les clients et les salariés du service client de la société.

En juillet 2018, les clients et prospects de la société concernés étant situés dans plusieurs pays européens, la CNIL a informé l'ensemble des autorités de contrôle européennes de sa compétence pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par la société et ouvert la procédure pour la déclaration des autorités concernées sur ce cas.

En 2019, la Présidente de la CNIL a décidé d'engager une procédure de sanction à l'encontre de la société.

Le 28 juillet 2020, sur la base des investigations menées, la CNIL a considéré dans une délibération n°SAN-2020-003 que la société avait manqué à plusieurs obligations prévues par le RGPD.

Manquement au principe de minimisation des données (article 5-1, c du RGPD)

Pour rappel, l'article 5-1 c) du RGPD dispose que les données à caractère personnel doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données).* »

Enregistrement intégral et permanent des appels téléphoniques reçus par les salariés du service client

L'enregistrement intégral et permanent des appels téléphoniques reçus par les salariés du service client est jugé excessif par la CNIL : selon elle, le fait d'enregistrer tous les appels n'est pas justifié car la personne chargée de la formation des salariés n'écoute qu'un enregistrement par semaine et par salarié.

Enregistrement des données bancaires lors des appels téléphoniques passés avec la société

L'enregistrement et la conservation des coordonnées bancaires des clients, communiquées lorsque les commandes sont passées par téléphone, n'est pas jugé non plus nécessaire pour la finalité poursuivie, à savoir la formation des salariés.

Collecte de données dans le cadre de la lutte contre la fraude

Au vu de la finalité du traitement et du caractère résiduel du nombre de copies de cartes d'identité traitées par la société, la CNIL considère que la copie de la carte d'identité peut constituer un justificatif pertinent.

Par contre, la collecte en Italie de la copie de la « carte de santé » des clients est jugée excessive. Pour la CNIL, la communication de ce document qui contient davantage d'informations que la carte d'identité, alors même qu'une copie de la carte d'identité est également demandée, est excessive et non pertinente.

Manquement à l'obligation de limitation de la durée de conservation des données (article 5-1, e du RGPD)

Pour rappel, l'article 5-1 e) du RGPD dispose que les données à caractère personnel doivent être « *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation).* »

Lors du contrôle de la CNIL, la CNIL a constaté qu'aucune durée de conservation des données des clients et des prospects n'était mise en place par la société, qui n'effaçait pas régulièrement les données personnelles et ne les archivait pas.

Durées de conservation

Si la société a prévu après le contrôle de la CNIL de conserver ces données pendant cinq ans, la CNIL a tout de même retenu un manquement pour la conservation pendant plusieurs années d'un nombre très important de données d'anciens clients (plus de 3 millions de clients ne s'étant pas connectés à leur compte depuis plus de 5 ans).

Concernant les données des prospects en particulier, la CNIL a constaté que la société n'adressait pas de prospection commerciale à ces personnes si elles ne manifestaient pas d'intérêt pour ses produits ou services durant deux ans. Elle a donc considéré que la conservation des données des prospects n'était pas nécessaire au-delà de ce délai de deux ans.

Point de départ du délai de conservation

Dans sa délibération, la CNIL note que *« les données des prospects permettent à un responsable de traitement d'adresser des messages, par exemple par courrier électronique, à des personnes qui montrent un intérêt pour ses produits ou services* ».

Elle considère à cet égard que « *lorsque le point de départ du délai de conservation des données est le dernier contact émanant du prospect, il doit s'agir d'un évènement permettant de démontrer l'intérêt de la personne pour le message reçu, tel qu'un clic sur un lien hypertexte contenu dans un courriel* ».

Elle précise cependant que « *la seule ouverture d'un courriel ne peut être considérée comme un contact émanant du prospect, dans la mesure où celui-ci peut être ouvert involontairement du fait des modalités de fonctionnement du logiciel de messagerie utilisé ou par erreur*. »

Anonymisation

Après le délai de conservation des données des clients de cinq ans, la société a expliqué qu'elle supprimait certaines données (les nom, prénom et date de naissance) mais en conservait d'autres (adresse électronique et mot de passe) qui sont hachées par un algorithme et transférées au sein d'une autre table.

La CNIL a relevé que si l'algorithme en question, SHA-256, est considéré par l'Agence nationale de sécurité des systèmes d'information (ANSSI) et la CNIL comme garantissant un niveau de sécurité suffisant des données, sa fonction de hachage ne permet pas d'anonymiser des données et donc de justifier leur conservation de manière indéfinie par un responsable de traitement.

Relevant au passage que la société indiquait que l'objectif de la mise en place d'une telle mesure était de permettre à ses clients de se reconnecter à leur compte, alors même que les données étaient censées avoir été supprimées, la CNIL a considéré que les données personnelles des anciens clients devaient être définitivement supprimées à l'issue de l'expiration du délai de conservation de celles-ci en base active ou en base archive, une fois les obligations légales expirées, et ne pouvaient être conservées pour une hypothétique utilisation future.

