Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence
PFPDT

Protection des données

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 06 février 2025, dernière mise à jour le 23 avril 2025 (Version 1.2)

Versions

Version 1.0	06.02.2025	Publication
Version 1.1	26.02.2025	Précisions linguistiques aux points 1.2 et 1.7
Version 1.2	23.04.2025	Nouveau point 1.2 Notification et précisions linguistiques dans le (nouveau) point 1.4 Droit d’annonce

Contenu

Conformément à son premier article, la loi sur la protection des données (LPD) vise à protéger la personnalité et les droits fondamentaux des personnes physiques dont les données font l'objet d'un traitement. L'art. 24 LPD règle les obligations des responsables du traitement et les droits des personnes concernées lorsqu'un tel traitement des données personnelles donne lieu à une violation de la sécurité des données. En vertu de l'art. 5, let. h LPD, on peut supposer qu'il y a violation de la sécurité des données lorsque des données personnelles sont perdues, effacées, détruites ou modifiées de manière accidentelle ou illicite ou sont divulguées ou rendues accessibles à des personnes non autorisées.

Les violations de la sécurité des données qui portent gravement atteinte au secret commercial, au secret de fabrication, au secret de fonction ou au secret professionnel, mais ne concernent pas des données personnelles n'entrent donc pas dans le champ d'application de l'art. 24 LPD. Cela vaut de la même façon pour les données qui se rapportent exclusivement à des personnes décédées et ne permettent pas de tirer des renseignements portant atteinte à la personnalité de personnes vivantes, étant donné que la personnalité finit par la mort conformément à l'art. 31, al. 1 CC.

Ce guide du PFPDT traite des conditions légales pour l'annonce des violations de la sécurité des données au PFPDT, en particulier de la notion de « risque vraisemblablement élevé » de l'art. 24 al. 1 LPD. Il définit également les conditions d'information des personnes concernées en cas de violation de la sécurité des données selon l'art. 24 al. 4 LPD.

1 Annonces des violations de la sécurité des données au PFPDT

1.1 Objet de l'annonce

L'annonce a pour objet de dépeindre des faits et des appréciations avec lesquels le responsable du traitement décrit la violation de la sécurité des données au PFPDT, en l'informant notamment de la nature, du moment, de la durée et de l'étendue de la violation et de ses conséquences déjà connues ou redoutées pour les personnes concernées. L'art. 15, al. 1 de l'ordonnance sur la protection des données (OPDo) énumère les informations nécessaires permettant, le cas échéant, au PFPDT de prendre les mesures qui s'imposent au profit des personnes concernées par la violation de la sécurité des données, en donnant p. ex. l'ordre de les informer de l'incident (voir le point 2 ci-après).

1.2 Notification

Il incombe au responsable du traitement de signaler les violations au PFPDT (et d'informer les personnes concernées). Le sous-traitant est quant à lui tenu d'informer le ou les responsables du traitement de toute violation de la sécurité des données. Ce devoir d'informer n'est pas lié à une évaluation des risques comme prévu à l'art. 24, al. 1, LPD ; le sous-traitant doit informer le responsable du traitement de toute violation de la sécurité des données, qu'elle soit susceptible ou non d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

1.3 Obligation d'annoncer

En vertu de l'art. 24, al. 1 LPD, le responsable du traitement est tenu d'annoncer 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. Si l'analyse des risques réalisée dans le cadre des délais serrés d'une violation de la sécurité des données révèle qu'un tel risque élevé existe vraisemblablement ou qu'il ne peut être déterminé avec certitude dans ce court délai (concernant la question du risque, voir le point 1.5 ci-après), le responsable du traitement doit communiquer la violation de la sécurité des données au PFPDT. Par exemple, dans le cas d'une attaque par rançongiciel, une première analyse devra, selon les circonstances, supposer un « risque vraisemblablement élevé ». Selon la loi, le responsable doit signaler l'incident « le plus rapidement possible » et ne peut donc pas attendre dans de tels cas que des clarifications plus longues soient effectuées, qui pourraient confirmer ou exclure sans aucun doute le risque vraisemblablement élevé

L'annonce obligatoire doit contenir toutes les informations énumérées à l'art. 15, al. 1 OPDo, sachant que les annonces ultérieures sont également autorisées dans les conditions prévues à l'al. 2 (voir point 1.4 ci-après).

