_swissprivacy.law

Le devoir de formation et de surveillance de l'employeur sous l'angle de la nLPD

Kevin Guillet et Nina Aguiar, le 23 février 2023

De façon générale, tout employeur traite de nombreuses données personnelles dans le cadre de ses activités opérationnelles. Avec l'entrée en vigueur le 1er septembre 2023 de la nouvelle Loi fédérale sur la protection des données, les obligations de l'employeur en la matière vont s'accroître. Il incombera notamment aux employeurs d'assurer la formation des employés sur ces aspects.

En vertu de l'art. 8 al. 1 de la nouvelle Loi fédérale du 25 septembre 2020 sur la protection des données (nLPD), les responsables du traitement et les sous-traitants doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru, dont les exigences minimales seront précisées dans l'ordonnance d'application (art. 8 al. 3 nLPD).

Sans définir concrètement les exigences minimales de sécurité, l'approche choisie consiste dans l'analyse fondée sur le risque, de sorte que les mesures de sécurité minimales doivent être adéquates au risque encouru, au regard de l'ensemble des circonstances.

Si ni la nLPD, ni son ordonnance ne reprennent expressément les exigences minimales applicables en vertu du RGPD, l'un des buts poursuivis par la révision de la loi a consisté dans l'harmonisation du droit suisse aux fins d'assurer une libre et sécure transmission des données entre les entreprises suisses et européennes (FF 2017 6565). Par suite, les minimas prescrits par la règlementation européenne et par les décisions prononcées en son application peuvent servir de guide quant aux minimas à respecter par les entreprises, employeurs et sous-traitants suisses.

Dans une décision du 18 octobre 2021, l'Information Commissioner's Office (ICO) anglais a sanctionné l'association HIV Scotland pour ne pas avoir pris les mesures de sécurité adéquates et ainsi violé le principe de sécurité des données (art. 32 par. 1 et 2 RGPD et 5 par. 1 let. f RGPD ; cf. www.swissprivacy.law/104). Les mesures de sécurité inadéquates avaient résulté en la divulgation d'adresses électroniques de personnes identifiables et susceptibles d'être séropositives ou à risque de contracter le virus. La violation avait consisté dans l'envoi, par un employé, d'un e-mail groupé à 105 personnes par copie carbone (cc) et non par copie cachée (cci), rendant ainsi toutes les adresses visibles à tous les destinataires.

L'intérêt de cette décision au regard de la nLPD ne consiste pas dans la sanction prononcée par l'autorité, mais plutôt dans les mesures qui, selon elle, auraient dû être adoptées par l'association condamnée afin de protéger adéquatement les données des personnes concernées.

Selon l'ICO, une organisation telle que HIV Scotland – laquelle est amenée à traiter des données sensibles – aurait notamment dû mettre en place des formations spécifiques à destination de son personnel, portant sur le maniement des données, l'utilisation des outils informatiques dans ce contexte et sur la confidentialité. L'autorité ajoute que le simple renvoi à la politique de confidentialité n'était pas suffisant et que de réelles formations spécifiques auraient dû être mises en place, ceci avant le traitement effectif par les employés de données personnelles, voire, au plus tard, un mois après leur entrée en fonction.

À supposer que ces exigences doivent être transposées au nouveau droit suisse de la protection des données – ce qui, à teneur du Message du Conseil fédéral, semble être le cas – cela implique que l'art. 8 nLPD et l'ordonnance d'application imposent notamment au responsable de traitement, soit en particulier à l'employeur, qu'il forme effectivement son personnel au maniement de données personnelles et à la confidentialité, dans une mesure à déterminer selon le risque concret encouru et à la sensibilité des données traitées.

En droit du travail, l'art. 328 CO impose à l'employeur une double obligation : celle de ne pas porter atteinte à la personnalité de ses employés et celle de la protéger. L'art. 328b CO dispose que l'employeur ne peut traiter des données concernant le travailleur que dans la mesure où ces données portent sur les aptitudes du travailleur à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail, la Loi fédérale sur la protection des données étant applicable pour le surplus.

L'art. 328b CO instaure ainsi une présomption de licéité du traitement, mais n'exempte pas l'employeur de se conformer aux dispositions de la LPD (TF 4A_518/2020 du 25 août 2021).

Bien que le devoir de protection de l'employeur soit antérieur à l'entrée en vigueur de la nLPD, les nouvelles prescriptions minimales de sécurité impliqueront, à notre sens, un devoir plus étendu de formation de la part de l'employeur, ceci à compter de l'entrée en vigueur de la nLPD. À défaut, l'employeur risque d'engager sa responsabilité tant vis-à-vis des personnes lésées par le traitement des données non conforme, que vis-à-vis de ses propres employés.

Pour satisfaire à ses obligations découlant de l'art. 8 nLPD, l'employeur doit s'assurer de la

formation effective et adéquate de ses auxiliaires s'agissant du maniement de données personnelles et de confidentialité. À cet effet et comme pour les risques liés à la santé des employés, l'employeur doit notamment :

- identifier les risques ;
- informer ses employés de ces risques ;
- donner des instructions adéquates au sujet des mesures de sécurité à prendre pour les éviter ; et
- veiller au respect strict de ces instructions (WYLER R./HEIZER B., Droit du travail, p. 406).

En cas de violation de ce qui précède, l'employeur risque de se rendre coupable, par négligence, ou intentionnellement, d'une violation de l'art. 8 nLPD, susceptible d'aboutir au paiement d'une amende pouvant aller jusqu'à CHF 250'000.- (art. 61 let. c nLPD), et/ou au paiement d'une indemnité pour tort moral en faveur d'un employé lésé (TF 4A_518/2020 du 25 août 2021).

De surcroît, un licenciement prononcé en raison de la violation par l'employé de la politique de sécurité interne ou de la nLPD, pourrait être considéré, en l'absence de formation, d'instructions et de suivi adéquats, comme un licenciement abusif, prononcé par un employeur qui exploiterait sa propre violation de ses obligations.

Il ressort de ce qui précède que l'adoption d'une règlementation – parfois fournie et peu claire pour les personnes amenées à la suivre – n'est aujourd'hui plus suffisante pour l'entreprise.

En conclusion, le droit de la protection des données se précise, prend de l'importance et constitue un élément indiscutable de la personnalité, suivant l'évolution logique initiée il y a quelques années en matière de sécurité et de santé au travail, puis en matière de lutte contre le harcèlement psychologique et sexuel.

À la lumière de la règlementation à venir, on ne saurait trop recommander à tout employeur la mise en œuvre, à tout le moins, d'une formation consacrée au maniement de données personnelles et à la confidentialité, accompagnée de l'établissement de processus internes clairs.

Ce commentaire est repris de celui des mêmes auteurs publié sous www.sigmalegal.ch. Une version anglaise est également disponible.

Proposition de citation : Kevin GUILLET / Nina AGUIAR, Le devoir de formation et de surveillance de l'employeur sous l'angle de la nLPD, 23 février 2023 *in* www.swissprivacy.law/203