VIOLATION DES DONNEES PERSONNELLES : Comment réagir ?

FICHE INFO DU PPDT

INTRODUCTION

Les violations de données personnelles sont de plus en plus fréquentes. Elles constituent un non-respect, involontaire ou de source malveillante, du principe de la sécurité des données (consacré par l'art. 37 LIPAD). Ces violations peuvent intervenir auprès de l'institution publique elle-même ou auprès d'un sous-traitant.

La LIPAD, dans sa version actuelle, ne prévoit pas de dispositions relatives à une annonce de violation de données personnelles. Toutefois, tant la Convention 108+ du conseil de l'Europe que la nouvelle LPD et le RGPD prévoient des règles à cet égard.

Outre la question d'une éventuelle notification des violations de données personnelles, quelles sont les mesures qu'une institution publique confrontée à une telle situation doit prendre ? Le but de la présente fiche informative est de décrire les situations visées par une « violation des données personnelles », les mesures à prendre lorsque la violation intervient auprès de l'institution publique elle-même, respectivement auprès d'un de ses sous-traitants, l'éventuel rôle du Préposé cantonal, ainsi que les principales obligations découlant des textes légaux en matière de protection des données.

LE PRINCIPE DE LA SECURITE DES DONNEES

Toute institution publique qui traite de données personnelles doit en garantir la sécurité. L'art. 37 LIPAD prévoit à cet égard que :

[1] Les données personnelles doivent être protégées contre tout traitement illicite par des mesures organisationnelles et techniques appropriées.

[2] Les institutions publiques prennent, par le biais de directives ainsi que de clauses statutaires ou contractuelles appropriées, les mesures nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des données personnelles qu'elles traitent ou font traiter.

[3] Les institutions publiques sont tenues de contrôler le respect des directives et clauses visées à l'alinéa 2. S'il implique l'exploitation de ressources informatiques et le traitement de données personnelles, ce contrôle doit s'exercer conformément à des procédures spécifiques que les instances mentionnées à l'article 50, alinéa 2, doivent adopter à cette fin, après consultation du préposé cantonal.

Il est complété par l'art. 13 RIPAD :

En général

[1] Les institutions publiques prennent les mesures organisationnelles et techniques propres à assurer la sécurité des données personnelles.

[2] Pour l'administration cantonale, les mesures techniques et organisationnelles nécessaires à la sécurité des données personnelles sont définies notamment par le respect :

a) du règlement sur l'organisation et la gouvernance des systèmes d'information et de communication, du 26 juin 2013;
b) de l'article 23A, alinéa 5, du règlement d'application de la loi générale relative au personnel de l'administration cantonale, du pouvoir judiciaire et des établissements publics médicaux, du 24 février 1999;
c) des directives approuvées par la commission de gouvernance des systèmes d'information et de communication;
d) des règles et mesures de sécurité édictées par les maîtres de fichiers, les responsables départementaux de la sécurité de l'information et l'office cantonal des systèmes d'information et du numérique, sur la base des compétences définies par les règlements visés aux lettres a et b;
e) des prescriptions réglementaires et des directives en matière d'archivage.

Accès aux systèmes d'information

[3] Les institutions publiques tiennent à jour un répertoire des personnes ayant accès aux systèmes d'information contenant des données personnelles.

Ce principe de la sécurité des données se retrouve également à l'art. 7 de la convention 108+, 8 nLPD, ou encore art. 32 et suivants RGPD.

VIOLATION DES DONNEES PERSONNELLES : Comment réagir ?

FICHE INFO DU PPDT

LA NOTION DE VIOLATION DE DONNEES

La notion de violation de données personnelles est définie par la nouvelle LPD, à son art. 5 let. h, comme : « toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données ».

L'art. 4 ch. 12 RGPD en donne une définition presque similaire.

La notion de violation de données personnelles vise ainsi des situations aussi diverses que par exemple l'envoi de données personnelles à un mauvais destinataire (ex : mail envoyé par erreur), la perte d'un ordinateur sur lequel les données ne sont pas chiffrées, une cyberattaque, l'accès aux données par des autorités étrangères, un rançongiciel, le vol de données par un employé ou encore la destruction de données non sauvegardées par ailleurs à la suite d'une mauvaise manipulation.

LES PREMIERES MESURES A PRENDRE EN CAS DE VIOLATION DE DONNEES

Dans tous les cas de violations de données

Le responsable LIPAD de l'institution publique concernée doit être informé de la violation des données et associé aux démarches entreprises. Il en va de même si la violation des données est intervenue auprès d'un sous-traitant. Ce dernier doit en effet annoncer au responsable de traitement (l'institution publique qui a délégué le traitement de données) toute situation de violation de données.

