ANWALTS
REVUE
DE L'AVOCAT

Stämpfli
Verlag

Anwaltsrevue|Revue de l'avocat 8/2024 | S. 323–327

Thema

LE DEVOIR D'INFORMER DE L'AVOCAT LORS D'UNE VIOLATION DE LA SÉCURITÉ DES DONNÉES

Célian Hirsch Docteur en droit, avocatà Genève, chercheur affilié au Centre de droit bancaire et financier de l'Université de Genève

Mots-clés: violation de la sécurité, protection des données, secret de l'avocat, devoir d'informer

Si l'avocat subit une violation de la sécurité des données – laquelle est une notion très large –, il doit examiner s'il est soumis à un devoir d'informer le PFPDT ou les personnes concernées de cette violation. La présente contribution présente la notion de violation de la sécurité des données et expose l'examen auquel doit procéder l'avocat afin de déterminer s'il est soumis à un tel devoir d'informer. Elle analyse ensuite la limite du devoir d'informer en raison du secret professionnel de l'avocat et conclut que cette limite est relative.

I. Introduction

La sécurité absolue n'existe pas[1]. Les études d'avocats suisses, aussi bien protégées soient-elles, peuvent être victimes de cyberattaques[2]. Ces études doivent-elles annoncer ces violations au Préposé fédéral à la protection des données et à la transparence (PFPDT)? Doivent-elles également en informer les clients et tiers?

Cette contribution répond à ces questions en exposant le nouveau devoir d'informer en cas de violation de la sécurité (art. 24 LPD) et en examinant si le secret d'avocat (art. 13 LLCA; art. 321 CP) peut limiter ce devoir. Elle se fonde sur la thèse de doctorat publiée par l'auteur de ces lignes[3].

II. Le devoir d'informer lors d'une violation de la sécurité (art. 24 LPD)

1. La violation de la sécurité (art. 5 let. h LPD)

A) La notion légale

L'ancienne LPD de 1992 (aLPD) ne connaissait pas la notion de violation de la sécurité des données[4]. Le Règlement général de l'UE sur la protection des données (RGPD) a introduit cette notion en 2016[5]. Le législateur suisse a suivi en ajoutant cette notion dans la nouvelle LPD entrée en vigueur le 1er septembre 2023[6]. Constitue ainsi une «violation de la sécurité des données» *(Verletzung der Datensicherheit),* au sens de l'art. 5 let. h LPD, «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 autorisé à ces données»[7]. Les divers cas de violation de la sécurité sont examinés ci-dessous.

L'existence de cette violation ne dépend pas des risques consécutifs à la violation de la sécurité. Les risques – à savoir les potentielles conséquences de la violation de la sécurité – sont uniquement pertinents pour déterminer l'existence d'un devoir d'informer le PFPDT[8].

B) La perte

La perte *(Verlust)* signifie que le responsable du traitement a perdu le contrôle ou l'accès aux données, même momentanément.[9] La perte porte atteinte à la disponibilité des données. Elle constitue une violation de la sécurité, même sans accès indu. Par exemple, la perte d'une clé USB, d'un ordinateur portable ou d'un document papier contenant des données personnelles est une violation de la sécurité[10]. Entre le 1er septembre 2023 et le 8.8.2024, 144 des 353 annonces de violation de la sécurité concernaient des cas de pertes de données[11].

C) L'altération

La modification, l'effacement ou la destruction de données *(Änderung, Löschung oder Vernichtung von Daten)* peuvent être regroupés dans «l'altération» des données[12]. Lors d'une altération de données, l'intégrité des données est atteinte[13].

Par exemple, en cas d'attaque par *ransomware* (rançongiciel), les données sont chiffrées. Si le responsable du traitement possède une copie de ces données, il n'a heureusement pas perdu les données chiffrées. Cela étant, ces dernières sont altérées en raison de ce chiffrement. Il y a donc une violation de la sécurité à cause de cette altération illicite[14].

