_swissprivacy.law

Le PFPDT guide les responsables du traitement quant à leur devoir d'informer des violations de la sécurité des données

David Dias Matos et Célian Hirsch, le 19 février 2025

Une violation de la sécurité des données peut imposer au responsable du traitement d'en informer tant le PFPDT que les personnes concernées. Le guide du PFPDT précise la vision de l'autorité quant à l'application de ce devoir d'informer.

PFPDT, Guide relatif à l'annonce des violations de la sécurité des données et l'information des personnes concernées en vertu de l'art. 24 LPD du 6 février 2025

La sécurité des données est un équilibre délicat, où chaque faille peut laisser entrer des risques menaçant l'intégrité, la disponibilité et la confidentialité des informations. Lorsqu'une violation de la sécurité se produit, le droit impose à certaines conditions une direction : celle de l'alerte et de la transparence.

Pour orienter les responsables du traitement, le Préposé fédéral à la protection des données (PFPDT) offre un guide visant à éclairer le devoir d'annonce des violations de la sécurité des données.

L'annonce d'une violation de la sécurité des données (art. 24 LPD) que ce soit au PFPDT (al. 1) ou aux personnes concernées (al. 4) présuppose la survenance d'une violation de leur sécurité. A teneur de l'art. 5 let. h LPD, il s'agit de

> *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.*

En cas de violation de la sécurité des données, l'art. 24 LPD prévoit des obligations pour le responsable du traitement et des droits pour les personnes concernées.

Dans son Guide relatif à l'annonce des violations de la sécurité des données et l'information des personnes concernées en vertu de l'art. 24 LPD, le PFPDT présente dans un premier temps les conditions légales pour l'annonce des violations au PFPDT (art. 24 al. 1 LPD). Dans

un deuxième temps, il précise les conditions d'information des personnes concernées (art. 24 al. 4 LPD). La présente contribution en restitue les grandes lignes et propose quelques remarques critiques.

Annonces au PFPDT

L'art. 24 al. 1 LPD prévoit que

> *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.*

Lorsque le responsable du traitement a connaissance d'une violation de la sécurité des données (art. 5 let. h LPD), il doit conduire une analyse afin d'en déterminer l'étendue et les risques. Si l'analyse des risques révèle qu'un risque élevé au sens de l'art. 24 al. 1 LPD existe ou ne peut être exclu, le responsable du traitement doit communiquer la violation de sécurité des données au PFPDT.

Le fait d'admettre un devoir d'informer en raison du simple fait que le risque élevé « ne peut être exclu » n'est pas convaincant. Cela ne correspond ni à l'exigence de la lettre de la loi (existence d'un risque élevé), ni à l'intention du législateur. En effet, le seuil de risque élevé a pour but « d'éviter l'annonce de violations insignifiantes » (FF 2017 6681). La lecture du PFPDT reviendrait à créer une présomption de risque élevé. Or, contrairement au législateur européen (cf. art. 33 RGPD), le législateur suisse n'a pas voulu de telle présomption (cf. art. 17 al. 1 AP-LPD ; Hirsch Célian, Le devoir d'informer lors d'une violation de la sécurité des données – Avec un regard particulier sur les données bancaires, thèse, Genève 2023, p. 146 ss).

Le contenu de l'annonce est énuméré à l'art. 15 al. 1 OPDo. Elle contient notamment la nature de la violation (let. a), les catégories de données personnelles et de personnes concernées (let. c et d), ainsi que les conséquences, y compris les risques, (let. e) et les mesures prises ou prévues pour y remédier (let. f).

Lorsque le PFPDT reçoit l'annonce, il examine succinctement si les mesures d'urgence et de suivi prises ou prévues par le responsable du traitement pour protéger les personnes concernées et réduire les inconvénients (art. 15 al. 1 let. f OPDo) paraissent appropriées, suffisantes et opportunes.

Selon le Guide, le PFPDT peut demander au responsable du traitement des précisions concernant les faits décrits et de modifier ou de compléter les mesures prises ou prévues. Il pourrait également prendre contact avec lui afin de s'assurer que l'incident soit bien documenté.