Manquement à l'obligation d'information des personnes (article 13 du RGPD)

Les articles 12, 13 et 14 du RGPD prévoient les modalités d'information des personnes concernées. Si l'article 12 concerne les conditions de cette information, les articles 13 et 14 énumèrent les aspects devant être couverts par cette information.

Information des clients

Pour la CNIL, l'information fournie dans la politique de confidentialité des données du site web n'était pas conforme. En effet, la société y indiquait que le consentement était la base légale de tous les traitements alors que plusieurs d'entre eux reposaient en réalité sur d'autres bases légales (comme le contrat ou les intérêts légitimes poursuivis par la société).

Information des salariés du service client

La CNIL a considéré l'information sur l'enregistrement des appels téléphoniques passés avec les clients insuffisante. En particulier, les salariés n'étaient pas informés de la finalité poursuivie par le traitement, de la base légale du dispositif, des destinataires des données, de la durée de conservation des données et de leurs droits.

Manquement à l'obligation d'assurer la sécurité des données (article 32 du RGPD)

L'article 32 du RGPD, qui porte sur la sécurité, prévoit que « *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, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins, (…)* ».

Mots de passe d'accès aux comptes clients

Lors du contrôle, la CNIL a constaté que les personnes souhaitant créer un compte utilisateur sur le site web de la société pouvaient créer un mot de passe composé de six caractères comportant une seule catégorie de caractères. Après le contrôle, la société a mis en place une mesure de blocage d'une minute du compte (après 19 tentatives d'accès infructueuses à un compte à partir d'une même adresse IP en moins d'une minute) puis exigé des mots de passe composés d'au moins huit caractères. Pour la société, la longueur et la complexité d'un mot de passe n'étaient pas des critères élémentaires permettant d'apprécier la force de celui-ci.

La CNIL ne partage pas cette opinion : « *pour assurer un niveau de sécurité suffisant et satisfaire aux exigences de robustesse des mots de passe, lorsqu'une authentification repose uniquement sur un identifiant et un mot de passe, le mot de passe doit comporter au minimum douze caractères – contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial – ou le mot de passe doit comporter au moins huit caractères – contenant trois de ces quatre catégories de caractères – et être accompagné d'une*

mesure complémentaire 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.

Elle rejoint l'ANSSI pour qui « *un bon mot de passe est avant tout un mot de passe fort, c'est à dire difficile à retrouver même à l'aide d'outils automatisés. La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant. En effet, un mot de passe constitué de minuscules, de majuscules, de caractères spéciaux et de chiffres est techniquement plus difficile à découvrir qu'un mot de passe constitué uniquement de minuscules* ».

Données bancaires des clients

Dans le cadre de la lutte contre la fraude, la société avait mis en place un dispositif permettant aux clients d'envoyer en clair, par courriel non chiffré à partir de leur boîte électronique, des photographies ou des scans de leur carte bancaire contenant l'intégralité du numéro de la carte bancaire. Ces données étaient conservées, au même titre que les justificatifs demandés dans le cadre de la lutte contre la fraude, pendant six mois, en clair dans la base de données.

La CNIL a considéré que la conservation pendant six mois et en clair des numérisations de la carte bancaire utilisée lors d'une commande ne permet pas de garantir la sécurité des données.

Sanction

Compte tenu du nombre de manquements, la CNIL a prononcé une amende de 250 000 euros et décidé de rendre publique sa sanction.

Elle a notamment pris en considération :

- la gravité des manquements (en lien avec l'enregistrement des conversations téléphoniques et la conservation des données bancaires) ;
- le nombre de personnes concernées, les données de plusieurs milliers de personnes étant conservées au-delà des durées nécessaires (plus de 3 millions d'anciens clients et plus de 25 millions de prospects) ;
- le fait que plusieurs des manquements portent, pour l'essentiel, sur des obligations qui existaient déjà avant l'entrée en application du RGPD.

La société a été enjointe de mettre ses traitements en conformité avec le RGPD et d'en justifier sous un délai de trois mois à compter de la notification de la délibération, sous astreinte de 250 euros par jour de retard.

Soulier Avocats est un cabinet d'avocats pluridisciplinaire proposant aux différents acteurs du monde industriel, économique et financier une offre de services juridiques complète et intégrée.

Nous assistons nos clients français et étrangers sur l'ensemble des questions juridiques et fiscales susceptibles de se poser à eux tant dans le cadre de leurs activités quotidiennes qu'à l'occasion d'opérations exceptionnelles et de décisions stratégiques.

Chacun de nos clients bénéficie d'un service personnalisé adapté à ses besoins, quels que soient sa taille, sa nationalité et son secteur d'activité.

Pour plus d'informations, nous vous invitons à consulter notre site internet : www.soulier-avocats.com.