L'altération doit être «accidentelle ou illicite». En effet, une modification volontaire et licite de données, par exemple leur destruction après une certaine période, ne constitue logiquement pas une violation de la sécurité. Il suffit que l'altération soit accidentelle ou illicite (condition alternative) pour qu'il y ait violation de la sécurité[15].

D) La divulgation et l'accès non autorisé

Un accès non autorisé *(unbefugte Zugänglichkeit)* se produit dès qu'une personne a la possibilité concrète de prendre connaissance des données sans en avoir le droit, indépendamment du fait qu'elle en ait effectivement pris connaissance. C'est la confidentialité des données qui est atteinte[16]. Il y a par exemple un accès non autorisé si les données de l'avocat peuvent être accessibles par Internet sans effort particulier[17]. Pour sa part, la notion de divulgation non autorisée est complètement absorbée par la notion d'accès non autorisé. En effet, dès qu'il y a une divulgation non autorisée, c'est-à-dire qu'un tiers a pris connaissance des données, il y a aussi un accès non autorisé[18].

L'accès aux données n'a pas besoin d'être direct. En effet, la possibilité concrète d'avoir accès au support de données (clé USB, ordinateur, téléphone portable, etc.) constitue déjà un accès si celui-ci n'est pas protégé contre l'accès non autorisé (par exemple en raison de l'absence de mot de passe)[19].

Entre le 1er septembre 2023 et le 8.8.2024, 295 des 353 annonces de violation de la sécurité concernaient des cas de divulgation de données[20]. Il s'agit probablement des cas les plus fréquents de violation de la sécurité qui entrainent un risque élevé pour les personnes concernées (cf. *infra* 2).

Afin de se prémunir contre ces divers types de violation de la sécurité, l'avocat doit nécessairement adopter des mesures organisationnelles et techniques appropriées, conformément à l'art. 8 LPD et aux art. 1 ss OPDo[21].

2. Le devoir d'informer le PFPDT (art. 24 al. 1 LPD)

L'art. 24 al. 1 LPD (annonce des violations de la sécurité des données; *Meldung von Verletzungen der Datensicherheit*) prévoit que «[l]e 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.»[22]

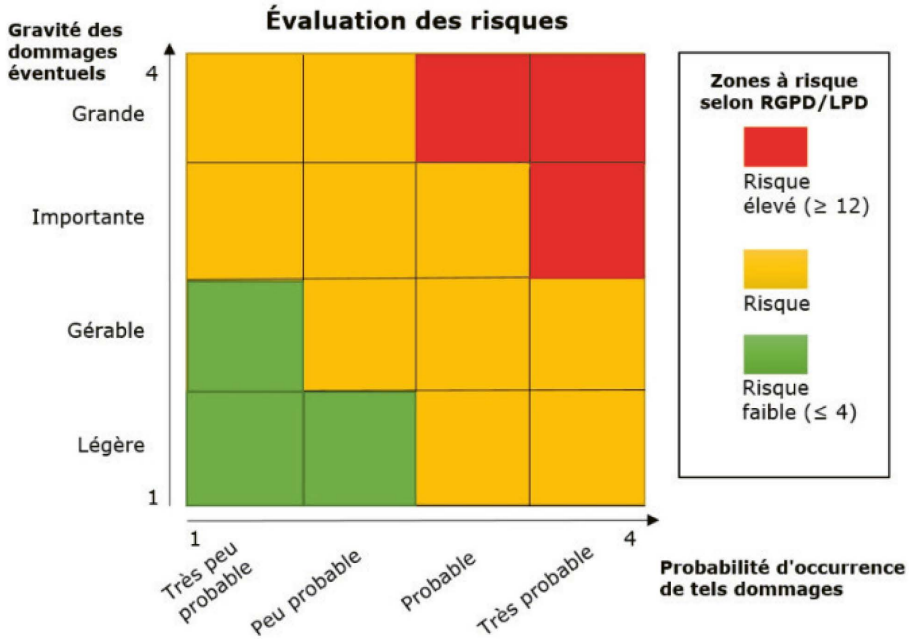
Afin de déterminer si une violation de la sécurité va entraîner «vraisemblablement un risque élevé» pour les

personnes concernées, l'avocat doit examiner les conséquences vraisemblables de la violation de la sécurité selon les éléments suivant:

