Site internet et protection des données personnelles : la CNIL sanctionne un site web de vente en ligne SPARTOO

Conseils pratiques publié le **10/08/2020**, vu **684 fois**, Auteur : PROCESCIAL AVOCAT

Les sites internet doivent absolument respecter la réglementation européenne sur la protection des données personnelles (RGPD). A défaut, les sanctions de la CNIL peuvent être sévères.

En plus des règles prévues par le Code de la consommation pour la protection des consommateurs, un site Internet de vente en ligne doit respecter l'ensemble des règles relatives à la protection des données à caractère personnel et notamment les dispositions du Règlement UE n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016, également appelé RGPD.

Il s'agit d'une grave erreur que de croire que les règles relatives à la protection des données personnelles sont de simples incantations. Leur effectivité est garantie par de lourdes sanctions pécuniaires dont une société de vente en ligne vient de faire les frais.

En effet, dans sa Délibération n° SAN-2020-003 du 28 juillet 2020, la formation restreinte de la CNIL a infligé à la société de vente en ligne SPARTOO, une amende administrative d'un montant de 250.000€, pour différents manquements à la réglementation sur la protection des données.

A travers cette décision, la CNIL rappelle quelques principes applicables en la matière qu'il convient d'expliquer brièvement.

Le principe de minimisation des données personnelles

Le premier manquement à la réglementation européenne sur la protection des données personnelles, reproché au site web de vente en ligne, porte sur le principe de minimisation des données.

Le principe de minimisation des données est posé par l'article du RGPD qui prévoit : « *Les données à caractère personnel doivent être : [...] c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données)* ».

Ainsi, sous aucun prétexte, un site internet ne doit collecter des données personnelles qui ne sont pas nécessaires à la finalité du traitement.

En l’espèce, sous prétexte de lutte contre la fraude à la carte bancaire, la société de vente en ligne collectait des données personnelles qui n’étaient pas nécessaires, compte tenu de la finalité du traitement.

La nécessité de limiter la durée de conservation des données personnelles

Le second manquement reproché au site web de vente en ligne a porté sur l’absence de limitation de la durée de conservation des données personnelles collectées.

L’article 5-1 e) du RGPD dispose que les données à caractère personnel doivent être conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées, sauf exception liée « *à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques* ».

Le site internet doit définir une durée de conservation des données personnelles collectées, proportionnelle à la finalité du traitement. Il doit également détruire les données ainsi collectées, à l’issue de la durée de conservation, sauf exception.

Dans sa décision, le Gendarme de la protection des données personnelles a constaté que d'une part, la société de vente en ligne ne déterminait pas de durée de conservation pour certaines données des clients et des prospects et que d'autre part, elle ne procédait à aucun effacement régulier ou archivage des données pour lesquelles une durée de conservation était fixée, à l’issue de ladite durée.

L’obligation de fournir un certain nombre d’informations à la personne concernée par la collecte des données personnelles

Le troisième manquement reproché à SPARTOO est relatif à l’obligation d’informer les personnes auprès de qui les données personnelles sont collectées.

Sur ce point, l’article 13 du RGPD dispose qu’au moment où les données sont obtenues, plusieurs informations doivent être portées à la connaissance de la personne concernée. Parmi ces informations figure l'indication des destinataires des données collectées et de la base sur laquelle le traitement est effectué.

Or, la CNIL a considéré que le site web SPARTOO n’a ni indiqué la bonne base de traitement des données dans sa politique de confidentialité, ni même informé les internautes que leurs données personnelles seraient transférées dans un pays étranger, en l’occurrence un pays hors Union Européenne.

L’obligation de mettre en place des mesures de sécurité adaptées pour assurer la protection des données collectées

Le quatrième manquement est relatif à l’obligation de sécuriser les données personnelles collectées.

La sécurité du traitement des données personnelles est régie par les dispositions de l'article 32 du Règlement européen sur la protection des données. Ce texte prévoit notamment que « *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* ».

Pour respecter la réglementation relative à la protection des données personnelles, il ne suffit pas de collecter légalement des données personnelles. Il faut également les protéger de manière adéquate, compte tenu du niveau de risque encouru.

Dans l'affaire en cause, la CNIL a reproché au site web de permettre la création de comptes utilisateurs avec des mots de passe non sécurisés, composés de 6 caractères comportant une seule catégorie de caractères. De tels mots de passe ne permettent pas d'assurer la sécurité des comptes utilisateurs et des données personnelles qu'ils contiennent.

En outre, le site web demandait à ses clients, dans le cadre de la lutte contre la fraude, de lui transmettre par mail, un scan de la carte bancaire utilisée lors de la commande, alors même qu'aucune mesure appropriée n'était mise en place pour assurer la sécurité de ces données bancaires.

Les lourdes sanctions encourues en cas de manquement à la réglementation sur la protection des données personnelles par le site web de vente en ligne

Au regard de l'ensemble de ces manquements la CNIL a infligé à la société SPARTOO une amende administrative de 250.000€ assortie d'une injonction de mise en conformité dans un délai de 3 mois sous peine d'astreinte de 250€ par jour de retard.

Pour rappel l'article 20 de la Loi Informatique et libertés qui transpose l'article 83 du RGPD, prévoit que la formation restreinte de la CNIL peut, en cas de violation des règles en matière de protection des données personnelles, infliger une amende administrative.

L'amende administrative peut être particulièrement élevée puisqu'elle peut aller jusqu'à 20 millions d'euros pour une personne physique, ou s'agissant d'une entreprise, 4% du chiffre d'affaires annuel mondial total de l'exercice précédent.

Une telle amende administrative est sans préjudice des sanctions pénales prévues par les dispositions des articles 226-16 et suivants du Code pénal (5 ans d'emprisonnement et 300.000€ d'amende).

Autant dire que les propriétaires de sites internet ainsi que les agences de création de sites internet, ont le plus grand intérêt à connaître la réglementation sur la protection des données personnelles ou à s'attacher les services de professionnels qui les maîtrisent (avocats ou Délégués à la Protection des Données).

PROCESCIAL AVOCAT, Avocat en droit du travail ; Avocat en procédure d'appel ; Avocat en contentieux de la création de site internet et créateur de sites web pour avocats ; Avocat défenseur des victimes d'arnaque à la création de sites internet

37 rue des ponts de comines

59000 Lille

Tél : 07 49 07 36 34

Mail : contact@procescial-avocat.fr

Article original publié sur le site web de PROCESCIAL AVOCAT