ARTISET

Guide pour la mise en œuvre de la protection des données

Mesures à prendre par les institutions et les structures pour personnes ayant besoin de soutien

1. Introduction

Dans le cadre de l'entrée en vigueur, le 1er septembre 2023, de la loi fédérale totalement révisée sur la protection des données (LPD), un grand nombre d'entreprises et d'organisations sont tenues de prendre des mesures techniques et organisationnelles pour satisfaire aux nouvelles exigences, plus strictes. Le présent document a pour objectif de guider les institutions et les structures pour personnes ayant besoin de soutien dans cette démarche.

Toutes les informations du présent document relatives aux dispositions des lois et ordonnances sur la protection des données se réfèrent à leurs versions révisées, qui entrent en vigueur le 1er septembre 2023, soit:

- Nouvelle loi fédérale sur la protection des données («LPD»)
- Nouvelle ordonnance sur la protection des données («OPDo»)

Dans le présent document, l'expression «établissement» désigne des dresser un état des lieux ns et les structures pour personnes ayant besoin de soutien (personnes âgées, personnes en situation de handicap, enfants et adolescents ayant des besoins spécifiques).

2. État des lieux

Chaque établissement devrait commencer par dresser un état des lieux **de ses saisies et collectes de données personnelles**. La fédération ARTISET met à disposition sur son site internet une telle **check-list** susceptible d'être utile à cet effet. Ladite liste vise à fournir un aperçu du type et de l'étendue de la nécessité d'agir au sein de l'établissement en matière de protection des données.

3. Concept de protection des données

Il est conseillé d'adopter un concept de protection des données à l'aide du **modèle de concept de protection des données** mis à disposition par ARTISET, et ce, même si l'élaboration d'un tel concept n'est pas exigée par la loi. Un concept de protection des données tient compte de l'importance de la protection des données pour le respect de la sphère privée et des droits de la personnalité des bénéficiaires des prestations, respectivement des résident·e·s, des employé·e·s et, le cas échéant, des partenaires commerciaux de l'établissement concernée. Le **but principal** d'un tel concept est de garantir la protection de la personnalité des personnes physiques contre tout traitement illicite ou disproportionné de données personnelles. Le concept doit donc, en tant que directive, aider les personnes travaillant pour l'établissement à adopter un comportement adéquat dans le respect du droit de la protection des données. L'élaboration d'un tel instrument est facultative; la loi n'exige en effet pas sa mise sur pied.

ARTISET

Zieglerstrasse 53, 3007 Berne
Tél. +41 31 385 33 33
info@artiset.ch, artiset.ch

Föderation der Dienstleister
für Menschen mit Unterstützungsbedarf

Il est en outre recommandé d'inviter les personnes et sociétés externes en contact avec l'établissement dans le cadre de leurs affaires à s'engager par écrit à respecter le concept de protection des données de l'établissement.

4. Cahier des charges de la / du responsable du traitement des données

Chaque établissement doit désigner un·e «responsable du traitement» des données personnelles. Celui-ci/Celle-ci peut être un collaborateur ou une collaboratrice de l'établissement ou une personne externe – même une personne morale (par exemple une fiduciaire). Il/elle décide de la finalité et des moyens du traitement des données personnelles dans l'établissement (cf. art. 5 let. j LPD). Il/elle peut déléguer des tâches à des «sous-traitant·e·s» (cf. art. 5 let. k LPD).

Les différentes obligations de la / du responsable du traitement au sein d'un établissement sont définies dans la loi et l'ordonnance sur la protection des données (cf. notamment art. 5 let. j LPD). Il est de ce fait judicieux de créer un cahier des charges de la/du responsable du traitement des données. Cela permet de maintenir un aperçu clair et synthétique de ses obligations. ARTISET met à cet effet un **modèle** à disposition.

5. Registres des activités de traitement

La création d'un ou de plusieurs registre(s) des activités de traitement n'est pas obligatoire pour les établissements employant moins de 250 personnes (cf. art. 12 LPD et art. 24 OPDo), mais elle est dans tous les cas judicieuse. Pour que de tels documents prennent tout leur sens, il faut aussi les actualiser en permanence, ou du moins à intervalles réguliers. ARTISET fournit un **modèle** à cet effet.

6. Collectes de données personnelles: accès et actualisation

Il est conseillé de définir par écrit qui, dans l'établissement, a accès à quelles données personnelles et d'aménager les autorisations d'accès correspondantes (mots de passe pour le classement électronique, clés pour le classement papier).