- la nature, la taille et le contenu des données concernées[23];
- le type et les circonstances de la violation de la sécurité;
- le nombre de personnes concernées[24];
- la facilité d'identification des personnes concernées[25].

L'avocat doit procéder à un pronostic après avoir tenu compte de chacun de ces éléments [26]. Enfin, l'exigence de la vraisemblance du risque élevé *(voraussichtlich, verosimilmente, likely)* signifie que le risque élevé ne doit pas être certain. Il doit cependant être suffisamment probable[27].

Le tableau ci-dessous, élaboré par Rosenthal[28], illustre l'examen du risque en matière de violation de la sécurité:



L'avocat, comme tout responsable du traitement, est soumis à une obligation de collaborer avec le PFPDT lorsque ce dernier ouvre une enquête à son encontre[29]. Il devra partager son analyse du risque avec l'autorité.

Cette dernière pourra ainsi examiner directement si cette analyse a été effectuée correctement, au lieu de procéder à la sienne *ab initio*[30].

L'art. 15 OPDo précise l'information à communiquer au PFPDT[31]. L'avocat ne devra jamais communiquer les données des personnes concernées. Le secret de l'avocat ne peut ainsi en aucun cas s'opposer à l'information au PFPDT.

En pratique, le PFPDT a mis en place un formulaire web pour que le responsable du traitement puisse procéder aux annonces de la violation de la sécurité[32]. Ce formulaire propose notamment que le responsable du traitement indique si les données concernées par la violation de la sécurité sont des données soumises au secret professionnel. Le responsable du traitement peut aussi indiquer s'il a informé les personnes concernées.

Entre le 1er septembre 2023 et le 8.8.2024, le PFPDT a reçu 353 annonces de violation de la sécurité[33]. Parmi ces 353 annonces, 111 cas concernent des données soumises au secret professionnel, administratif ou fiscal, et 121 ont pour conséquence une divulgation de secrets de fonction ou professionnels. De ces 353 annonces, 25 concernent entre 500 et 200 personnes concernées et 37 concernent même plus de 2000 personnes concernées[34].

En pratique, le PFPDT se concentre sur cet aspect, conformément au but de la LPD[35]. Il va ainsi pouvoir inciter l'avocat à informer les personnes concernées, conformément à l'art. 24 al. 4 LPD examiné ci-dessous.

3. Le devoir d'informer les personnes concernées (art. 24 al. 4 LPD)

A) La base légale

L'art. 24 al. 4 LPD (annonce des violations de la sécurité des données) prévoit que «[l]e responsable du traitement informe par ailleurs la personne concernée lorsque cela est nécessaire à sa protection ou lorsque le PFPDT l'exige»[36].

Comme pour l'art. 34 par. 1 RGPD[37], il existe ainsi deux conditions alternatives à l'existence d'un devoir d'information en faveur de la personne concernée: soit cela est nécessaire à sa protection, soit le PFPDT l'exige. Contrairement à l'art. 24 al. 1 LPD (information au PFPDT), l'art. 24 al. 4 LPD ne conditionne pas le devoir d'informer les personnes concernées à l'existence d'un risque[38].

