RGPD

L'envoi d'un courriel à un destinataire erroné doit-il être notifié ?

Comme chaque mois, Alexandre Fiévée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en nous appuyant sur les décisions rendues par les autorités nationales de contrôle au niveau européen. Ce mois-ci, il se penche sur une décision de la CNPD, autorité de contrôle luxembourgeoise, relative à l'envoi par un assureur d'un courriel contenant des données de santé d'un assuré à un mauvais destinataire qui s'analyse comme une violation de données justifiant une notification à l'autorité de contrôle ainsi qu'une communication à la personne concernée.

« *Tous les organismes qui traitent des données personnelles doivent, rappelle la Cnil, mettre en place des mesures pour prévenir les violations de données et réagir de manière appropriée en cas d'incident. Les obligations prévues par le RGPD visent à éviter qu'une violation cause des dommages ou des préjudices aux organismes comme aux personnes concernées.* »[1] La violation de données personnelles est définie à l'article 4.12) du RGPD comme « *une violation de la sécurité entraînante, 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 y a donc une violation de données si un incident de sécurité impliquant un traitement de données personnelles se produit et que cet incident a un impact sur l'intégrité, la confidentialité et/ou la disponibilité des données, et ce peu importe que l'incident soit d'origine malveillante ou non et qu'il se soit produit de manière intentionnelle ou non.

Rappel du principe

En cas de violation de données, l'article 33 du RGPD impose au responsable du traitement de documenter, dans un registre, les violations de données personnelles et de notifier les violations présentant un risque pour les droits et libertés des personnes à l'autorité de contrôle et, dans certains cas, lorsque le risque est élevé, aux personnes concernées. La notification à la Cnil doit intervenir dans les meilleurs délais et au plus tard 72h après que le responsable du traitement en a pris connaissance. En pratique, le point de départ de ce délai correspond au moment où le responsable du traitement a acquis « *un degré de certitude raisonnable* » qu'un incident a eu lieu et a touché des données personnelles. « *Cela implique, précise la Cnil, qu'il ait mis en place des mesures de détection des violations et qu'il mène au plus tôt des investigations permettant d'atteindre une telle certitude raisonnable. Durant cette phase d'investigation, le responsable du traitement n'est pas considéré comme ayant connaissance de la violation.* »[2]

L'affaire

Un assuré a été informé par son assureur qu'un courriel qui lui était destiné a été adressé par erreur à un mauvais destinataire.

Ce courriel comprenait, dans le corps du texte, notamment son nom de famille, son sexe, ainsi que des indications détaillées concernant certaines pathologies, et, en pièces jointes, trois formulaires distincts relatifs aux pathologies qu'il avait déclarées auprès de son assurance. L'assuré a saisi la CNPD d'une réclamation, étant précisé que cette erreur s'est répétée une seconde fois.

Dans ce contexte, l'autorité de contrôle luxembourgeoise a décidé d'ouvrir une enquête, qui s'est traduite par un contrôle sur place dans les locaux de l'assureur.

La question qui se posait était de savoir si l'incident en question devait s'analyser comme une violation de données et, dans l'affirmative, si l'assureur aurait dû notifier la violation à la CNPD et informer le ou les personne(s) concernée(s). Selon l'assureur, les obligations du RGPD ne s'appliquaient pas au cas d'espèce, dans la mesure où les données transmises par les deux courriers électroniques litigieux ne permettaient pas d'identifier le réclamant.

La CNPD n'a pas suivi cette analyse et a considéré que : « *l'envoi de courriers électroniques contenant des données à caractère personnel à un destinataire erroné est dès lors à qualifier de violation de données à caractère personnel du type "violation de la confidentialité", cette dernière ayant entraîné, de manière accidentelle, une divulgation de données à caractère personnel à des personnes tierces qui n'étaient pas autorisées à prendre connaissance des informations contenues dans les courriers électroniques et leurs annexes.* »[3]

Au vu de ce qui précède et considérant que cette violation présentait un risque élevé pour les droits et libertés, la CNPD a estimé que le responsable du traitement a manqué à ses obligations (i) en ne documentant pas la violation dans son registre, (ii) en ne notifiant pas ladite violation à l'autorité de contrôle et en ne communiquant pas à la personne concernée les informations requises de l'article 34.1 du RGPD.

Enfin, la CNPD a retenu à l'encontre de l'assureur un manquement à l'obligation de sécurité, car, selon elle, « *un chiffrement par encryptage, des mots de passe ou toute technique garantissant une protection similaire selon l'état de l'art actuel et les bonnes pratiques applicables en la matière, auraient dû être appliquées aux communications en l'espèce afin de garantir un niveau de sécurité adapté aux risques d'atteinte à la vie privée de la personne concernée, surtout pour une entreprise comme celle du contrôlé* ». Partant, l'autorité de contrôle luxembourgeoise a prononcé une amende d'un montant de 135.000 euros.

Quelles recommandations ?

Chaque incident doit être documenté dans un registre, dans lequel une analyse technique et juridique doit indiquer si l'incident a un impact sur des données personnelles en termes d'intégrité, de confidentialité et/ou de disponibilité.

Dans l'affirmative, il appartient au responsable du traitement d'évaluer le risque pour les droits et libertés des personnes concernées. Cette évaluation peut reposer sur deux critères : la facilité d'identification des personnes concernées par la violation et le caractère préjudiciable de la violation pour ces personnes, étant précisé que chacun de ces critères doit être apprécié selon des valeurs : risque maximal (4), important (3), limité (2), négligeable (1).

Selon les résultats de cette évaluation, une notification s'impose si un risque important a été identifié (ex. : la valeur totale des deux critères est égale à 6) ; une communication aux personnes concernées se justifie par ailleurs si un risque maximal a été identifié (ex. : la valeur totale des deux critères est supérieure à 6).

Alexandre FIEVEE

Avocat associé
Derriennic associés

Notes

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

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

(3) Délibération n° 31FR/2021, 5 août 2021.

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info