Il est également conseillé de définir par écrit qui doit indiquer au/ à la responsable du traitement des données dans l'établissement quelles collectes de données personnelles ont subi des modifications de contenu pour que celui-ci/celle-ci ou une personne mandatée par lui/elle actualise les registres des activités de traitement des données correspondants.

7. Mesures de protection techniques et organisationnelles

Il est conseillé de mettre en œuvre les mesures nécessaires pour garantir la protection des données de l'établissement en procédant à des reconfigurations techniques («Privacy by Design») et des configurations par défaut («Privacy by Default» ; cf. art. 7 LPD, art. 3 OPDo). La sécurité des données doit être garantie par ce biais (cf. art. 8 LPD). Des contrôles d'accès et de supports de données personnelles doivent empêcher que des personnes non autorisées accèdent à des stocks de données, les modifient, les détruisent ou les volent.

Étant donné l'évolution constante de la technique, la nouvelle législation sur la protection des données se garde délibérément d'imposer des solutions techniques déterminées: la loi se contente d'exiger des établissements qu'ils mettent en place des mesures techniques et organisationnelles afin que le traitement respecte les prescriptions de protection des données (art. 7 al. 1 LPD).

Les mesures correspondantes doivent être appropriées au regard notamment de l'état de la technique, du type de traitement et de son étendue, ainsi que du risque que le traitement des données présente pour la personnalité ou les droits fondamentaux des personnes concernées (art. 7 al. 2 LPD). Une sécurité des données adaptée au risque doit être garantie (art. 8 al. 1 LPD).

L'utilisation d'adresses HIN (cryptées) pour les e-mail contenant des données personnelles sensibles est par exemple une bonne chose. On ne saurait cependant affirmer sans autre qu'un trafic par des canaux classiques de transmission des e-mail serait inadmissible. Mais avec l'utilisation d'adresses HIN, on améliore sans aucun doute la sécurité.

La protection des données personnelles traitées électroniquement doit être assurée par l'utilisation des moyens suivants:

- cryptage;
- mise en place de de pare-feux, de logiciels antivirus et d'adresses HIN pour les e-mail contenant des données sensibles;
- éventuelle mise en œuvre d'autres mesures techniques de protection;
- établissement de protocoles d'accès.

8. Consentement à la collecte et au traitement des données

En principe, la personne concernée doit être informée par le/la responsable de la protection des données de la collecte de données personnelles la concernant (art. 19 al. 1 LPD ; il existe toutefois des exceptions, voir chapitre suivant). Ce devoir d'information s'applique également lorsque les données ne sont pas collectées auprès de la personne concernée. En outre, les données personnelles ne peuvent être collectées et traitées que dans un but précis et reconnaissable par la personne concernée (art. 6 al. 3 LPD). En outre, le traitement de données personnelles ne peut pas avoir lieu si la personne concernée s'y oppose expressément (art. 30 al. 2 let. b LPD a contrario).

Il ressort de cette interaction de dispositions légales que la personne concernée doit être informée à l'avance des buts de l'utilisation (et donc des traitements prévus) de ses données personnelles. La manière dont leur consentement est recueilli ne doit pas revêtir une forme particulière (en soi, un simple signe suffit.

Le traitement de *données personnelles sensibles* (telles que des informations sur l'état de santé) requiert cependant le consentement exprès de la personne concernée (cf. art. 6, al. 7, let. a, LPD).

En règle générale, il n'y a pas atteinte à la personnalité lorsque la personne concernée a rendu les données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement (cf. art. 30, al. 3, LPD).

9. Obligation d'information de l'établissement

Pour permettre au / à la responsable du traitement des données et aux services concernés au sein de l'établissement de se conformer à leur obligation d'informer, au sens des art. 19-20 LPD et 13 OPDo, les bénéficiaires de leurs prestations, leurs partenaires commerciaux et leur personnel, il est conseillé de prévoir le respect des étapes/limites suivantes au moyen de directives:

- Lorsque l'établissement collecte des données personnelles, la/le responsable du traitement des données en informe la personne concernée, et ce, même lorsque lesdites données ne sont pas collectées auprès de cette personne.
- La/le responsable du traitement des données est tenu·e par la loi d'indiquer à la personne dont les données sont collectées au moins:

- l'identité et les coordonnées de la/du responsable du traitement des données;
- la finalité du traitement;
- éventuellement, les destinataires ou les catégories de destinataires dont les données personnelles sont communiquées;
- les catégories de données personnelles traitées, dans la mesure où les données ne sont pas collectées auprès de la personne concernée;
- l'État ou l'organisme international auquel / à laquelle les données personnelles sont communiquées et, le cas échéant, les garanties prévues à l'art. 16 al. 2 LPD ou l'application de l'une des exceptions prévues à l'art. 17 LPD, si lesdites données sont communiquées à l'étranger.