B) Lorsque cela est nécessaire à la protection de la personne concernée

L'avocat informe la personne concernée de la violation de la sécurité de ses données uniquement si cela est nécessaire à sa protection (art. 24 al. 4 LPD). Il doit procéder, comme pour le devoir d'annonce au PFPDT, à un pronostic. Ce pronostic lui permet d'estimer si la personne concernée est plus apte qu'elle, voire qu'un tiers, à exécu-

ter les mesures lui permettant de réduire les risques. Si, au contraire, l'avocat est plus à même de prendre les mesures nécessaires à la protection de la personne concernée, l'informer de la violation de la sécurité ne sera pas nécessaire. Cette approche permet de respecter la condition de nécessité, à savoir qu'aucune autre mesure plus proportionnée ne permet d'atteindre le but visé[39]. En outre, l'avocat peut s'inspirer de l'art. 34 par. 3 let. a et b RGPD[40] afin de juger de la nécessité d'informer la personne concernée. Enfin, comme pour l'art. 34 par. 1 RGPD, et contrairement à l'analyse de risque prévue par l'art. 24 al. 1 LPD, le nombre de personnes concernées n'est pas

pertinent pour l'information aux personnes concernées[41].

Ainsi, si l'avocat est victime d'une attaque par *ransomware* (rançongiciel) avec extraction de données, il devra examiner les conséquences de la publication des données sur le *darkweb.* Vu la potentielle forte atteinte réputationnelle pour de nombreux clients, il sera en principe nécessaire de les en informer afin qu'ils puissent eux-mêmes adopter rapidement les mesures nécessaires.

C) Lorsque le PFPDT l'exige

L'art. 24 al. 4 LPD permet au PFPDT d'exiger que le responsable du traitement informe la personne concernée de la violation de la sécurité. Ainsi, si l'avocat considère qu'informer la personne concernée n'est pas nécessaire à sa protection, le PFPDT peut procéder à son propre pronostic. Si l'autorité arrive à la conclusion que l'information à la personne concernée est «nécessaire à sa protection», et qu'aucune exception ne trouve application, le PFPDT pourra ordonner à l'avocat d'en informer les personnes concernées[42].

Comme dans l'UE[43], le PFPDT ne peut pas aller au-delà de l'exigence légale. Il peut ainsi ordonner à l'avocat d'informer la personne concernée uniquement lorsque cela «est nécessaire à sa protection». Si cette condition n'est pas remplie, le PFPDT ne peut pas imposer à l'avocat d'informer la personne concernée de la violation de la sécurité[44].

La décision du PFPDT est attaquable auprès du Tribunal administratif fédéral[45]. Dès son entrée en force, et si la décision du PFPDT contient la menace d'une sanction pénale au sens de l'art. 63 LPD, l'avocat qui n'informe volontairement pas les personnes concernées commet un acte pénalement répréhensible[46].

III. L'exception du secret d'avocat au devoir d'informer?

Le devoir d'informer le PFPDT ne connaît aucune exception[47]. Au contraire, le devoir d'informer les personnes concernées est expressément limité par l'art. 24 al. 5 LPD. L'avocat «peut restreindre l'information de la personne concernée, la différer ou y renoncer [lorsqu'un] devoir légal de garder le secret (...) l'interdit» (art. 24 al. 5 let. a LPD).

Cette disposition constitue un rappel que les dispositions légales sur le secret l'emportent sur la LPD en tant que *lex specialis.* Comme pour l'art. 20 al. 1 let. c LPD (exceptions au devoir d'informer et restrictions), la confidentialité prime ainsi le devoir d'information. Néanmoins, et de manière semblable à l'art. 9 al. 1 let. b LPD, le secret ne constitue pas une restriction absolue. Il faut vérifier si l'avocat peut respecter son devoir d'informer de manière conforme à l'obligation de protéger le secret[48].

On doit dès lors se demander si l'avocat viole nécessairement son secret[49] s'il informe les personnes concernées de la violation de la sécurité des données.