Il sied tout d'abord de comprendre la nature de l'incident et sa portée. Il convient donc de déterminer :

- La nature de la violation et sa cause (perte de données, destruction, manipulation, accès non autorisé, communication à une personne non autorisée, etc…).
- Le moment où la violation est intervenue et le moment où elle a été constatée.
- Les données concernées (nom, prénom, adresse, éventuelles données sensibles, etc…).
- Le nombre approximatif de personnes touchées.
- Si d'autres institutions publiques ont été touchées ou devraient être informées.
- Les conséquences avérées et/ou possibles de la violation (en particulier pour les personnes concernées, à savoir risque d'usurpation d'identité, de pertes financières, de dommage réputationnel, de violation d'un secret, etc…).
- Les mesures prises et à prendre pour limiter les conséquences dommageables de l'incident et éviter qu'il ne puisse se reproduire.
- S'il convient de notifier l'incident et à qui.

Quelle que soit la nature de la violation, il est recommandé à l'institution publique confrontée à un tel incident de documenter précisément les éléments relatifs aux points susmentionnés, afin de pouvoir y remédier de manière optimale. En effet, l'envoi d'un courriel au mauvais destinataire ne nécessite pas le même type de mesures qu'être victime d'une intrusion malveillante dans ses systèmes informatiques.

Une fois ce premier bilan établi, l'institution publique confrontée à une violation de données pourra déterminer quelles mesures techniques ou organisationnelles doivent être prises.

Si la violation est constitutive d'une infraction pénale (art. 143 et 143bis CP), une plainte peut être déposée.

Dans certains cas, la notification de la violation au Préposé cantonal ou aux personnes concernées est recommandée (voir ci-dessous pp. 3-4).

En cas de cyberattaque spécifiquement

Les mesures préconisées ci-dessus visant tous les cas de violations de données doivent être mises en place également en cas de cyberattaque.

En plus de ces mesures, en cas *d'intrusion dans ses systèmes informatiques*, il appartient à l'institution publique de reprendre le contrôle sur les données, dans les meilleurs délais. Il convient donc de prendre contact avec les services informatiques de l'institution publique. Si les connaissances requises font défaut à l'interne, il sied de faire appel à une entreprise de sécurité informatique.

L'on peut se référer au site internet du centre national pour la cybersécurité (NCSC) qui propose plusieurs aide-mémoires, selon différents cas de figure : https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-behoerden/vorfall-was-nun.html

Une telle attaque peut d'ailleurs lui être annoncée : https://www.report.ncsc.admin.ch/fr/

FICHE INFO DU PPDT

VIOLATION DES DONNEES PERSONNELLES : Comment réagir ?

LA NOTIFICATION DES VIOLATIONS DE DONNEES

L'art. 7 § 2 de la **Convention 108+** dispose que chaque Etat membre prévoit que le responsable du traitement est tenu de notifier, sans délai excessif, à tout le moins à l'autorité de contrôle compétente au sens de l'art. 15 de la Convention, les violations des données susceptibles de porter gravement atteinte aux droits et libertés fondamentales des personnes concernées.

Le rapport explicatif[1] précise sur ce dernier point que la révélation de données couvertes par le secret professionnel, ou susceptibles d'entraîner un préjudice financier, une atteinte à la réputation, des dommages corporels ou une humiliation, pourrait être jugée constitutive d'une atteinte « grave ». De même, le risque d'un traitement discriminatoire, un vol ou une usurpation d'identité sont considérés comme des violations comportant des risques importants pour les droits et libertés des personnes concernées (Rapport explicatif, § 64-65).

La **LIPAD** ne prévoit à ce jour pas de notification de violation de données, qu'il s'agisse d'une notification auprès des personnes concernées ou auprès du Préposé cantonal. Cette situation résulte du fait que la LIPAD n'a pas encore été mise à jour au regard des obligations découlant de la Convention 108+. Une révision prochaine de la loi devrait y remédier.

La LPD actuelle ne connaît pas non plus de devoir d'annonce de violation de données ; toutefois, la **nouvelle LPD**, dont l'entrée en vigueur devrait intervenir au deuxième semestre 2022, prévoit à son art. 24 que :

[1] Le responsable du traitement annonce dans les meilleurs délais au PFPDT les cas de violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

[2] L'annonce doit indiquer au moins la nature de la violation de la sécurité des données, ses conséquences et les mesures prises ou envisagées.

[3] Le sous-traitant annonce dans les meilleurs délais au responsable du traitement tout cas de violation de la sécurité des données.

[4] Le responsable du traitement informe la personne concernée lorsque cela est nécessaire à sa protection ou lorsque le PFPDT l'exige.

[5] Il peut restreindre l'information de la personne concernée, la différer ou y renoncer, dans les cas suivants :

a. il existe un motif au sens de l'art. 26, al. 1, let. b, ou 2, let. b, ou un devoir légal de garder le secret qui l'interdit;
b. l'information est impossible à fournir ou exige des efforts disproportionnés;
c. l'information de la personne concernée peut être garantie de manière équivalente par une communication publique.