Les modalités suivantes doivent en outre être respectées :

- Si les données ne sont pas collectées auprès de la personne concernée, la/le responsable du traitement des données doit lui communiquer lesdites informations au plus tard un mois après obtention desdites données.
- Si la/le responsable du traitement des données communique les données personnelles avant l'échéance de ce délai, elle/il en informe la personne concernée au plus tard lors de la communication.
- La/Le responsable du traitement est délié·e du devoir d'information si:
  - la personne concernée dispose déjà des informations correspondantes;
  - le traitement est prévu par la loi;
  - la/le responsable du traitement des données est soumis·e à une obligation légale de garder le secret.
- Lorsque les données personnelles ne sont pas collectées auprès de la personne concernée, le devoir d'information ne vaut pas dans les cas suivants:
  - l'information est impossible à donner;
  - la transmission de l'information nécessite des efforts disproportionnés.
- La/Le responsable du traitement des données peut en outre limiter ou différer la communication des informations, ou y renoncer, dans les cas suivants:
  - les intérêts prépondérants de tiers l'exigent;
  - l'information empêche le traitement d'atteindre sa finalité;
  - les intérêts prépondérants de la/du responsable du traitement des données l'exigent;
  - les données personnelles ne sont pas communiquées à des tiers (nota bene: les établissements appartenant à un même groupe ne sont, dans ce cadre, pas considérées comme des tiers).

10. Droit de consultation et d'accès des personnes concernées

Pour permettre aux personnes dont les données sont traitées par l'établissement («personnes concernées») de faire valoir leurs droits de consultation et d'accès conformément aux art. 25-26 LPD et 16-19 OPDo, il est conseillé de prévoir le respect des étapes / limites suivantes au moyen de directives:

- Tout un chacun peut demander à la/au responsable du traitement des données si des données personnelles la concernant sont traitées.
- La personne concernée obtient les informations nécessaires pour lui permettre de faire valoir ses droits et pour garantir la transparence du traitement. Les informations suivantes doivent dans tous les cas lui être communiquées:
  - identité et coordonnées de la / du responsable du traitement des données;
  - données personnelles traitées;
  - personnes impliquées dans la collecte;
  - le cas échéant: destinataires des données;

  - finalité du traitement des données personnelles;
  - durée de conservation des données personnelles ou, si cela n'est pas possible, critères permettant de fixer cette durée;
  - renseignements disponibles sur la provenance des données personnelles, si les données n'ont pas été collectées auprès de la personne concernée.
- L'établissement doit fournir l'information dans les 30 jours, d'une manière qui puisse être comprise facilement et par écrit.
- Si la fourniture de l'information n'occasionne pas d'efforts disproportionnés, elle doit intervenir gratuitement.
- Les données dont le traitement est illicite ou incorrect ou dont le contenu est erroné doivent être corrigées ou détruites par l'établissement.
- Chaque personne concernée peut faire bloquer la communication de ses données si elle justifie d'un intérêt légitime.
- L'existence éventuelle d'une décision individuelle automatisée est communiquée à la personne concernée ainsi que la logique ayant présidé à ladite décision (en pratique, il est cependant très rare que les établissements prennent des décisions individuelles automatisées).
- La personne concernée est informée des destinataires ou des catégories de destinataires auxquel·le·s ses données personnelles sont le cas échéant communiquées.
- Si les données personnelles sont communiquées à l'étranger:
  - informations mentionnées à l'art. 19 al. 4 LPD;
  - État ou organisme international concerné auquel elles sont communiquées, avec, le cas échéant, les garanties prévues à l'art. 16 al. 2 LPD ou l'application de l'une des exceptions prévues à l'art. 17 LPD.
- La fourniture d'informations et les droits de consultation peuvent exceptionnellement être limités ou refusés si une loi le prévoit, si les intérêts prépondérants de tiers ou de l'établissement s'y opposent, si les données personnelles ne sont pas communiquées à des tiers, ou encore si la demande de renseignement est manifestement infondée.

Il est recommandé de prévoir une procédure (sommaire) d'annonce permettant aux personnes concernées de faire valoir leur droit d'être renseignées et aux responsables du traitement des données ainsi qu'aux services concernés de l'établissement de donner suite à cette requête de façon efficiente.