Tout d'abord, le détenteur du secret, c'est-à-dire l'avocat, ne peut pas l'invoquer contre son maître, à savoir le client[50]. Ainsi, le secret ne s'oppose jamais à informer le client d'une violation de la sécurité. Mais qu'en est-il des autres personnes concernées? La question paraît ici plus délicate. Afin d'y répondre, il convient d'examiner si l'information à la personne concernée constitue une révélation du secret.

Concrètement, l'avocat pourrait d'abord obtenir le consentement du client afin d'informer les tiers[51]. Le secret ne s'opposerait ainsi plus à l'information. En l'absence du consentement, l'avocat doit examiner si le fait d'informer la personne concernée constitue une révélation de son secret. Tel n'est pas le cas si la personne concernée sait déjà que l'avocat traite des données à son sujet. En effet, les informations que l'avocat doit lui fournir au sujet de la violation de la sécurité ne révèlent alors aucun fait protégé par le secret[52]. Au contraire, si la personne concernée ne sait pas que l'avocat traite ses données, le simple fait de l'informer d'une violation de la sécurité

révèle qu'il traite ses données, ce qui constitue un fait protégé par le secret[53].

Ainsi, si un avocat doit informer une personne concernée d'une violation de la sécurité, il doit examiner si celle-ci sait déjà qu'il traite ses données, par exemple parce qu'elle est partie dans une procédure pendante ou qu'elle l'était dans une procédure terminée. Le cas échéant, l'avocat peut sans autre en informer la personne concernée sans violer son secret, puisque cette personne savait déjà que l'étude traitait ses données. Au contraire, si un avocat est par exemple en train de préparer une action judiciaire, la personne concernée ne sait potentiellement pas que l'avocat traite ses données. L'informer d'une violation de la sécurité consisterait alors en une révélation du secret, qui est prohibée[54].

Par ailleurs, l'avocat doit également examiner si le devoir d'informer peut être restreint, et non éteint, conformément au principe de proportionnalité. Il s'agit en particulier de caviarder les informations couvertes par le secret.

IV. L'absence de conséquences pénales lors d'une violation du devoir d'informer

L'avant-projet de la LPD (AP-LPD) proposait une amende jusqu'à CHF 500000 pour la personne privée qui ne respectait pas son devoir d'informer le PFPDT ou les personnes concernées, même en cas de négligence (art. 50 AP-LPD). Cette disposition a été critiquée pour sa contradiction avec le principe *nemo tenetur* et l'absence de protection contre l'exploitation du rapport de violation en procédure pénale[55].

En réponse aux critiques, le Conseil fédéral a remanié le projet en limitant les sanctions pénales aux «devoirs essentiels»[56]. Informer le Préposé ou les personnes concernées d'une violation de la sécurité n'a pas été retenu comme un «devoir essentiel». Partant, le projet final (P-LPD) ne prévoyait plus de sanctions pénales pour le non-respect de cette obligation. Cependant, le Conseil fédéral a proposé d'octroyer au PFPDT le pouvoir de rendre une décision avec menace de sanction pénale (art. 57 P-LPD).

Lors des débats parlementaires, aucune proposition de réintroduire des sanctions pénales pour le manquement au devoir d'informer n'a été faite. Par conséquent, le responsable du traitement qui n'informe pas le PFPDT ou les personnes concernées d'une violation de la sécurité ne risque aucune sanction pénale directe. Une seule exception subsiste: le PFPDT peut ordonner cette information sous menace de sanction pénale. L'art. 63 LPD prévoit que les personnes privées qui ne se conforment pas à une décision du PFPDT sous menace de peine peuvent être punies d'une amende jusqu'à CHF 250000[57].

V. Conclusion

En cas de violation de la sécurité des données, l'avocat peut devoir informer de cette violation le PFPDT ainsi que les personnes concernées.

L'avocat doit informer le PFPDT si la violation entraîne probablement un risque élevé pour les personnes concernées. Il doit dès lors procéder à un pronostic des potentielles conséquences de la violation ainsi que la probabilité qu'elles se réalisent.

