Données de santé et utilisation des cookies : DOCTISSIMO sanctionné par une amende de 380 000 euros

La CNIL a prononcé une sanction de 380 000 euros à l'encontre de la société DOCTISSIMO pour avoir manqué à des obligations du RGPD, notamment celle de recueillir le consentement des personnes à la collecte et l'utilisation de leurs données de santé, et pour ne pas avoir respecté les règles sur les cookies.

Le contexte

À la suite d'une plainte de l'association PRIVACY INTERNATIONAL, la CNIL a procédé à quatre missions de contrôle auprès de la société DOCTISSIMO. Le site web doctissimo.fr propose principalement des articles, tests, quiz et forums de discussion en lien avec la santé et le bien-être, à destination du grand public.

Lors de ses investigations, la CNIL a relevé plusieurs manquements, notamment concernant les durées de conservation des données, la collecte de données de santé via des tests en ligne, la sécurisation des données ainsi que les modalités de dépôt des cookies sur le terminal des utilisateurs.

En conséquence, la formation restreinte – organe de la CNIL chargé de prononcer des sanctions – a prononcé deux amendes à l'encontre de DOCTISSIMO :

une amende de 280 000 euros au regard des manquements au règlement général sur la protection des données (RGPD). Cette amende a été prise en coopération avec l'ensemble des homologues européens de la CNIL dans le cadre du guichet unique, car le site web a des visiteurs dans tous les États membres de l'Union européenne.

une amende de 100 000 euros concernant le manquement relatif à l'utilisation des cookies (l'article 82 de la loi Informatique et Liberté). Dans ce cas, la CNIL est compétente pour agir seule.

Afin de déterminer le montant de la sanction, la CNIL a pris en compte la nature et la gravité des manquements, les catégories de données personnelles (données de santé) et le nombre de personnes concernées ainsi que la situation financière de la société. Elle a également pris en considération le fait qu'au vu de sa nature et de son secteur d'activité, c'est-à-dire la diffusion de contenus numériques relatifs à la santé, la société aurait dû faire preuve d'une vigilance particulière quant au recueil du consentement des personnes pour collecter leurs données de santé.

Les manquements sanctionnés

La CNIL a retenu quatre manquements au RGPD et un manquement à la loi Informatique et Libertés à l'encontre de la société DOCTISSIMO.

Un manquement à l'obligation de conserver les données pour une durée limitée à l'objectif recherché (article 5.1.e du RGPD)

La société conservait les données relatives aux tests réalisés par les internautes pendant 24 mois, puis 3 mois, à compter de leur réalisation. La CNIL considère que ces durées de conservation sont excessives, car elles ne correspondent pas au strict besoin de la société qui collecte les données des tests afin de permettre à l'utilisateur de prendre connaissance des résultats du tests, de les partager ainsi que de réaliser des statistiques agrégées.

Les données des utilisateurs dont le compte était inactif depuis plus de trois ans étaient aussi conservées sans, par exemple, de procédure d'anonymisation.

Un manquement à l'obligation de recueillir le consentement des personnes pour collecter leurs données de santé (article 9 du RGPD)

DOCTISSIMO ne prévoyait aucun avertissement particulier ni mécanisme de recueil du consentement sur ses tests en ligne, afin de s'assurer que l'utilisateur avait conscience et consentait au traitement de ses données de santé, considérées comme particulièrement sensibles au regard du RGPD.

Selon la société, la collecte des données de santé concernait environ 5 % des tests.

Un manquement à l'obligation d'encadrer par contrat les traitements effectués avec un autre responsable de traitement (article 26 du RGPD)

La société DOCTISSIMO met en œuvre des traitements de données personnelles avec d'autres sociétés, liés notamment à la commercialisation des espaces publicitaires sur le site web. Ces relations de responsabilités conjointes n'étaient pas encadrées par un document formalisé, comme un contrat.

Un tel document doit notamment indiquer la répartition des obligations entre chaque responsable de traitement.

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

La société utilisait jusqu'en octobre 2019 un protocole de communication « http », qui n'est pas sécurisé et exposait alors les données à des risques d'attaques informatiques ou de fuite.

En outre, elle conservait les mots de passe des utilisateurs dans un format insuffisamment

sécurisé, alors qu'ils permettaient d'accéder à l'espace personnel contenant notamment les nom, prénom, date de naissance, adresse électronique et sexe de la personne concernée.

Un manquement aux obligations liées à l'utilisation des cookies (article 82 de la Loi Informatique et Libertés)

La CNIL a constaté le dépôt d'un cookie publicitaire sur le terminal de l'utilisateur sans son consentement et dès son arrivée sur le site, ainsi que le dépôt de deux cookies publicitaires après avoir cliqué sur le bouton « TOUT REFUSER ».

Elle considère que l'absence de recueil du consentement a concerné chaque visiteur du site web, soit des centaines de millions d'internautes.

La société ayant pris des mesures pour se mettre en conformité sur l'ensemble des manquements, la CNIL a procédé à la clôture de la procédure.