RGPD : Mariott paie (très) cher le manque de protection de ses données client

Quel est le coût d'une défaillance de l'application du RGPD ? Dans le cas de Mariott International, la réponse est une amende de 18,4 millions de livres, soit près de 20 millions €, infligée par la Cnil britannique (Information Commissioner's Office – ICO).

> *We have fined Marriott International Inc £18.4million for failing to keep customers' personal data secure. Marriott estimated that 339 million guest records worldwide were affected.*
>
> *Read more about the fine: https://t.co/S99ixGrLU7 pic.twitter.com/b2br06QfVh*
>
> *— ICO (@ICOnews) October 30, 2020*

La chaîne hôtelière américaine peut se féliciter d'avoir échappé à une sanction plus sévère puisque l'ICO avait préconisé, en juillet 2019, un montant de 99 millions £ (plus de 110 millions €) pour la violation de données affectant des centaines de millions de personnes.

« Lorsqu'une entreprise ne prend pas en charge les données de ses clients, l'impact n'est pas seulement une amende possible, ce qui compte le plus, c'est le public dont elle avait le devoir de protéger les données.» estime Elizabeth Denham, responsable de l'ICO.

Non respect des règles du RGPD

L'enquête menée par le régulateur britannique conclut que Marriott n'avait pas mis en place des mesures techniques ou organisationnelles appropriées pour protéger les données personnelles traitées sur ses systèmes, comme l'exige le règlement général sur la protection des données (RGPD).

La violation de données avait eu lieu lorsque les systèmes du groupe hôtelier Starwood avaient été compromis en 2014 . Marriott a acquis Starwood en 2016, mais l'exposition d'informations des clients n'a été découverte qu'en 2018.

Ce piratage a affecté les données personnelles et les données de cartes de paiement de 340 millions de personnes depuis 2014. » Les données personnelles impliquées différaient selon les individus, mais pouvaient inclure des noms, des adresses e-mail, des numéros de téléphone, des numéros de passeport non cryptés, des informations d'arrivée / départ, le statut VIP des clients et le numéro d'adhésion au programme de fidélité. » explique l'ICO.

Et de donner des détails sur l'attaque : « En 2014, un attaquant inconnu a installé un morceau de code connu sous le nom de « shell web » sur un appareil du système Starwood, leur donnant la possibilité d'accéder et de modifier le contenu de cet appareil à distance. Cet accès a été exploité afin d'installer des logiciels malveillants, permettant à l'attaquant d'avoir un accès à distance au

système en tant qu'utilisateur privilégié. En conséquence, l'attaquant aurait eu un accès illimité à l'appareil concerné et aux autres appareils du réseau auxquels ce compte aurait eu accès.
D'autres outils ont été installés par l'attaquant pour collecter les informations de connexion d'utilisateurs supplémentaires au sein du réseau Starwood. Avec ces informations d'identification, l'attaquant a accédé et exporté la base de données stockant les données de réservation pour les clients Starwood.»

Le régulateur précise avoir tenu compte, en infligeant son amende, des mesures prises par Marriott pour atténuer les effets de l'incident ainsi que de l'impact économique de la pandémie sur les activités du groupe.

Cette sanction intervient deux semaines après l'amende record de 20 millions £ prononcée par l'ICO contre la compagnie aérienne British Airways à propos du piratage d'informations personnelles de ses passagers en 2018.