L'avocat doit informer les personnes concernées si cela est nécessaire à leur protection. Il doit procéder à une analyse afin de déterminer si les personnes concernées sont plus aptes que lui-même à diminuer les potentielles

conséquences de la violation de la sécurité.

Le secret d'avocat ne s'oppose pas à l'information au PFPDT, mais peut s'opposer à l'information envers les personnes concernées. Vu que le client est maître du secret, le secret ne limite pas à l'information au client. Concernant l'information aux personnes concernées qui ne sont pas clientes, l'avocat doit examiner dans chaque cas si le fait d'annoncer la violation de la sécurité constitue nécessairement une révélation d'un fait soumis au secret. Si tel est le cas, le secret l'empêche d'informer la personne concernée. En revanche, si la personne concernée sait déjà que l'avocat traite ses données, l'information quant à la violation de la sécurité ne révèle aucun fait protégé par le secret. L'avocat doit ainsi l'informer de la violation.

Enfin, si l'avocat ne respecte pas son devoir d'informer, il ne risque aucune conséquence au niveau pénal, car la violation du devoir d'informer ne constitue pas un acte pénalement répréhensible. Cela étant, il n'est pas exclu qu'une telle violation puisse constituer une violation de l'art. 12 let. a LLCA[58].

---

1 Même la société FireEye, mondialement reconnue comme experte en cybersécurité, a été victime d'une cyberattaque (cf. New York Times, FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State, 8.12.2020 (›https://www.nytimes.com/2020/12/08/technology/fireeye-hacked-russians.html‹ >). Cette cyberattaque a permis à FireEye de découvrir une bien plus large cyberattaque, nommée SolarWinds en raison du nom de l'entreprise touchée (cf. not. l'annonce *[Form 8-K]* de SolarWinds à la SEC le 14.12.2020: ›https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm‹ >).

2 Pour un cas rendu public, au Royaume-Uni, cf. Hirsch Célian, L'étude d'avocats victime d'une cyberattaque, 21.4.2022 *in* swissprivacy.law/137.

3 Hirsch Célian, Le devoir d'informer lors d'une violation de la sécurité des données, Avec un regard particulier sur les données bancaires, Genève, thèse, 2023.

4 Hirsch (n. 3), p. 66.

5 Art. 4 ch. 12 RGPD; Hirsch (n. 3), p. 66 s.

6 Le Conseil fédéral admet expressément que la notion de «violation de la sécurité des données» au sens de la LPD correspond à celle de la «violation de données à caractère personnel» du RGPD (Conseil fédéral, Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15.9.2017, FF 2017 p. 6565 ss, p. 6642).

7 Art. 5 let. h LPD. En version allemande: *«eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden»;* en version italienne: *«violazione della sicurezza dei dati: qualsiasi violazione della sicurezza in seguito alla quale, in modo accidentale o illecito, dati personali vanno persi, sono cancellati, distrutti, modificati oppure divulgati o resi accessibili a persone non autorizzate».*

8 Cf. *infra* II.2.

9 GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES (G29), Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, adoptées le 3.10.2017 et révisées le 6.2.2018, p. 7; Mantz Reto, art. 4 RGPD N 178, in: Sydow Gernot/Marsch Nikolaus (édit.), Europäische Datenschutzgrundverordnung, Handkommentar, 3e éd., Baden-Baden 2022; Hirsch (n. 3), p. 85 s.

10 Conseil fédéral (n. 6), p. 6642 s.; Mantz (n. 9), art. 4 RGPD N 178; Comité européen de la protection des données (CEPD), Exemples concernant la notification de violations de données à caractère personnel, 14.12.2021, p. 28 N 85 ss; G29 (n. 9), p. 7; Hirsch (n. 3), p. 85 s.

11 Ces chiffres ont été obtenus sur demande auprès du PFPDT.

12 Ce terme est d'ailleurs utilisé dans le RGPD. Cf. ég. Métille Sylvain/Meyer Pauline, Annonce des violations de la sécurité des données: une nouvelle obligation de la nLPD, RSDA 2021, p. 25.

