RGPD

Violation de données par un ancien employé

Comme chaque mois, Alexandre Fievée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en s'appuyant sur les décisions rendues par les autorités nationales de contrôle au niveau européen. Ce mois-ci, il se penche sur une décision de l'UODO, autorité de protection des données polonaise, qui a condamné une banque à une amende administrative pour ne pas avoir notifié une violation de données, caractérisée par plusieurs accès non autorisés par un ancien employé à sa plateforme de services électroniques.

Une violation de données, en application de l'article 4.12) du RGPD est « *une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données* ». Il s'agit, précise la Cnil, de « *tout incident de sécurité, d'origine malveillante ou non, (...) se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles* »[1]. Ainsi, et à titre d'exemple, le CEPD considère comme une violation de données la copie par un salarié des données commerciales du fichier clients de l'entreprise et leur réutilisation après avoir quitté son emploi, afin de contacter lesdits clients pour les attirer dans sa nouvelle activité[2].

En cas de violation de données, l'article 33 du RGPD impose au responsable du traitement de documenter, dans un registre, ladite violation et de la notifier à l'autorité de contrôle dès lors qu'elle présente un risque pour les droits et libertés des personnes. Si ce risque est considéré comme élevé, une communication doit être, par ailleurs, adressée aux personnes concernées.

L'affaire[3]

Après la cessation de son emploi, un ancien employé de la Santander Bank Polska SA, qui n'avait pas été privé de l'accès à la plateforme de services électroniques de ladite banque, a continué à s'y connecter, consultant ainsi toute une série de données personnelles concernant les salariés de la banque. Parmi ces données figuraient le nom, le prénom, le numéro PESEL, l'adresse de résidence (ou de séjour) et des données de santé, telles que des informations relatives aux arrêts de travail. Considérant qu'il ne s'agissait pas d'une violation de données au sens de l'article 4 du RGPD, la Santander Bank Polska SA n'a procédé à aucune notification. Selon l'organisme bancaire, il n'y avait pas violation de données dans la mesure où aucun « *traitement illicite* » n'avait été constaté. Et même à considérer qu'il y ait eu une violation de données, la notification à l'autorité de contrôle ne s'imposait pas car l'incident en question ne présentait pas un risque pour les droits et libertés des personnes. Plusieurs motifs étaient invoqués par la banque pour justifier une telle analyse : (i) les accès non autorisés avaient été réalisés par une personne « *de confiance* », qui, avant la cessation de son emploi, occupait un poste au titre duquel elle était autorisée à traiter des données personnelles pour le compte de la banque et connaissait donc la politique de protection des données en vigueur dans l'organisation ; (ii) l'incident avait été signalé à l'entreprise par cette personne, ce qui excluait tout risque d'utilisation illicite des données par cette dernière (« *Il ne peut être considéré qu'un ancien employé, en signalant lui-même l'irrégularité, puisse utiliser un accès illicite aux données des employés de la banque. Le contraire serait contraire aux principes de l'expérience de vie et aux principes de la logique.* »)

Cette argumentation n'a pas emporté la conviction de l'autorité polonaise de protection des données, qui a considéré que l'accès non autorisé à la plateforme de services électroniques devait s'analyser comme une « *violation de la confidentialité* » présentant « *un risque élevé* » pour les droits et libertés des personnes concernées. A cet égard, elle précise que, dans l'appréciation de la violation de données, il importe peu que la personne non autorisée ait pris connaissance ou non des données personnelles stockées sur la plateforme. Le simple fait que le risque existe suffit à caractériser la violation de données. La banque a ainsi été sanctionnée pour ne pas avoir notifié la violation de données à l'autorité de contrôle et aux personnes concernées, en l'occurrence les employés dont les données personnelles étaient accessibles depuis la plateforme.

Quelles recommandations ?

Dans ce genre de situation, l'entreprise doit prendre les mesures nécessaires pour neutraliser le risque, en coupant les accès litigieux. Afin d'atténuer les effets négatifs de la violation, une action en justice immédiate doit être mise en œuvre pour empêcher une utilisation inappropriée des données par la personne à l'origine de la violation. Dans un second temps, il convient de prendre les mesures qui s'imposent pour éviter qu'une telle situation ne se reproduise. Une meilleure gestion des droits d'accès/habilitation au moment du départ d'un salarié semble être une mesure de bon sens.

Alexandre FIEVÉE
Avocat associé
Derriennic Associés

Notes

(1) https://www.cnil.fr/fr/les-violations-de-donnees-personnelles

(2) CEPD, Lignes directrices 01/2021 sur les exemples de notification des violations de données personnelles, 14 décembre 2021.

(3) UODO, décision DKN.5131.33.2021, 19 janvier 2022.