Une *notification* au PFPDT est donc prévue lorsque le cas de violation entraîne « un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée ». Quels sont les cas de figure visés ?

Une évaluation devra intervenir au cas par cas. La question à se poser est la suivante : quelle est la probabilité (faible, moyenne, élevée) que la violation ait une conséquence négative déterminée (atteinte à la réputation, humiliation, perte d'emploi, discrimination, dommages corporels par exemple) sur la personne concernée et comment cette conséquence négative serait-elle qualifiée (légère, moyenne, grave)[2] ? Il conviendra de prendre en compte, dans l'examen, la nature et le type de données, le type de violation, le nombre de personnes concernées notamment[3].

Des exemples d'atteintes justifiant une annonce au Préposé fédéral pourraient être la perte par un employé d'une clé USB contenant des données privées avec les salaires en texte clair, le piratage d'accès informatiques en ligne (identifiants et mots de passe), l'envoi de documents avec des informations soumises au secret (fiscal par exemple) aux mauvais destinataires[4].

En cas de doute, il est préférable de signaler une violation des données que de la cacher[5].

Le contenu de l'annonce est détaillé à l'art. 24 al. 2 nLPD. Il s'agit essentiellement des informations relatives à l'analyse de l'incident et à sa portée.

---

[1] Rapport explicatif – STCE 223 – Traitement automatisé des données à caractère personnel. Protocole d'amendement), 10.X.2018, disponible à l'adresse suivante : https://rm.coe.int/16808ac91b

[2] Rosenthal David, La nouvelle loi sur la protection des données, jusletter 16 novembre 2020, n°162. Les nombreux exemples cités par cet auteur, ainsi que sa matrice d'analyse du risque, sont des éléments d'aide auxquels il est recommandé de se référer.

[3] Métille Sylvain / Meyer Pauline, Annonce des violations de la sécurité des données : une nouvelle obligation de la nLPD, RSDA 1/2021, p. 26.

[4] Rosenthal, op. cit., n°163.

[5] Métille / Meyer, op. cit., p. 26.

Aucun délai n'est expressément prévu pour l'annonce au Préposé fédéral ; cette dernière doit intervenir le plus rapidement possible dès que les informations minimales requises par la loi sont connues[6].

Le but d'une telle annonce est que le Préposé fédéral puisse suivre la situation et prodiguer des conseils sur les mesures à prendre et sur l'éventuelle nécessité d'informer les *personnes concernées*.

S'agissant de la notification aux personnes concernées, l'obligation prévue par l'art. 24 al. 4 nLPD va moins loin que l'obligation d'annonce au PFPDT. Elle doit intervenir lorsque cela est nécessaire à la protection de la personne concernée ou lorsque le PFPDT l'exige. Si la personne concernée peut elle-même prendre des mesures pour sa protection (changement de mot de passe par exemple), il convient de l'en informer.

Au niveau européen, les art. 32 et 33 **RGPD** prévoient des exigences d'annonce sensiblement plus exigeantes que la nouvelle LPD. A ce propos, il est renvoyé à un document élaboré par la CNIL : https://www.cnil.fr/fr/les-violations-de-donnees-personnelles et https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Pour des exemples détaillés, toujours en application du RGPD, l'on peut se référer aux lignes directrices 01/2021 sur les exemples de notifications de violation de données adoptées le 14 décembre 2021, dans lesquelles sont traités des cas aussi différents que la situation du rançongiciel ou de la perte de documents :

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en

CONCLUSION

La présente fiche informative a pour vocation de donner quelques lignes directrices sur les mesures à prendre suite à une violation de données personnelles. A cet égard, les obligations légales (d'annonce) vont être renforcées pour le secteur privé et les organes fédéraux avec l'entrée en vigueur de la nLPD. La LIPAD va très certainement subir des modifications dans un même esprit.

Dans l'attente de ces modifications, le Préposé cantonal recommande aux institutions publiques touchées par une violation de données de procéder d'ores et déjà aux annonces comme proposé dans la présente fiche informative. De plus, afin de pouvoir répondre à une violation des données avec réactivité, il est vivement recommandé aux institutions publiques d'agir également de manière préventive en préparant et testant des processus clairs à suivre concernant la détection de la violation, la mise en place de mesures correctrices, l'annonce et la collecte d'informations nécessaires[7].

PPDT – 24.02.2022

Le Préposé cantonal à la protection des données et à la transparence (PPDT) est une autorité indépendante qui renseigne, conseille et surveille l'application de la LIPAD par les autorités et institutions publiques genevoises. N'hésitez pas à appeler en cas de questions au n° de téléphone 022 546 52 40 ou à adresser un courriel à ppdt@etat.ge.ch.

[7] Métille / Meyer, op. cit., p. 26.