Si le responsable du traitement omet d'adresser cette annonce au PFPDT, celui-ci peut, après avoir pris connaissance de l'incident par un autre moyen, lui ordonner de réparer cette omission (art. 51, al. 3, let. f LPD).

Après réception de l'annonce, le PFPDT 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 (voir art. 15, al. 1, let. f OPDo) paraissent appropriées, suffisantes et opportunes. Si nécessaire, le PFPDT lui demandera dans un premier temps d'apporter des précisions concernant les faits et appréciations décrits et de modifier ou de compléter les mesures prises ou prévues. Le cas échéant, le PFPDT entrera également en contact avec le responsable du traitement afin de s'assurer que l'incident est documenté p. ex. par la sauvegarde de procès-verbaux de journalisation. Il examine en outre si les personnes concernées sont informées de l'incident et de ses conséquences de façon appropriée (voir art. 15, al. 3 et 4 OPDo). Si le responsable du traitement ne se conforme pas aux demandes du PFPDT, ce dernier peut ouvrir une enquête formelle conformément à l'art. 49 LPD et faire appliquer les demandes par des mesures conformément à l'art. 51 LPD.

S'il en va de l'intérêt général, le PFPDT peut également informer le public de ses constatations et de ses décisions sur la base de l'art. 57, al. 2 LPD.

1.4 Droit d'annoncer

La pratique a montré que les responsables du traitement veulent parfois annoncer au PFPDT des violations de la sécurité des données qui ne présentent pas de risque élevé. Le PFPDT enregistre également ces annonces de violation de la sécurité des données qui lui sont adressées spontanément. Celles-ci s'avèrent particulièrement pertinentes pour toutes les parties prenantes, mais également utiles du point de vue de l'intérêt public dans les cas où l'analyse des risques présente un risque faible sur la base des données concernées, mais serait par exemple en mesure de susciter un grand intérêt médiatique en raison du nombre élevé de personnes concernées (voir point 1.5 ci-après).

Après examen succinct de l'annonce, le PFPDT décide s'il ordonne ou prend lui-même d'éventuelles mesures d'information des personnes concernées ou du grand public.

1.5 Dépôt d'annonces

Les annonces doivent être adressées au PFPDT dans les meilleurs délais et être formulées de façon à refléter de la manière la plus complète possible les circonstances qui sous-tendent la violation de la sécurité des données et ses conséquences. Si le responsable du traitement n'est pas en mesure d'annoncer simultanément toutes les informations, il fournit les informations manquantes dans les meilleurs délais (voir art. 15, al. 2 OPDo).

Pour les annonces obligatoires, le PFPDT met un portail d'annonce (databreach.edoeb.admin.ch) à disposition. Le portail d'annonce garantit la transmission sécurisée des données au PFPDT. Le formulaire interactif garantit également que l'annonce contient l'ensemble des informations énumérées à l'art. 15, al. 1 OPDo et que l'obligation d'annoncer est ainsi remplie correctement. Le portail d'annonce délivre en outre une confirmation du moment de l'annonce et permet d'adresser des annonces ultérieures à tout moment pour compléter l'annonce initiale.

Les annonces spontanées s'effectuent quant à elles en dehors du portail d'annonce et n'entraînent pas d'office des actions du PFPDT, comme vu plus haut.

1.6 Risque élevé en vertu de l'art. 24, al. 1 LPD

En vertu de l'art. 24, al. 1 LPD, le responsable du traitement est tenu d'annoncer 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.

La LPD utilise la notion de « risque élevé » ainsi que de « risque vraisemblablement élevé » dans un grand nombre de dispositions. Lors de l'interprétation du « risque élevé », il convient de tenir dûment compte des différentes finalités de ces dispositions.

Lors de l'évaluation du risque élevé en vertu de l'art. 24, al. 1 LPD, les responsables du traitement doivent en premier lieu clarifier dans quelle mesure la violation de la sécurité des données a déjà entraîné des atteintes à la personnalité ou aux droits fondamentaux de personnes physiques. Deuxièmement, ils s'appuient sur le critère de « vraisemblance » mentionné dans la loi pour intégrer également dans l'évaluation de leur obligation d'annoncer les conséquences de la violation de la sécurité des données pour les personnes potentiellement concernées qui ne sont ni mesurables de manière définitive, ni prévisibles de manière certaine au moment de ladite évaluation.