À notre avis, la simple existence d'une violation de la sécurité ne permet pas au PFPDT d'imposer des mesures de sécurité au responsable du traitement. S'il veut imposer de telles mesures, il doit démontrer une violation du principe de sécurité des données (art. 8 *cum* art. 51 LPD), ce qui diffère d'une violation de la sécurité au sens de l'art. 5 let. h LPD (cf. Hirsch, *op. cit.*, p. 77 ss).

En outre, l'obligation de documenter l'incident ne trouve pas sa source dans la loi. Elle nous semble ainsi invalide en raison de l'absence d'une base légale formelle (cf. Hirsch, *op. cit.*, p. 361 ss).

Le PFPDT examine si les personnes concernées sont informées de l'incident et de ses conséquences (art. 15 al. 3 et 4 OPDo). S'il en va de l'intérêt général, il peut également informer le public de ses constatations et décisions conformément à l'art. 57 al. 2 LPD.

Selon la jurisprudence, la publication d'une décision constitue une sanction en soi (ATF 143 I 352 c. 4.1, résumé *in* LawInside.ch/480/ ; TF, 2D_8/2021 (publié aux ATF 148 I 226), c. 4.3.2, commenté *in* LawInside.ch/1218/). Vu que la LPD ne prévoit pas ce type de sanction, nous considérons que le PFPDT ne devrait pas pouvoir publier une décision non anonymisée (cf. Hirsch, *op. cit.*, p. 109 s.). Il peut cependant publier un communiqué de presse nommant le responsable du traitement « [s]'il en va de l'intérêt général » (comp. 2C_682/2023*, commenté *in* LawInside.ch/1510/, au sujet de la pratique de publication de la FINMA).

Le PFPDT a également la faculté de réceptionner les annonces de violation de la sécurité des données adressées spontanément. C'est le cas notamment des situations dans lesquelles les responsables du traitement n'identifient pas de risque élevé pour les personnes concernées, mais souhaitent tout de même l'en informer. Cette possibilité est particulièrement utile en présence d'une violation de la sécurité impliquant un risque faible, mais un grand nombre de personnes concernées dont une couverture médiatique n'est pas à exclure.

Afin de déposer une annonce selon l'art. 24 al. 1 LPD, le PFPDT met un portail d'annonce à disposition (databreach.edoeb.admin.ch). Ce portail garantit la transmission sécurisée des données au PFPDT. Il garantit également que l'annonce contient les informations énumérées à l'art. 15 al. 1 OPDo.

Dans la mesure où aucune forme n'a été imposée par la loi, l'utilisation d'un formulaire sur le site du PFPDT peut être recommandée, mais l'autorité ne saurait refuser de traiter une annonce qui lui parviendrait par courrier postal (cf. CR LPD-Métille/Meyer, art. 24, N 53). Cependant, afin de structurer et de simplifier les démarches, il semblerait opportun d'en faire usage.

Risque élevé selon l'art. 24 al. 1 LPD

Comme évoqué, le responsable du traitement a l'obligation d'annoncer une violation de la sécurité lorsqu'elle entraîne « vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée ».

L'évaluation du risque élevé se fait en deux temps. Dans un premier, le responsable du traitement doit clarifier dans quelle mesure la violation a déjà entrainé des atteintes à la personnalité ou aux droits fondamentaux des personnes physiques. Dans un deuxième, tout en s'appuyant sur le critère de « vraisemblance » mentionné dans la loi, il intègre à son évaluation les conséquences pour les personnes potentiellement concernées. Ce facteur n'est ni mesurable définitivement, ni prévisible de manière certaine au moment de l'évaluation.

Selon le Guide, l'évaluation du risque vraisemblablement élevé (art. 24 al. 1 LPD) doit être faite sans tenir compte des mesures correctives prises après la violation. Toutefois, dans la pratique du PFPDT, les mesures d'urgence prises avant l'annonce peuvent être considérées si elles ont effectivement réduit ou éliminé le risque.

Par exemple, si une entreprise reprend rapidement le contrôle de ses bases de données et prouve qu'aucun usage malveillant n'a eu lieu, cela peut atténuer l'évaluation du risque. Cependant, en cas de doute, l'annonce doit être faite sans attendre, notamment lorsqu'on ignore si des données volées ont été exploitées, comme dans le cas d'une attaque par rançon logiciel (*ransomware*).