13 Cf. le principe d'intégrité ancré à l'art. 5 par. 1 let. f RGPD; G29 (n. 9), p. 8; Schreibauer Marcus/Spittka Jan, art. 33 RGPD N 16, in: Wybitul Tim (édit.), EU-Datenschutz-Grundverordnung, Handbuch, Francfort 2017; Métille/Meyer (n. 12), p. 24; Hirsch (n. 3), p. 86 s.

14 CEPD (n. 10), p. 9 N 17; Hirsch (n. 3), p. 86 s.

15 Hirsch (n. 3), p. 87.

16 Hirsch (n. 3), p. 88 ss.

17 Cf. CNIL, Délibération de la formation restreinte n° SAN -2021-020 du 28.12.2021 concernant la société SLIMPAY, par. 58, commenté in Hirsch Célian, Les données de douze millions de consommateurs en libre accès, 31.1.2022*in* ›www.swissprivacy.law/120.‹

18 Hirsch (n. 3), p. 87 s.

19 Consid. 39 RGPD; Mantz (n. 9), art. 4 RGPD N 179; Hirsch (n. 3), p. 88 ss.

20 Ces chiffres ont été obtenus sur demande auprès du PFPDT.

21 Cf. ég. PFPDT, Guide relatif aux mesures techniques et organisationnelles de la protection des données (TOM), 15.1.2024. Concernant la disctinction entre le principe de sécurité des données et la violation de la sécurité, cf. Hirsch (n. 3), p. 77 ss.

22 Cf. la version allemande: *«Der Verantwortliche meldet dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt»;* et italienne: *«Il titolare del trattamento comunica quanto prima all'IFPDT qualsiasi violazione della sicurezza dei dati personali che comporta verosimilmente un grave rischio per la personalità e i diritti fondamentali della persona interessata».*

23 Notamment le type et la sensibilité des données concernées.

24 Un tel risque peut exister même si la violation de la sécurité ne concerne qu'une seule personne.

25 G29 (n. 9), p. 28; Hirsch (n. 3), p. 147 s.

26 Hirsch (n. 3), p. 148.

27 *Id.*

28 Rosenthal David, Das neue Datenschutzgesetz, Jusletter 16.11.2020, N 153.

29 Art. 49 al. 3 LPD. Cf. ég. Conseil fédéral, Rapport du Conseil fédéral donnant suite au postulat 18.4100 de la CIP-N du 1er novembre 2018, 23.2.2022, FF 2022 776, p. 63 ss sur l'obligation de collaborer en droit administratif.

30 Hirsch (n. 3), p. 150.

31 Hirsch (n. 3), p. 247.

32 ›https://databreach.edoeb.admin.ch/report‹; Hirsch (n. 3), p. 326.

33 10% de ces annonces sont cependant des annonces erronées (spam, annonce test, fausse juridiction, saisies erronées).

34 Ces chiffres ont été obtenus sur demande auprès du PFPDT.

35 La LPD «vise à protéger la personnalité et les droits fondamentaux des personnes physiques dont les données personnelles font l'objet d'un traitement» (art. 1 LPD).

36 Cf. ég. la version allemande: *«Der Verantwortliche informiert die betroffene Person, wenn es zu ihrem Schutz erforderlich ist oder der Beauftragte es verlangt»;* et italienne: *«Il titolare del trattamento informa la persona interessata se è necessario per proteggerla o se lo richiede l'Incaricato».*

37 Hirsch (n. 3), p. 157 ss.

38 Hirsch (n. 3), p. 160 ss; cf. *contra* Bieri Adrian/Powell Julian, Meldung von Verletzungen der Datensicherheit, PJA 2021, p. 785. Cf. ég. CR LPD-Metille/Meyer, Art. 24 N 72 et PC LPD-Beguin/Vignieu, Art. 24 LPD N 47, qui s'appuient précisément sur Bieri/Powell pour soutenir la condition du risque élevé.