Le risque vraisemblablement élevé en vertu de l'art. 24, al. 1 LPD doit être identifié sans tenir compte des mesures que le responsable du traitement ne prévoit, n'annonce ou n'a ordonnées qu'après la violation de la sécurité des données. – Jusqu'à présent dans la pratique du PFPDT, il a en revanche été possible de tenir compte, lors de l'évaluation du risque, de mesures d'urgence que le responsable du traitement a pu prendre avant même d'adresser l'annonce respectant les délais et dont il a été prouvé qu'elles ont exclu ou réduit les conséquences redoutées d'une potentielle atteinte à la personnalité. Par exemple, lorsque le responsable du traitement a rapidement repris le contrôle de bases de données personnelles inaccessibles à court terme grâce aux mesures d'urgence prises et a pu exclure tout traitement inapproprié de ces données en quelques heures avec une probabilité suffisante à l'aide de procès-verbaux de journalisation ou d'autres indices. Toutefois, en cas de doute quant à l'exclusion de la survenue d'un risque élevé avec une probabilité suffisante, les responsables du traitement ne doivent pas attendre pour s'acquitter de leur obligation d'annoncer. Une obligation d'annoncer doit donc p. ex. être remplie avant que le responsable du traitement soit, avant ou après paiement d'une rançon, dans l'incertitude quant à la façon dont des données personnelles récupérées pourraient avoir été traitées par des cybercriminels.

Les critères pour l'évaluation du niveau du risque vraisemblable résultant de la violation de la sécurité des données sont les suivants :

1.6.1 Gravité des conséquences :

Il convient en premier lieu d'évaluer la gravité des atteintes déjà survenues ou redoutées à la personnalité ou aux droits fondamentaux des personnes physiques concernées par la violation de la sécurité des données. Dans ce cadre, l'intensité de l'atteinte portée aux personnes les plus touchées est déterminante. Les critères suivants peuvent être envisagés lors de l'évaluation de la gravité des conséquences :

- Degré de protection des données personnelles concernées : la nature des données personnelles concernées par la violation de la sécurité des données est un aspect central de l'examen. Plus ces données sont sensibles, plus le risque que les personnes concernées aient fait l'objet d'une violation de leur personnalité ou de leurs droits fondamentaux est élevé. Si des données personnelles sensibles au sens de l'art. 5, let. c LPD sont concernées, p. ex. données de santé, données biométriques ou données sur l'aide sociale, on peut dans de nombreux cas tabler sur un risque élevé. Mais les données qui n'entrent pas dans cette catégorie peuvent également signifier automatiquement un risque élevé, par exemple la perte de (copies de) documents d'identité ou les données de la carte de crédit. Selon le contexte dans lequel les données personnelles concernées par une violation de la sécurité des données sont traitées, il faut donc également tabler sur un « risque vraisemblablement élevé » lorsqu'il s'agit de données personnelles non sensibles. Par exemple lorsque des données de contact ou d'adresse concernées par une violation de la sécurité des données ont été traitées par la personne autorisée à des fins de poursuite pénale ou de mesures d'aide sociale dans le cadre desquelles des données sensibles au sens de l'art. 5, let. c LPD sont régulièrement produites. Si les données personnelles concernées étaient déjà accessibles au public avant la violation de la sécurité des données, le risque ne doit généralement pas être considéré comme élevé.

