Divulgation d'adresses électroniques : l'association HIV Scotland et la nécessité de sécuriser les courriels de masse

Pauline Meyer, le 17 novembre 2021

Dans une décision prononcée le 18 octobre 2021, l'*Information Commissioner's Office* anglais (ICO) a sanctionné l'association HIV Scotland pour ne pas avoir pris les mesures de sécurité adéquates (32 par. 1 et 2 RGPD) et violé le principe de la sécurité des données (art. 5 par. 1 let. f RGPD). Ses manquements ont eu pour conséquence la divulgation d'adresses électroniques d'individus dont on pouvait raisonnablement déduire qu'ils étaient séropositifs ou à risque de contracter le virus.

Information Commissioner's Office, Monetary Penalty Notice du 18 octobre 2021 contre HIV Scotland

HIV Scotland est une association caritative fournissant un soutien aux personnes séropositives, à risque de contracter le virus HIV ou soutenant ces groupes. En juin 2019, l'association a décidé de se doter d'un compte MailChimp, plateforme conçue et développée pour les entreprises utilisant les courriels pour atteindre leurs marchés cibles, afin de sécuriser l'envoi de ses messages groupés. Elle a progressivement migré ses listes de contacts sur cette plateforme d'envoi de masse, sous réserve de celle de son *HIV Scotland's Community Advisory Network* (CAN), qui n'a pas été transférée. Ce réseau regroupe des défenseurs de personnes séropositives qui soutiennent et informent sur le travail de l'organisation ; ils reçoivent des mises à jour, principalement à l'occasion de leurs réunions trimestrielles.

Le 3 février 2020, HIV Scotland a envoyé, par le biais de Microsoft Outlook, un courriel à 105 participants individuels du CAN pour un évènement. Au lieu de correspondre par copie cachée ou copie carbone invisible (« Cci »), l'association a utilisé la fonctionnalité copie carbone (« Cc »), dévoilant ainsi les adresses électroniques de tous les destinataires. L'organisation a tenté de rappeler les courriels, mais a reçu des réponses l'alertant de l'incident.

Les adresses électroniques divulguées constituent des données à caractère personnel au sens de l'art. 4 ch. 1 RGPD et leur divulgation consiste en une violation de données à caractère sexuel (art. 4 ch. 12 RGPD). D'une part, 65 adresses contenaient les noms et prénoms des destinataires. Dans la mesure où leur participation au sein d'une organisation soutenant les personnes séropositives est combinée avec le contenu du courriel et l'ordre du jour, des

données sensibles pouvaient être déduites, plus précisément des données concernant la santé (art. 4 ch. 15 RGPD). D'autre part, même les adresses ne contenant ni nom ni prénom pouvaient être utilisées pour identifier des individus, en les combinant avec d'autres informations issues notamment de recherches internet. L'association aurait dû envoyer ses courriels en « Cci ».

Elle a par la suite contacté l'ICO et a notifié la violation de données à caractère personnel (art. 33 RGPD) quelques heures après ledit incident. Elle a également envoyé un courriel d'excuses à l'ensemble des destinataires, les a contactés pour présenter des excuses et demander la suppression des courriels, a effectué un communiqué sur son site internet et s'est tenue à disposition des personnes concernées en cas de dommage. Elle a finalement achevé la migration de ses listes de contacts et bases de données sur MailChimp courant février 2020.

L'ICO a estimé que, bien que l'association eût pris des mesures, ces dernières n'étaient pas suffisantes, raison pour laquelle une violation de la confidentialité des données s'est produite.

Tout d'abord, l'ICO reconnaît que HIV Scotland disposait d'une politique de confidentialité publique dont ses collaborateurs devaient prendre connaissance. Cependant, le renvoi des collaborateurs à cette politique de confidentialité externe ne suffisait pas pour fournir les informations appropriées pour le personnel traitant des données personnelles, en lien notamment avec la sécurité des données ; il aurait fallu disposer d'une politique spécifique sur le traitement sécurisé des données personnelles au sein de l'association.

Ensuite, il est vrai que l'association disposait également d'une formation contenant un module sur le RGPD et sensibilisait ses collaborateurs à l'exigence de l'utilisation du « cci » pour les courriels groupés. Néanmoins, la formation dispensée sur la protection des données en question devait être complétée par les collaborateurs sur une base annuelle, ce qui n'est pas suffisant pour l'ICO qui estime qu'une formation sur la protection des données personnelles devrait être effectuée avant l'accès d'un collaborateur à des données personnelles, surtout sensibles, et au plus tard un mois après son entrée en fonction.

