SOULIER BUNCH

Publié le 30 août 2018

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

Lire cet article en ligne

Fuite de données : la CNIL impose une nouvelle amende record à Optical Center

250 000 euros. C'est le montant de l'amende qu'a prononcée la CNIL à l'encontre d'Optical Center, une entreprise française spécialisée dans l'optique, pour un défaut de sécurisation de son site internet www.optical-center.fr.

C'est la première fois que la CNIL impose une amende aussi forte. Et ce n'est pas en application du Règlement général sur la protection des données (RGPD) (les faits ayant été constatés avant) qui prévoit des amendes pouvant aller jusqu'à 20 millions d'euros et 4% du chiffre d'affaires.

Le 28 juillet 2017, la CNIL a été informée d'une possible *fuite de données conséquente concernant Optical Center*, le signalement faisant état de données rendues librement accessibles à partir de plusieurs URL ayant une structure identique.

Le 31 juillet 2017, la CNIL a réalisé un contrôle en ligne et constaté qu'il était possible, en renseignant plusieurs URL dans la barre d'adresse d'un navigateur, d'accéder à des centaines de factures de clients de la société. Ces factures contenaient des données telles que les nom, prénom, adresse postale ainsi que des données de santé (correction ophtalmologique) ou encore, dans certains cas, le numéro de sécurité sociale des personnes concernées.

Elle a immédiatement alerté la société qui s'est rapprochée de son prestataire pour qu'il prenne les mesures nécessaires afin de mettre fin à cet incident de sécurité. La correction du défaut de sécurité a été réalisée le 2

août 2017 par l'ajout d'une fonctionnalité.

Le 9 août 2017, la CNIL a ensuite réalisé un contrôle sur place, dans les locaux de la société qui a reconnu que son site internet présentait bien un défaut de sécurité.

En l'espèce, le site www.optical-center.fr n'intégrait pas de fonctionnalité permettant de vérifier qu'un client est bien connecté à son espace personnel (« espace client ») avant de lui afficher ses factures. Il était ainsi relativement simple d'accéder aux documents d'un autre client de la société.

La CNIL a directement engagé une procédure de sanction à l'encontre de la société Optical Center.

Il est intéressant de noter que la société s'est plainte de l'absence de mise en demeure préalable, une « une formalité substantielle » de la procédure selon elle qui concourt au respect des droits de la défense.

La CNIL a balayé cet argument d'un revers de main, la loi prévoyant que lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure, elle peut prononcer sans mise en demeure préalable et après une procédure contradictoire, des sanctions notamment pécuniaires.

Elle a donc prononcé une sanction pécuniaire d'un montant de 250.000 euros, estimant que la société avait manqué à son obligation de sécurité des données personnelles, en méconnaissance de l'article 34 de la loi Informatique et Libertés.

Bien que la société ait été réactive dans la résolution de la faille, la CNIL a considéré :

- que la question de la restriction d'accès aux documents mis à disposition des clients, à partir de leur espace réservé, aurait dû faire l'objet d'une attention particulière de la part de la société. La mise en place d'une telle fonctionnalité constitue selon la CNIL une précaution d'usage essentielle,
- que l'exploitation de la violation de données ne nécessitait aucune compétence technique particulière. La CNIL a rappelé que l'exposition de ressources sans contrôle d'accès préalable est identifiée depuis de nombreuses années comme faisant partie des failles de sécurité devant faire l'objet d'une surveillance particulière et de vérifications dans le cadre d'audits de sécurité,
- que la société ne pouvait pas ignorer les risques liés à un défaut de sécurisation de son site dès lors qu'une sanction de 50 000 euros avait déjà été prononcée en raison d'un défaut de sécurité en 2015.

Elle a également décidé de rendre publique sa décision, compte tenu notamment :

- de la particulière sensibilité des données ayant été rendues librement accessibles,
- du nombre de clients impactés, et
- du volume de documents contenus dans la base de données de la société à la date de l'incident (plus de 334 .000).

Soulier Bunch 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, visitez soulierbunch.com.