British Airways condamnée à une amende de £20’000’000.- pour violation de la sécurité des données

Célian Hirsch, le 27 octobre 2020

British Airways écope d’une amende de £ 20’000’000.- en raison de la violation de l’intégrité et la confidentialité des données traitées, ainsi qu’en raison de l’absence de mesures techniques et organisationnelles appropriées, ce qui a conduit à une violation de la sécurité des données (*data breach*).

Information Commissioner’s Office, Penalty Notice COM08783542 du 16octobre 2020 contre British Airways plc

Le 6 septembre 2018, British Airways a annoncé au *Information Commissioner’s Office* (ICO), l’autorité britannique de protection des données, avoir été victime d’une violation de données *(data breach* ; art. 4 ch. 12 RGPD). En effet, entre le 22 juin et le 5 septembre 2018, des hackers ont eu accès aux données de British Airways, notamment des numéros de cartes de crédit, dont le numéro CVV, d’environ 321’000 clients.

Le 16 octobre 2020, l’ICO a rendu sa décision condamnant British Airways à une amende de £20’000’000.-. En résumé, elle lui reproche de ne pas avoir protégé l’intégrité et la confidentialité des données (art. 5 par. 1 let. f RGPD), ainsi que de ne pas avoir mis en place « les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque » au sens de l’art. 32 RGPD. Le montant de l’amende a néanmoins été réduit drastiquement (l’ICO avait mentionné en 2019 le chiffre de £ 183’390’000.-), notamment en raison de la crise du coronavirus et de ses conséquences pour la compagnie aérienne.

La décision de l’ICO nous donne quelques indications sur le déroulement du *hacking*, même si de nombreux passages sont logiquement caviardés.

On retiendra notamment que l’origine de l’attaque provient du fait que les hackers ont tout d’abord réussi à se procurer les identifiants (nom d’utilisateur et mot de passe) d’un employé d’une société tierce (Swissport). Or ce compte n’était pas protégé par une authentification forte. Première erreur… En effet, les hackers cherchent logiquement des portes d’entrée les plus vulnérables (« *supply chain attack* »). L’accès au compte de l’employé de Swissport leur

a permis en l'espèce d'accéder au réseau interne de British Airways.

L'entreprise d'aviation s'est défendue en produisant son contrat avec Swissport, lequel prévoyait des informations sur la sécurité des mots de passe. Néanmoins, selon l'ICO, un simple accord imposant des mesures à la société tierce n'était pas suffisant. En outre, British Airways prévoyait dans ses propres directives internes l'utilisation de l'authentification forte. Elle aurait ainsi également dû la prévoir pour les sociétés tierces.

Grâce à l'accès de l'employé, les hackers ont ensuite réussi à casser des portes de sécurité, afin d'avoir accès à des systèmes qui n'étaient en principe pas accessibles aux employés externes. Bien que les détails de cette partie de l'attaque soient caviardés, on retiendra que les hackers ont finalement réussi à rediriger les utilisateurs du site Internet de British Airways sur BAways.com pendant plusieurs jours. Les hackers recevaient ainsi les informations des cartes de crédit des utilisateurs. Ces derniers ne se doutaient de rien puisque leurs informations étaient également transmises à British Airway. Leurs réservations de vols avaient ainsi effectivement lieu.

Outre le reproche de l'absence de l'authentification forte pour les employés de sociétés tierces, l'ICO souligne que British Airways n'aurait pas dû garder les numéros CVV des cartes de crédit. De plus, la majorité de ces numéros n'était pas cryptée. Or, au moins avec l'entrée en vigueur du RGPD le 25 mai 2018, British Airways aurait dû procéder à des vérifications internes, afin de s'assurer que son système protégeait correctement les données personnelles et qu'il respectait le principe de minimisation des données (*data minimisation* ; art. 5 par. 1 let. c RGPD).

British Airways a tenté de se défendre en soulignant que les hackers avaient utilisé des méthodes particulièrement sophistiquées. L'ICO lui répond que non seulement de telles attaques sont courantes contre des grandes entreprises, mais que l'attaque n'atteignait en l'espèce pas un tel degré de complexité qu'elle permettrait à British Airways d'exclure toute responsabilité. Au contraire, pour chacune des étapes de l'attaque, British Airways aurait pu et dû mettre en place des mesures de sécurité qui auraient permis d'éviter ce *data breach*.

Dans la dernière partie de sa décision, l'ICO explique de manière circonstanciée les éléments factuels pertinents pour déterminer le montant de l'amende administrative en application de l'art. 83 RGPD. Elle souligne notamment que la violation de donnée concerne un nombre important de données personnelles, dont des données financières.

S'il faut retenir une seule chose de cette décision, c'est à notre avis l'importance de mettre

en place une authentification forte. La mise en œuvre d'une telle mesure est d'ailleurs obligatoire pour les prestataires de service de paiement au sein de l'Union européenne (art. 97 DPS2), bien que sa mise en œuvre fasse pour l'instant l'objet d'une certaine souplesse.

Proposition de citation : Célian HIRSCH, British Airways condamnée à une amende de £20'000'000.- pour violation de la sécurité des données, 27 octobre 2020 *in* www.swissprivacy.law/19