- Nature et circonstances de la violation ainsi que cercle et motivations des tiers non autorisés : concernant l'évaluation du risque, le fait qu'une erreur humaine, une intention criminelle ou un problème technique ait entraîné une violation de la sécurité des données peut faire une différence. L'évaluation du risque peut être différente selon la cause. Cependant, si des données personnelles disparues deviennent p. ex. accessibles à un large public via une publication sur le darknet, cela conduit à une évaluation du risque ayant tendance à être élevée, et ce, que les données soient parvenues jusque-là du fait d'un problème technique ou d'un acte criminel. La suppression de données personnelles sur le serveur du responsable du traitement imputée à une simple intention de nuire peut en revanche indiquer un risque plus faible. Une confiance subjective des responsables du traitement dans les bonnes intentions de destinataires de données inconnus ne peut toutefois pas exclure un risque objectivement élevé si elle n'est pas justifiée en détail.
- Efforts déployés pour identifier des personnes : autre indicateur pour l'évaluation du risque : les efforts en termes de travail et de moyens financiers qu'il a fallu déployer pour traiter des informations obtenues de manière illicite et éventuellement rendues accessibles à un large public, p. ex. via le darknet, de façon à ce qu'il devienne possible de remonter à des personnes identifiables. Plus il est facile de déduire l'identité d'une personne donnée à partir des données obtenues de manière illicite, plus le risque est élevé pour cette personne. Si par exemple « seul » un numéro de client disparaît sans que d'autres données permettant de faire le lien entre le numéro de client et la personne soient disponibles, le risque est plus faible que lorsque des adresses e-mail éloquentes (prénom.nom@XXXX.com) sont concernées. Si des données personnelles concernées par une violation de la sécurité des données ont été cryptées efficacement par le responsable du traitement, elles restent illisibles pour toutes les personnes qui ne possèdent pas la clé. Du point de vue du droit de la protection des données, de telles données sont donc considérées comme anonymes pour tous les tiers ne disposant pas d'accès, raison pour laquelle l'obligation d'annoncer en vertu de l'art. 24, al. 1 LPD ne s'applique pas. En revanche, les données concernées par une violation de la sécurité des données qui ont seulement été pseudonymisées sont considérées comme des données personnelles qui peuvent, le cas échéant, entraîner une obligation d'annoncer en vertu de cette disposition.
- Volume et durée de traitement : le volume et la durée de traitement des informations concernées par une violation de la sécurité des données relatives à une même personne peuvent être un facteur déterminant pour évaluer l'intensité.
- Préjudice moral et économique : on peut tabler sur des conséquences graves pour les différentes personnes concernées lorsqu'une violation de la sécurité des données permet des abus comme l'usurpation d'identité ou la fraude à la carte bancaire entraînant des préjudices comme l'atteinte à la réputation, la discrimination ou des dommages économiques, qui causent des torts portant atteinte à la personnalité des personnes concernées, comme du souci ou de l'anxiété.
- Personnes vulnérables : si une violation de la sécurité des données concerne par exemple des données de personnes mineures ou handicapées, cela peut également indiquer des conséquences graves.
- Volume total de personnes et de données concernées par la violation de la sécurité des données : un grand nombre de personnes concernées ou de grands volumes de données personnelles ne suffisent pas à affirmer que le risque est élevé. En cas de violation de la sécurité des données avec un grand nombre de personnes concernées, un intérêt public et privé par rapport à leur information peut néanmoins exister. Dans la pratique, il s'avère également qu'il n'est pas rare que les responsables du traitement annoncent spontanément de telles violations de la sécurité des données au PFPDT (voir point 1.3).

1.6.2 Probabilité de conséquences redoutées :

Après qu'une violation de la sécurité des données est survenue et a été identifiée par le responsable du traitement, il s'agit pour lui d'évaluer la probabilité que des conséquences de la violation de la sécurité des données qui n'ont pas encore été évaluées de manière définitive ou qui ne sont pas encore survenues atteignent effectivement le potentiel d'atteinte redouté pour la plupart des personnes concernées. Ce potentiel devra, pour un hôpital concerné par une violation de la sécurité des données

qui, outre des données factuelles administratives et scientifiques, traite un grand nombre de données personnelles sensibles, être estimé à un niveau plus élevé que pour un distributeur de denrées alimentaires, par exemple. En conséquence, un hôpital concerné ne doit pas attendre d'être sûr que la violation de la sécurité des données ait touché non seulement des informations factuelles, mais aussi des données de patientes et de patients pour annoncer ladite violation au PFPDT. Lors de l'évaluation de la probabilité de survenue de conséquences redoutées, les mesures que les responsables du traitement n'ont prévues, annoncées ou introduites qu'après la survenue de la violation de la sécurité des données doivent être occultées. En d'autres termes, les responsables du traitement ne doivent pas attendre la réalisation et l'évaluation de futures mesures pour informer le PFPDT d'une violation de la sécurité des données soumise à l'obligation d'annoncer en raison du potentiel d'atteinte élevé.