Selon le PFPDT, l'évaluation du risque vraisemblablement élevé repose sur plusieurs critères. Nous en restituons ici quelques-uns.

La nature des données est déterminante. Plus elles sont sensibles (de santé, biométriques, sur l'aide sociale), plus le risque est élevé. Toutefois, même des données non sensibles peuvent présenter un risque selon leur contexte d'utilisation.

Les circonstances de la violation jouent également un rôle clé. Une fuite due à un acte crimi-

nel ou une exposition sur le darknet augmente le risque, tandis qu'une suppression involontaire sans diffusion externe en réduit l'impact. De même, plus il est facile d'identifier les personnes concernées, plus le risque est élevé, sauf si les données sont efficacement chiffrées.

D'autres facteurs entrent en compte, comme le volume et la durée du traitement, le préjudice moral ou économique (usurpation d'identité, fraude, discrimination) et la vulnérabilité des personnes concernées (mineurs, personnes en situation de handicap).

Enfin, un grand nombre de personnes touchées ne signifie pas automatiquement un risque élevé, mais peut justifier une annonce pour des raisons d'intérêt public. L'évaluation repose ainsi sur une analyse globale des données, des circonstances et des conséquences potentielles.

De surcroît, encore faut-il évaluer la probabilité des conséquences redoutées. Cela consiste à estimer si les effets négatifs d'une violation de la sécurité des données sont susceptibles de se produire. En règle générale, plus les données concernées sont sensibles, plus cette probabilité est élevée. Par exemple, un hôpital traitant des données médicales doit considérer un risque plus important qu'un distributeur alimentaire, même avant d'avoir la certitude que des informations sensibles ont été compromises.

Principe de transparence

Les annonces de violations de la sécurité des données au PFPDT sont soumises au principe de transparence prévu par la loi fédérale sur la transparence (LTrans). Elles sont considérées comme des documents officiels et sont donc, en principe, accessibles au public, qu'elles soient obligatoires ou spontanées. Toutefois, le PFPDT peut limiter ou différer l'accès selon les exceptions prévues les art. 7 ss LTrans. Avant toute divulgation, il doit consulter les tiers concernés et statuer par une prise de position ou une décision.

À notre avis, le PFPDT doit en particulier examiner si l'annonce contient certaines informations protégées par le secret d'affaires (art. 7 al. 1 let. g LTrans ; cf. Hirsch, *op. cit.*, p. 432 ss). Il doit en tout état effectuer une pesée des intérêts si le requérant désire obtenir un rapport de violation de la sécurité non anonyme (art. 7 al. 2 et 9 LTrans ; cf. Hirsch, *op. cit.*, p. 439 s.).

Obligation et sanction

Si le responsable du traitement omet de notifier une violation de la sécurité des données au PFPDT, ce dernier peut lui ordonner de rectifier l'omission (art. 51 al. 3 let. f LPD). D'autres mesures administratives peuvent être imposées, par exemple si les exigences de l'art. 8 LPD ne sont pas respectées.

Selon le Guide, le non-respect total ou partiel de l'obligation de notification n'est pas sanctionné par la LPD. Une précision est de mise. Lorsque le PFPDT ordonne au responsable du traitement d'annoncer une violation de la sécurité par décision sous la menace de la peine prévue à l'art. 63 LPD, alors son non-respect est punissable. De plus, une violation de la sécurité des données peut entraîner des conséquences pénales si les exigences minimales de sécurité ne sont pas respectées (art. 61 let. c LPD).

En outre, l'art. 24 al. 6 LPD précise que les notifications obligatoires ne peuvent être utilisées dans une procédure pénale sans consentement préalable.

Information aux personnes concernées

Le Guide du PFPDT aborde également un aspect essentiel lié aux violations de la sécurité des données, à savoir l'obligation d'informer les personnes concernées en vertu de l'art. 24 al. 4 LPD. Cette obligation d'information est distincte de l'obligation de notification au PFPDT en vertu de l'art. 24 al. 1 LPD. Elle est régie par des conditions spécifiques.

L'obligation d'informer la personne concernée s'applique « lorsque cela est nécessaire à sa protection ou lorsque le PFPDT l'exige » (art. 24 al. 4 LPD). Cela est présumé lorsque la personne concernée peut ou doit prendre des mesures pour réduire ou éviter un dommage, comme modifier des mots de passe ou bloquer une carte de crédit. Le besoin de protection peut également exister dans d'autres situations, par exemple en cas de risques liés à des courriels de *phishing*.