39 Hirsch (n. 3), p. 162 ss; dans le même sens, cf. Rosenthal (n. 28), N 166.

40 Cf. Hirsch (n. 3), p. 157 ss.

41 Kleiner Jan, Meldepflicht bei Datenschutzverletzungen, digma 2017, p. 175; Rosenthal (n. 28), N 162. Cf. ég. De Werra Jacques/Benhamou Yaniv, Cyberassurance: instrument utile pour la cybersécurité des entreprises?, Jusletter 24.8.2020, N 14.

42 Hirsch (n. 3), p. 164 ss.

43 Dix Alexander, art. 34 RGPD N 18, in: Simitis Spiros et al. (édit.), Datenschutzrecht, Baden-Baden 2019.

44 Hirsch (n. 3), p. 165; *contra* PC LPD-Beguin/Vignieu, Art. 24 LPD N 49, qui soutiennent, de façon peu convaincante, que le PFPDT pourrait ordonner au responsable du traitement d'informer les personnes concernées pour d'autres motifs dignes de protection, notamment en raison de «l'importance» de la violation de la sécurité.

45 Le PFPDT est rattaché administrativement à la Chancellerie fédérale (art. 43 al. 3 LPD) et les recours auprès du Tribunal administratif fédéral contre ses décisions sont ainsi recevables (art. 33 let. d LTAF).

46 Art. 63 LPD; cf. Hirsch (n. 3), p. 530 ss.

47 Le secret d'avocat ne peut par exemple pas être invoqué afin de s'opposer à un tel devoir d'informer (CR LPD-Metille/Meyer, Art. 24 N 63). Sur la non-application du principe *nemo tenetur* à l'encontre du PFPDT, cf. Hirsch (n. 3), p. 282 ss.

48 Hirsch (n. 3), p. 392 ss.

49 Art. 13 LLCA; art. 321 CP.

50 Hirsch (n. 3), p. 314. Il n'y aurait alors pas de «révélation» (CR CP IIChappuis, art. 321 CP N 75).

51 CR CP II-Chappuis, art. 321 CP N 75.

52 Concernant les informations à fournir aux personnes concernées selon le droit suisse, cf. art. 15 al. 3 OPDo; cf. ég. Hirsch (n. 3), p. 254 s.

53 Hirsch (n. 3), p. 314 s.

54 À titre de comparaison, la loi autrichienne sur la profession d'avocat prévoit expressément que le devoir d'informer selon l'art. 34 RGPD est limité lorsque *«das Recht des Rechtsanwalts auf Verschwiegenheit zur Sicherstellung des Schutzes der Partei (...) erfordert»*(§ 9 al. 4 de la *Rechtsanwaltsordnung*). Cf. ég. PC LPD-Béguin/Vignieu, 2023, Art. 24 LPD N 59.

55 Cf. not. la Synthèse des résultats de la procédure de consultation du 10.8.2017 par l'Office fédéral de la justice, p. 48 ›https://www.bj.admin.ch/dam/bj/fr/data/staat/gesetzgebung/datenschutzstaerkung/ve-ber-f.pdf.download.pdf/ve-ber-f.pdf‹>; Hirsch (n. 3), p. 530.

56 Conseil fédéral (n. 6), p. 6715. Sur les infractions pénales de la LPD, cf.Pahud Joël/Pittet Sébastien, Les infractions pénales de la LPD, Jusletter 25.9.2023; Hirsch (n. 3), p. 530.

57 Hirsch (n. 3), p. 531.

58 Dans ce sens, cf. Barth Tano, La maîtrise des faits par l'avocat, Devoirs et limites durant l'investigation, l'allégation et la présentation des moyens de preuve, thèse, Genève, 2022, p. 178 N 758.