Cybersécurité : l'autorité britannique de protection des données, en coopération avec la CNIL, inflige deux amendes record

02 novembre 2020

Ces deux sanctions record rappellent le rôle du RGPD dans le domaine de la cybersécurité et illustrent une coopération fructueuse entre autorités de protection européennes, au service des citoyens.

Deux amendes record suite à des violations de données

L'ICO, autorité britannique de protection des données, a récemment infligé les amendes les plus importantes imposées en matière de sécurité au titre du règlement général sur la protection des données (RGPD).

Ces amendes, de 20 millions de livres sterling (environ 22 millions d'euros) pour British Airways et 18,4 millions de livres sterling (environ 20 millions d'euros) pour Marriott, font suite à des violations de données ayant rendu accessibles à des tiers de très nombreuses données personnelles.

Dans le cas de British Airways, les données d'environ 430 000 personnes, dont les noms, prénoms, adresses et, pour plus de 200 000 d'entre elles, leurs données bancaires (numéros de CB et codes CVV) ont été rendues accessibles.

Concernant le groupe hôtelier Marriott, 339 millions de comptes clients ont été concernés dont 30 millions de comptes européens contenant les noms, prénoms, emails et numéros de passeport.

Dans les deux cas, il s'agit de sociétés traitant de très nombreuses données personnelles et qui disposent des moyens financiers et d'un personnel fortement qualifié pour assurer un haut niveau de sécurité. Si les attaques concernées se sont révélées sophistiquées et menées sur une durée étendue, il n'en reste pas moins que de fortes exigences pèsent sur de tels organismes.

L'impérieuse nécessité de mettre en place des mesures de sécurité adaptées au service de la protection des données

Le RGPD a fait de la sécurité des données un principe général à respecter et créé de nouvelles obligations en la matière. Les manquements peuvent être sanctionnés jusqu'à 10 millions d'euros d'amende ou 2 % du chiffre d'affaires mondial.

Ces décisions rappellent que la sécurité des données nécessite une vigilance permanente, tout particulièrement pour de tels opérateurs, avec de lourdes conséquences en cas d'infractions.

Une précédente décision de l'autorité de protection allemande sur le fondement de l'obligation de sécurité avait déjà conduit à une amende de près de 10 millions d'euros à l'encontre d'un opérateur télécom. Au-delà de l'amende, de telles sanctions conduisent généralement à d'importants investissements visant à prévenir la répétition des violations de données personnelles et à renforcer la sécurité des organismes.

Ces différentes affaires positionnent clairement le RGPD et les autorités de protection des données comme des acteurs efficaces et à part entière de la cybersécurité, invitant les organismes à une bonne gestion de leur patrimoine informationnel.

Une coopération exemplaire entre les autorités de protection des données européennes

En application du mécanisme de coopération prévu par le RGPD, le « guichet unique », les projets de décisions ont été adressés aux autorités européennes de protection des données et ont été minutieusement examinés par la CNIL.

La formation restreinte de la CNIL s'est ainsi prononcée sur les suites à donner. Après des échanges fructueux avec l'ICO, son homologue britannique, la CNIL a approuvé les projets tant s'agissant des manquements retenus que des montants des amendes proposées. Elle a notamment estimé que ces montants substantiels et les plus élevés à ce jour en matière de sécurité étaient proportionnés au regard de la gravité des manquements constatés.

Le « guichet unique » permet ainsi d'aboutir à des décisions majeures à l'égard des traitements mis en œuvre à l'échelle européenne, en mettant en œuvre les mécanismes prévus dans le RGPD. La CNIL continuera à promouvoir et à prendre toute sa part dans la coopération européenne.

Texte reference

La décision de l'autorité britannique de protection des données

> ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure (en anglais)

Texte reference

Pour approfondir

> Cybersécurité
> Les violations de données personnelles
> Le guichet unique

Haut de page