COMMENTAIRE

JUILLET 2018

La CNIL confirme sa politique de sanction des manquements aux obligations de sécurité des données à caractère personnel

EN BREF

Le contexte : Avant même que le Règlement général sur la protection des données ("RGPD") n'entre en vigueur le 25 mai, les sanctions appliquées en cas de manquement aux obligations de sécurité des données personnelles ont connu une nette augmentation.

Les faits : La Commission nationale informatique et libertés (CNIL) a prononcé une sanction pécuniaire à l'encontre de l'entreprise d'optique Optical Center pour une faille de sécurité de son site de commerce en ligne.

À venir : Maintenant que le RGPD est entré en vigueur, il est indispensable que les responsables de traitement et les sous-traitants s'assurent qu'ils ont mis en place des politiques et des procédures de sécurité robustes.

Read the English Version >>

Par décision du 7 mai 2018, la Commission Nationale Informatique et Libertés (CNIL) a prononcé une sanction pécuniaire de 250 000 euros à l'encontre du fournisseur d'optique Optical Center pour une atteinte à la sécurité du site de commerce électronique de l'entreprise. Bien que la décision ait été prise avant le 25 mai, date d'entrée en vigueur du Règlement générale sur la protection des données ("RGPD"), cette décision confirme une tendance à l'accroissement des sanctions des manquements aux obligations de sécurité des données à caractère personnel, comme en témoigne déjà cette année la décision de la CNIL contre un distributeur d'appareils électro-ménagers.

Bien que la société ait réagi rapidement pour corriger l'anomalie dès qu'elle en a eu connaissance, la CNIL a considéré que des « mesures de sécurité élémentaires » n'avaient pas été mises en place sur le site Internet et a donc constaté que la société responsable du traitement avait manqué à ses obligations en matière de sécurité concernant les données personnelles de ses clients.

La CNIL avait pu accéder aux documents stockés sur les comptes clients, tels que les factures des clients et l'historique des commandes, sur le site de commerce électronique de l'entreprise. Les documents auxquels la CNIL a pu accéder comprenaient également les informations de santé contenues dans les ordonnances téléchargées par les clients, ainsi que les numéros de sécurité sociale. Le site Web ne contenait pas de système d'authentification lui permettant de restreindre l'accès aux documents à un client spécifique, et les comptes des clients pouvaient être accédés simplement en changeant les URLs.

La CNIL a noté que les communications avec le fournisseur de l'entreprise concernant les nouvelles fonctionnalités du site Web sont restées informelles. Il en résulte que le centre optique, en tant que responsable du traitement, a manqué de visibilité sur les actions, corrections ou recommandations de son fournisseur, y compris en termes de mesures de sécurité.

Sur la base du raisonnement de la CNIL détaillé dans la décision, les mesures minimales de sécurité suivantes auraient dû être appliquées sur le site Web.. :

> La CNIL a constaté que des "mesures de sécurité élémentaires" n'avaient pas été mises

- Mettre en œuvre des fonctions de contrôle d'accès permettant à l'entreprise de vérifier qu'un utilisateur est authentifié avant de lui donner accès à des documents personnels ;
- Effectuer des audits de sécurité sur le site Web, y compris pour tester les fonctions de contrôle d'accès ;
- Formaliser les communications avec les fournisseurs en ce qui concerne le développement du site Web, les corrections et les recommandations, y compris en termes de sécurité ;
- Décrire les procédures de test à appliquer avant de lancer de nouvelles fonctionnalités ou mises à jour, et documenter que les procédures de test ont été suivies dans chaque cas (par exemple, par le biais d'un formulaire d'acceptation formel).

> en place sur le site et a donc considéré que Optical Center n'avait pas respecté ses obligations en matière de sécurité relatives aux données personnelles de ses clients.

En prononçant une sanction sans mise en demeure préalable, la CNIL a utilisé ses nouveaux pouvoirs de sanction prévus par l'article 45 de la loi Informatique et libertés du 7 octobre 2016. La disposition permet des sanctions directes sans mise en demeure préalable lorsque la violation est telle qu'elle n'aurait pas pu être corrigée dans le contexte d'une mise en demeure, comme c'est le cas actuellement dans le cadre du RGPD.

La CNIL a ordonné que la sanction supplémentaire de publicité de la décision soit appliquée, malgré les arguments de l'entreprise selon lesquels la violation de la sécurité n'était pas intentionnelle, que l'entreprise n'en avait tiré aucun avantage, qu'il n'y avait aucune preuve que personne d'autre que les équipes d'enquête de la CNIL avait trouvé la violation et qu'aucun préjudice ne semblait avoir été causé aux personnes concernées.

Avec l'augmentation des sanctions dans le cadre du RGPD, cette décision confirme que les contrôleurs et les sous-traitants doivent vérifier qu'ils ont mis en place des politiques et des procédures de sécurité robustes, y compris en termes de restrictions sur les fournisseurs impliqués dans la mise en place d'outils de traitement des données. Dans le cadre du RGPD, les sanctions pour les manquements aux obligations de sécurité survenant depuis le 25 mai sont fixées à un maximum égale à 10 millions d'euros ou, si cette somme est plus élevée, à 2% du chiffre d'affaires annuel mondial de l'entreprise pour l'année précédente.

À RETENIR

Compte tenu des tendances actuelles et du renforcement récent de la réglementation avec l'entrée en vigueur du RGPD, les entreprises doivent s'assurer qu'elles disposent de politiques et de procédures solides pour protéger les données personnelles, et notamment celles des consommateurs. Les manquements aux obligations en matière de sécurité seront sanctionnés par des sanctions financières significatives.


Olivier Haas
Paris


Undine von Diemar
Munich


Daniel J. McLoon
Los Angeles


Mauricio F. Paez
New York

cabinet Jones Day. Tant l'envoi que la réception de cette publication ne saurait créer de relations entre le cabinet Jones Day et le destinataire de ladite publication.