Finalement, l'association, qui avait décidé de se créer un compte MailChimp en juin 2019, avait migré la majeure partie de ses bases de données et de ses listes de contact vers la plateforme en vue d'envoyer des courriels sécurisés sur toutes ses listes de diffusion. Bien que la plateforme ait été acquise en juillet 2019, l'enquête de l'autorité anglaise a démontré que la migration n'avait toujours pas été mise en œuvre de manière adéquate pour la liste CAN au moment de l'incident, soit début février 2020. Selon ses dires, l'association avait

souhaité attendre l'évènement de février 2020 pour procéder à cette migration, craignant que la communication du 3 février 2020 termine, à cause de perturbations, dans les dossiers indésirables des destinataires. Pour l'ICO, la situation ne semble pas convaincante et une mise en œuvre complète et correcte de MailChimp plus tôt aurait empêché la divulgation de données personnelles.

Pour ces motifs, l'ICO a conclu que HIV Scotland avait enfreint l'art. 5 par. 1 let. f RGPD en envoyant un courriel groupé plutôt que distinct à chaque destinataire, en n'ayant pas effectué une migration complète sur MailChimp et en n'utilisant pas la fonction « Cci » dans son courrier électronique. L'autorité a également conclu à une violation de l'art. 32 par. 1 et 2 RGPD, dans la mesure où l'association n'avait pas pris les mesures adéquates compte tenu du risque induit par ses traitements de données à caractère personnel.

L'amende prononcée par l'ICO en vertu des art. 58 par. 2 et 83 RGPD est de £10'000. Elle a été calculée compte tenu des circonstances du cas d'espèce et d'éléments atténuants comme aggravants. L'ICO a soulevé le fait qu'il s'était déjà prononcé pour des cas similaires et que l'association le savait (cette dernière avait par ailleurs précédemment émis une critique sur un autre responsable du traitement sanctionné dans une situation similaire). De plus, HIV Scotland devait être au courant de ses propres manquements en termes de sécurité. En outre, des conséquences négatives ont résulté de la violation du 3 février 2020, dès lors qu'il était possible de savoir que l'un des destinataires était séropositif ou qu'il soutenait quelqu'un qui l'était. Une plainte formelle avait par ailleurs été déposée par un destinataire, qui relevait la divulgation de sa séropositivité à des étrangers, le privant ainsi du choix de le dire ou non à son entourage ; un sentiment de détresse en avait découlé. L'ICO a également pris en considération des éléments tels que le fait que la violation avait été commise par négligence ou encore que HIV Scotland n'avait *a priori* pas commis d'infractions antérieures. La sanction a été atténuée, dès lors que des mesures, certes insuffisantes, avaient été prises préalablement à l'incident, et que, par la suite, l'association avait tenté de remédier à la violation et implémenté correctement MailChimp.

En Suisse, le ministère public pourra bientôt infliger une amende de 250 000 francs au plus pour non-respect intentionnel des exigences minimales de sécurité (art. 61 let. c nLPD). À l'inverse, pour les violations de sécurité commises par négligence, il ne sera pas possible d'infliger directement une sanction pénale, mais la seule possibilité sera pour le PFPDT d'ordonner des mesures administratives (art. 51 al. 1 et l. 3 let. b LPD) assorties de la menace d'une amende allant jusqu'au même montant (art. 63 nLPD). Quelques semaines après la décision de l'ICO au Royaume-Uni, l'Office du médecin cantonal vaudois a fait fuiter, par

erreur, les adresses électroniques d'individus non vaccinés pour le Covid-19 dans un courriel groupé non anonymisé. La situation juridique suisse différerait de celle prévue par le droit européen, que ce soit en termes de distinction entre dol éventuel et négligence consciente ou de sanctions, et ce au-delà des questions relatives à la violation d'éventuels secrets.

Proposition de citation : Pauline MEYER, Divulgation d'adresses électroniques : l'association HIV Scotland et la nécessité de sécuriser les courriels de masse, 17 novembre 2021 *in* www.swissprivacy.law/104