1.7 Annonces de violations de la sécurité des données au PFPDT et principe de la transparence

L'activité du PFPDT en tant qu'autorité de surveillance de la Confédération pour la protection des données est soumise à la loi fédérale sur le principe de la transparence dans l'administration (loi sur la transparence, LTrans ; RS 152.3). Les annonces des responsables du traitement, quelle que soit la forme qu'elles prennent, ainsi que les éventuels échanges entre le PFPDT et le responsable du traitement ou ses sous-traitants doivent en principe être considérés comme des documents officiels au sens de la LTrans. Les documents officiels résultant du traitement de cas de violation de la sécurité des données par le PFPDT dans l'exercice de ses missions légales sont donc en principe accessibles au public en vertu de la LTrans. Cela vaut notamment pour toutes les annonces de violations de la sécurité des données, qu'elles aient été effectuées spontanément ou dans le cadre de l'obligation d'annoncer prévue à l'art. 24, al. 1 LPD. Dans le cadre du traitement de demandes d'accès en vertu de la LTrans, le PFPDT examine si et dans quelle mesure un éventuel accès est limité ou différé, sur la base des dispositions d'exception de l'art. 7 ss LTrans. Dans le cadre de la procédure, le PFPDT doit, le cas échéant, entendre les tiers concernés au préalable. Il statue sur l'accès au moyen d'une prise de position ainsi que, sur demande, au moyen d'une décision. Il n'est pas réalisé de procédure de médiation au sens de l'art. 13 LTrans (voir à ce sujet l'arrêt du Tribunal administratif fédéral A-4781/2019 du 17 juin 2020, consid. 3).

1.8 Obligation d'annoncer et sanctions

Dans le cas où le responsable du traitement aurait dû informer le PFPDT des violations de la sécurité des données en vertu de l'art. 24, al. 1 LPD, mais a omis de le faire, le PFPDT peut, après avoir pris connaissance de l'incident par un autre moyen, lui ordonner de réparer cette omission (art. 51, al. 3, let. f LPD). Le PFPDT peut également ordonner d'autres mesures administratives dans le cadre d'une violation de la sécurité des données, p. ex. lorsque les exigences de l'art. 8 LPD n'ont pas été respectées.

Le non-respect total ou partiel de l'obligation d'annoncer en soi n'est pas passible de sanction en vertu de la LPD. Mais une violation de la sécurité des données peut relever du droit pénal lorsque le responsable du traitement n'a p. ex. pas respecté les exigences minimales en matière de sécurité des données (art. 61, let. c LPD). L'art. 24, al. 6 LPD prévoit à cet égard que les annonces obligatoires ne peuvent pas être utilisées dans le cadre d'une procédure pénale sans le consentement de la personne tenue d'annoncer. Cela vaut également pour les annonces spontanées (voir notamment Basler Kommentar Datenschutzgesetz, 4. Auflage [BSK] Art. 24 N 98 avec renvoi à MÉTILLE/MEYER, in Meier/Métille (éditeurs), Commentaire romand, Loi fédérale sur la protection des données, Bâle 2023, art. 24 N 35).

2 Information des personnes concernées par la violation de la sécurité des données

L'obligation d'annoncer du responsable du traitement en vertu de l'art. 24, al. 1 LPD est à distinguer de son obligation d'informer les personnes concernées par la violation de la sécurité des données. En vertu de l'art. 24, al. 4 LPD, le responsable du traitement doit informer les personnes concernées de la violation de la sécurité des données lorsque cela est nécessaire à la protection de ces personnes ou lorsque le PFPDT l'exige.

L'obligation d'informer les personnes concernées au sens de l'al. 4 doit être interprétée indépendamment de l'al. 1 et de la notion de risque élevé qui y est utilisée (voir MATHYS/THOMANN, in Vasella/Blechta (Hrsg.), BSK Art. 24 N 63).

Si le responsable du traitement peut établir de manière plausible que les personnes concernées ont, sans information complémentaire, déjà été suffisamment informées d'une violation de la sécurité des données et de ses conséquences et savent quelles mesures elles peuvent ou doivent prendre de leur côté pour se protéger, l'obligation d'informer peut être considérée comme respectée.

2.1 Obligation d'informer en raison du besoin de protection des personnes concernées

Le besoin de protection mentionné à l'art. 24, al. 4 LPD pour les personnes concernées doit être présumé lorsque celles-ci peuvent ou doivent prendre elles-mêmes des mesures pour réduire ou éviter un dommage résultant d'une violation de la sécurité des données. Par exemple lorsqu'elles doivent modifier des données d'accès ou des mots de passe (voir le message concernant la LPD révisée, FF 2017 6565 ss, 6682). Mais le besoin de protection des personnes concernées peut également exister dans d'autres cas, p. ex. lorsque des cartes de crédit doivent être bloquées, que des relevés de compte ou des messages et des demandes, c'est-à-dire des e-mails de phishing, doivent faire l'objet d'un examen critique (voir MATHYS/THOMANN, BSK, Art. 24 N 67).

