25 Mai 2015

A la une

Département Protection des données personnelles - vie privée

FAILLE DE SECURITE SUR UN SITE INTERNET : UNE SOCIETE SANCTIONNEE

La CNIL a prononcé un avertissement public à l'encontre d'une société française pour défaut de sécurité de ses données.

En juillet 2015, la CNIL a réalisé un contrôle à distance du site internet d'une société dédié à un programme de fidélité et à l'achat d'objets promotionnels de la marque.

Lors du contrôle, la CNIL a mis en évidence l'insuffisance des mesures de sécurité du site internet. En effet, la CNIL a pu librement accéder à certaines données personnelles de clients de la société (prénom, nom, adresse postale, email, numéro de téléphone, etc).

Après avoir été informée de cette faille de sécurité par la CNIL, la société a répondu que des mesures correctives avaient été mises en œuvre par son hébergeur.

Pourtant, après un second contrôle, la CNIL a constaté qu'en saisissent les URL d'accès direct aux fichiers litigieux, les données personnelles des clients de la société étaient toujours accessibles.

La CNIL a donc prononcé un avertissement public à l'encontre de la société.

Les points clés de la décision :

- Le site internet de la société n'était pas suffisamment sécurisé, entrainant la possibilité d'accéder à des données personnelles de clients (prénom, nom, adresse, numéro de téléphone, etc) ;
- La société avait contacté son hébergeur qui avait apparemment mis en œuvre les mesures nécessaires à la résolution du problème ;
- La CNIL a prononcé un avertissement public[1] pour sanctionner la violation des articles 34 et 35 de la loi Informatique et libertés (ces articles sont dédiés aux mesures de sécurité).

Que doit-on retenir de cette sanction ?

- L'article 35 de la loi Informatique et libertés prévoit que le responsable du traitement demeure responsable en cas de violation de l'obligation de sécurité ;
- Le responsable du traitement voit toujours sa responsabilité engagée en cas de manquement à son obligation de mettre en œuvre des mesures de sécurité suffisantes, même si (i) un sous-traitant est chargé de ces services et/ou (ii) il existe un contrat avec le sous-traitant encadrant ces prestations ;
- Le fait que la faille de sécurité n'ait engendré aucun dommage/préjudice pour les personnes concernées (ici, les clients de la société) n'a aucun impact ni conséquence sur l'existence du manquement ;
- Le responsable du traitement doit toujours vérifier que les actions correctives demandées ont été correctement mises en œuvre par le sous-traitant ;
- Les stipulations relatives aux mesures de sécurité insérées dans le contrat et éventuellement dans le contrat de transfert des données (ex : clauses contractuelles type) doivent être claires et devraient permettre au responsable du traitement d'agir en responsabilité à l'encontre de son sous-traitant si nécessaire et obtenir une indemnisation ;
- Cette décision s'inscrit en droite ligne de la sanction prononcée à l'encontre d'un opérateur de télécommunications français en 2014 (confirmée par le Conseil d'Etat en février 2016) ;
- Ces questions doivent être considérées avec beaucoup d'attention, notamment au regard des nouvelles dispositions du projet de loi pour une République numérique, qui vont sensiblement augmenter les pouvoirs de sanction de la CNIL (1.5 millions d'Euros) et permettront notamment à la CNIL de contraindre les responsables de traitement d'informer chaque personne concernée en cas de violation de la loi.

[1] L'intégralité de la décision est disponible à l'adresse suivante : https://www.cnil.fr/sites/default/files/atoms/files/deliberation-formation-restreinte-avertissment-public-ricard_ananonymisee.pdf

P.D.G.B Société d'Avocats

Hélène LEBON - Sandra TUBERT
Olivia RUIZ JOFFRE