Optical Center : 50 000 euros d’amende par la CNIL pour un défaut de sécurité de données clients



Optical Center : 50 000 euros d’amende par la CNIL pour un défaut de sécurité de données clients

La CNIL vient de sanctionner lourdement la chaîne d'optique Optical Center en lui infligeant une amende de 50 000 euros.



Malgré une première mise en demeure, toutes les requêtes de la CNIL n'avaient pas été satisfaites.
Oui, la CNIL (Commission Nationale Informatique et Libertés) peut se fâcher. Même si la majorité des « sanctions » infligées par l'autorité administrative indépendante reste du domaine du symbole ou de la mauvaise publicité quand le rappel à la loi est public, de lourdes amendes peuvent sanctionner les plus rétifs.
Optical Center vient d'en faire l'expérience en se voyant infliger une amende de 50 000 euros.
Suite à une plainte en juillet 2014, la CNIL avait enquêté sur les pratiques au sein de la chaîne de 400 magasins d'optique et un site web servant autant au e-commerce qu'à du back-office interne. Une mise en demeure de se mettre en conformité avec la loi avait suivi cette première inspection, fin 2014. Ce premier niveau de « sanction » est symbolique : il suffit au fautif d'appliquer les instructions reçues. Mais la CNIL a tenu à vérifier plus récemment que ses instructions avaient bien été appliquées. Or ce n'était pas totalement le cas.

Des obligations strictes de sécurité

Les manquements relevaient de la sécurité et de la confidentialité des données clients. Rappelons en effet que la Loi Informatique et Liberté oblige tout responsable de traitement à s'assurer de ces éléments susceptibles d'entraîner des compromissions de données personnelles. Des questions s'étaient posées sur la durée de la conservation des données mais la violation de la Loi n'a pas été jugée constituée sur ce point.
En tout premier lieu, la CNIL avait relevé une absence de chiffrement de la connexion au site, point ensuite corrigé. Mais le principal reproche fait concernait la gestion des mots de passe d'accès au site web par les clients et les collaborateurs du distributeur. En effet, la complexité des mots de passe des clients n'était pas suffisamment contrôlée, point non-corrigé pour les anciens clients. Et les mots de passe des collaborateurs étaient saisis par un administrateur au lieu d'être changé par chacun sans possibilité pour un tiers -même interne- de le connaître. Ce point précis a été corrigé.
Enfin, vue la sensibilité des données (médicales), la CNIL avait exigé la mise en place d'une authentification à deux facteurs et un verrouillage automatique des postes de travail en cas d'inactivité prolongée, ce qui n'avait pas été réalisé dans tout le groupe. Enfin, il a été reproché à Optical Center de ne pas avoir précisé les obligations de sécurité et de confidentialité dans les contrats liant l'entreprise avec un sous-traitant intervenant sur son système d'information.

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Même si remplir un formulaire de déclaration à la CNIL est gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !
Source : http://www.cio-online
.com/actualites/lire-op
tical-center%C2%A0-50-000-euros-d-amende-pour-un-defaut-de-securite-de-donnees-clients-8024.html