Le « risque vraisemblablement élevé » au sens de l'art. 24, al. 1 LPD, qui déclenche l'obligation d'annoncer du responsable du traitement vis-à-vis du PFPDT, n'est pas une condition juridique pour la justification d'une obligation d'informer les personnes concernées en vertu de l'al. 4 de cette disposition. Une telle obligation d'informer peut en particulier également exister lorsque le responsable du traitement peut exclure avec des arguments raisonnables un risque objectivement élevé sur la base de ses connaissances d'initié, mais que les personnes potentiellement concernées par une violation de la sécurité des données s'attendent, dans l'ignorance de la situation, au pire. À l'inverse, la présence d'un risque vraisemblablement élevé au sens de l'art. 24, al. 1 LPD indiquera généralement également une obligation d'informer en vertu de l'al. 4 de cette disposition.

2.2 Obligation d'informer en raison d'un ordre du PFPDT

Le PFPDT peut exiger du responsable du traitement qu'il informe les personnes concernées en vertu de l'art. 24, al. 4 LPD. Le PFPDT peut prononcer une telle demande, que le responsable du traitement lui ait préalablement communiqué la violation spontanément ou en tant qu'annonce obligatoire en vertu de l'art. 24, al. 1 LPD ou qu'il ne la lui ait pas notifiée du tout.

Le PFPDT exigera du responsable du traitement qu'il informe les parties prenantes s'il estime que le besoin de protection des personnes concernées par la violation de la sécurité des données l'exige. Mais il peut également l'exiger parce qu'il est d'avis qu'en raison du grand nombre de personnes concernées ou d'une couverture médiatique, il existe un intérêt public à ce que les responsables du traitement fournissent des informations détaillées et appropriées sur les conséquences d'une violation de la sécurité des données au grand nombre de personnes concernées, et donc indirectement également à un large public. Un tel intérêt peut en particulier exister lorsque des conséquences qui ont inspiré des inquiétudes et donné lieu à des spéculations dans un large public peuvent être évitées ou atténuées de manière déterminante. Dans la pratique, il n'est pas rare que dans de tels cas, les responsables du traitement décident d'adresser des annonces spontanées au PFPDT, ce que ce dernier salue (voir à ce sujet le point 1.3 Droit d'annoncer ci-dessus).

En principe, le PFPDT a dans ces cas-là la compétence, sur la base de l'art. 57, al. 2 LPD, d'informer le public de ses constatations à cet égard, étant donné qu'il s'agit là d'un cas d'intérêt général. Mais l'information autonome des personnes concernées par le responsable du traitement lui-même est généralement plus efficace.

2.3 Réalisation de l'information

Les personnes concernées doivent être informées dans un « langage simple et compréhensible » conformément à l'art. 15, al. 3 OPDo et contenir au moins les informations suivantes : la nature de la violation, c'est-à-dire ce qui s'est passé, les conséquences de la violation, y compris les risques pour les personnes concernées, les mesures prises ou prévues pour, d'une part, remédier à cette défaillance et,

d’autre part, atténuer les conséquences. Le nom et les coordonnées d’une personne de contact doivent également être fournis.

De plus, il n’y a pas de prescriptions concernant la forme de l’information, et le responsable du traitement doit choisir la méthode appropriée lui-même.

En principe, les personnes concernées doivent être informées directement et individuellement. Une information par une communication publique est possible à titre exceptionnel en vertu de l’art. 24, al. 5, let. c LPD lorsque l’information des différentes personnes concernées peut dans ce cadre être garantie de manière équivalente. L’obligation d’informer n’est pas levée par la communication publique, mais seulement modifiée (voir CÉLIAN HIRSCH, Le devoir d’informer lors d’une violation de la sécurité des données. Avec un regard particulier sur les données bancaires, Genève 2023, p. 315).

2.4 Obligation d’informer et sanctions

Dans le cas où le responsable du traitement aurait dû informer les personnes concernées d’une violation de la sécurité des données du fait de leur besoin de protection ou à la demande du PFPDT en vertu de l’art. 24, al. 4 LPD, mais a omis ou refusé de le faire, le PFPDT peut lui ordonner de réparer cette défaillance (art. 51, al. 3, let. f LPD). Le PFPDT peut également ordonner d’autres mesures administratives dans le cadre d’une violation de la sécurité des données, p. ex. lorsque les exigences de l’art. 8 LPD n’ont pas été respectées.