Publié le 30 janvier 2018

Soulier Bunch, Cabinet d'avocats d'affaires basé à Paris et Lyon

Lire cet article en ligne

Sécurité des données : sanction de Darty par la CNIL

Par une délibération en date du 8 janvier 2018, la CNIL a prononcé une sanction pécuniaire à l'encontre de DARTY d'un montant de 100 000 euros pour ne pas avoir suffisamment sécurisé les données de clients ayant effectué une demande en ligne de service après-vente.

Avec cette sanction, la CNIL adresse un avertissement aux entreprises qui doivent se mettre en conformité avec le règlement général sur la protection des données (RGPD) qui sera applicable à partir du 25 mai prochain.

Après avoir été informée par l'éditeur d'un site internet spécialisé dans la sécurité des systèmes d'information d'un incident de sécurité en février 2017, la CNIL a réalisé un contrôle en ligne en mars 2017 ce qui lui a permis de constater qu'une défaillance de sécurité permettait d'accéder librement à l'ensemble des demandes et des données renseignées par les clients de la société DARTY, via un formulaire en ligne de demande de service après-vente.

Plusieurs centaines de milliers de demandes ou réclamations contenant des données telles que les nom, prénom, adresse postale, adresse de messagerie électronique ou numéro de téléphone des clients étaient ainsi potentiellement accessibles.

Un contrôle sur place réalisé quinze jours plus tard a révélé que le formulaire de demande de service après-vente, à l'origine du défaut de sécurité, avait été développé par un prestataire externe.

Bien que la société DARTY ait été informée de l'incident de sécurité à l'issue du premier contrôle, la CNIL a constaté que les fiches des clients étaient toujours accessibles entre le premier et le second contrôle et que de nouvelles fiches avaient été créées dans ce laps de temps. Toutefois, le soir même du second contrôle, DARTY indiquait à la CNIL avoir mis en place les mesures de sécurisation nécessaires pour remédier à l'incident.

Au regard de ces éléments, la CNIL a considéré que DARTY avait manqué à son obligation de sécurité prévue par l'article 34 de la loi Informatique et Libertés en ne sécurisant pas suffisamment les données de clients ayant effectué en ligne une demande de service après-vente.

En plus de l'amende de 100 000 euros, elle a décidé de rendre publique sa décision notamment en raison « *du contexte actuel dans lequel se multiplient les incidents de sécurité et de la nécessité de sensibiliser les internautes quant au risque pesant sur la sécurité de leurs données* ».

C'est aussi un moyen d'informer les entreprises de leurs obligations. Et d'illustrer les grands changements apportés par le RGPD.

Sous-traitance

Dans sa décision, la CNIL rappelle que le fait que le formulaire ait été développé par un prestataire sous-traitant ne décharge en rien DARTY, le responsable du traitement des données, de son obligation de sécurité.

Si les obligations de la loi Informatique et Libertés ne s'imposent qu'au responsable de traitement, le RGPD imposera des obligations spécifiques aux sous-traitants.

Ces nouvelles obligations nécessiteront de définir une politique de gestion des sous-traitants et d'adapter les contrats.

Accountability

La CNIL estime que DARTY aurait dû s'assurer préalablement que les règles de paramétrage de l'outil mis en œuvre pour son compte ne permettaient pas à des tiers non autorisés d'accéder aux données des clients, et nous précise que « *la vérification préalable notamment des règles de filtrage des URL fait partie des tests élémentaires qui doivent être réalisés par une société en matière de sécurité des systèmes d'information* ».

Elle estime également que la société aurait dû procéder de façon régulière à la revue des formulaires permettant d'alimenter l'outil de gestion des demandes de service après-vente et souligne « *qu'une bonne pratique en matière de sécurité des systèmes informatiques consisterait à désactiver les fonctionnalités ou modules d'un outil qui ne seraient pas utilisés ou pas nécessaires* ».

Avec le RGPD, la logique déclarative est abandonnée au profit d'une logique de responsabilisation

(accountability) : il appartient aux entreprises de prendre toutes les mesures pour garantir la conformité des traitements de données et d'être en mesure de le démontrer à tout moment.

La CNIL nous donne ainsi des exemples de bonnes pratiques pour être conforme.

Incident de sécurité

La CNIL reproche à DARTY sa mauvaise gestion de la violation de sécurité. Ce n'est qu'après le second contrôle que l'incident a pris fin. Entre les deux, ce sont presque 6 000 fiches clients qui ont été créées, portant à presque 1 million le nombre de fiches accessibles.

Avec le RGDP, tous les organismes seront soumis à une obligation de notification des violations de données personnelles à la CNIL via un téléservice et ce dans les meilleurs délais, et si possible, 72 heures au plus tard après en avoir pris connaissance, et les personnes concernées par une violation de leurs données personnelles devront être informées en cas de risque élevé.

Il devient indispensable de prévoir, en interne pour chaque organisme, un processus propre de gestion des incidents.

Sanctions

Le montant de l'amende infligée à DARTY, 100 000 euros, est loin d'être le montant maximum des amendes que la CNIL peut prononcer.

Si, depuis la loi pour la République numérique du 7 octobre 2016, le plafond maximal des sanctions de la CNIL est passé de 150 000 à 3 millions d'euros, les amendes prévues par le RGDP pourront s'élever, selon la catégorie de l'infraction, à 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, de 2% jusqu'à 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.