Le PFPDT clarifie une controverse doctrinale : l'obligation d'informer les personnes concernées n'est pas conditionnée à l'existence d'un « risque élevé » au sens de l'art. 24 al. 1 LPD (cf. ég. Hirsch, *op. cit.*, p. 160 ss).

Selon le Guide, le PFPDT peut exiger que le responsable du traitement informe les personnes concernées tant en raison de leur besoin de protection qu'en raison d'un éventuel intérêt public, par exemple en raison d'un grand nombre de personnes concernées ou d'une couverture médiatique.

Comme le souligne Vasella, cette appréciation est erronée. Le PFPDT ne peut imposer au responsable du traitement de respecter que ses devoirs découlant de la LPD, à savoir informer la personne concernée « lorsque cela est nécessaire à sa protection » au sens de l'art. 24 al. 4 LPD. En d'autres termes, si le responsable du traitement n'informe pas la personne concernée, le PFPDT peut procéder à sa propre analyse de la nécessité de l'information en faveur des personnes concernées. Ce n'est que si l'information est en effet nécessaire à la protection de la personne concernée que le PFPDT pourra ordonner au responsable du traitement une annonce (cf. Hirsch, *op. cit.*, p. 164).

L'information fournie aux personnes concernées doit être claire et compréhensible, conformément à l'art. 15 al. 3 OPDo. Elle doit inclure la nature de la violation, ses conséquences, les risques pour les personnes concernées, ainsi que les mesures prises pour y remédier. La méthode d'information est laissée au choix du responsable du traitement, mais celle-ci doit être directe et individuelle. Une communication publique est possible uniquement dans des cas exceptionnels, lorsque l'information de toutes les personnes concernées peut être assurée de manière équivalente.

Si le responsable du traitement omet ou refuse d'informer les personnes concernées comme prévu par l'art. 24 al. 4 LPD, le PFPDT peut lui ordonner de rectifier cette défaillance, conformément à l'art. 51 al. 3 let. f LPD. En outre, des mesures administratives supplémentaires peuvent être prises, notamment si les exigences de l'art. 8 LPD n'ont pas été respectées.

En chiffres

Entre le 9 mai 2023 (à savoir la mise en ligne de la plateforme d'annonce du PFPDT) et le 8 août 2024, un total de 353 annonces de violation de la sécurité a été effectué. Comme indiqué dans le Guide, ces annonces permettent en pratique au PFPDT de vérifier si les personnes concernées ont été également informées et, si tel n'est pas le cas, d'inciter le responsable du traitement à les informer.

Les catégories de données personnelles les plus vulnérables ont été les noms, les adresses (email) ainsi que les données de carte d'identité, d'impôts ou encore d'AVS. Ces violations ont principalement conduit à l'usurpation d'identité des personnes concernées, de la fraude ou encore à la divulgation de secrets de fonction ou professionnels.

Conclusion

Le présent guide est le bienvenu pour épauler les responsables du traitement et réduire les

potentielles conséquences négatives sur les personnes concernées. Il ne constitue cependant que la vision du PFPDT et ne lie pas les tribunaux.

Les critères définis dans le guide du PFPDT sont largement en accord avec ceux identifiés dans les Lignes directrices 9/2022 sur la notification de violations de données à caractère personnel en vertu du RGPD (pour un exemple d'une affaire de violation de la sécurité à l'aune du RGPD, cf. swissprivacy.law/105/), ce qui témoigne d'une harmonisation croissante entre la législation suisse et européenne (concernant l'influence du RGPD sur la LPD, cf. Hirsch, *op. cit.*, p. 126 ss). Cela étant, pour interpréter la LPD, il convient de bien tenir compte de la volonté du législateur suisse, lequel a parfois voulu se distancer du RGPD (pour l'influence du droit de l'UE dans l'interprétation de la LPD, cf. Hirsch, *op. cit.*, p. 130 ss).

Proposition de citation : David Dias Matos / Célian Hirsch, Le PFPDT guide les responsables du traitement quant à leur devoir d'informer des violations de la sécurité des données, 19 février 2025 *in* www.swissprivacy.law/338