11. Sous-traitance

Le traitement de données personnelles peut être confié à un·e sous-traitant ·e (cf. art. 9 LPD et art. 7 OPDo). Dans ce cadre, il convient de noter que :

Un tel mandat ne doit pas nécessairement être accordé par écrit. Il peut également être confié oralement ou même par des actes concluants. ARTISET fournit un modèle de contrat de mandat écrit détaillé. Celui-ci constitue la formalisation détaillée et "compacte" des dispositions légales pertinentes (cf. art. 9 LPD et art. 7 OPDo ainsi que d'autres dispositions et principes du droit de la protection des données et du droit des obligations). Même s'il n'est pas indispensable de signer un contrat aussi détaillé, cela peut néanmoins s'avérer plus plus sûr: en effet, le/la responsable doit s'assurer que le/la sous-traitant·e respecte la loi dans la même mesure qu'il/elle le fait lui-/elle-même (devoir de diligence). Un mandat écrit a l'avantage de clarifier et de formaliser le cadre juridique.

En outre, il faut encore mentionner les points suivants:

- Une sous-traitance est également autorisée sans que la personne dont les données sont traitées doive donner son consentement.

- Un·e sous-traitant·e ne peut confier le traitement à un tiers qu'avec l'autorisation préalable du responsable du traitement.
- Le traitement de données au sein de la même personne morale (filiale, unité administrative, membres du personnel) ne constitue pas une sous-traitance. Il serait donc inutile d'accompagner chaque échange interne de données personnelles entre départements d'un même établissement d'un contrat de sous-traitance.
- Si des données sont conservées dans un "nuage" ("cloud "), il s'agit en principe d'un cas desous-traitances, qui doit en respecter les conditions. Si, dans ce cadre, des données personnelles sont communiquées à l'étranger, les conditions correspondantes doivent également être remplies (voir ci-dessous).

12. Droit de la personne concernée à la remise ou à la transmission de données personnelles

Conformément aux art. 28-29 LPD et 20-22 OPDo, chaque personne peut, lorsque les données sont traitées de façon automatisée, exiger de l'établissement que celui-ci lui remette les données personnelles qu'elle lui a communiquées, dans un format électronique courant et généralement sans frais. En pratique, un tel traitement automatisé des données par les établissements est cependant très rare.

13. Communication de données à l'étranger

Si des données personnelles sont communiquées à l'étranger, l'établissement doit prendre les mesures prévues aux art. 16-18 LPD et aux art. 8-12 OPDo.

14. Analyses d'impact relatives à la protection des données personnelles

Lorsque l'établissement traite des données personnelles susceptibles de présenter un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, la/le responsable du traitement des données réalise à chaque fois au préalable une analyse d'impact relative à la protection des données personnelles au sens de l'art. 22 LPD. Cette analyse d'impact doit contenir une description du traitement envisagé, une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée ainsi que les mesures prévues de protection de la personnalité et des droits fondamentaux (art. 22 al. 3 LPD).

En fonction des résultats de cette analyse, il est nécessaire de consulter le préposé fédéral à la protection des données et à la transparence (PFPDT), conformément à ce que prévoit l'art. 23 LPD.

En pratique, il n'est pas rare que les établissements traitent des données personnelles susceptibles de présenter un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Il est dès lors fréquemment nécessaire de réaliser des analyses d'impact en matière de protection des données personnelles.

15. Stockage et destruction de données personnelles

Les données personnelles, collectées dans un but précis, ne peuvent être conservées qu'aussi longtemps que cela est nécessaire pour atteindre ce but (art. 6 al. 4 LPD). Si elles ne sont plus utiles, elles doivent être anonymisées ou effacées/détruites, à moins que des raisons prépondérantes ne justifient leur conservation.

Ainsi, il convient de vérifier au cas par cas :

- combien de temps il est nécessaire de conserver des données personnelles en cause,
- s'il existe une obligation légale de les conserver

- ou s'il existe un intérêt prépondérant à leur conservation.

Il est donc recommandé de garantir au moyen de directives que:

- les données personnelles que l'établissement ne doit plus traiter sont compilées et stockées pendant une durée déterminée ou déterminable;
- les données personnelles d'importance secondaire sont détruites (broyées physiquement ou effacées électroniquement de manière irrévocable) dès que la finalité de leur traitement a été atteinte.

16. Traitement automatisé de données

Comme indiqué ci-dessus, il est en pratique peu fréquent que les établissements entreprennent des traitements automatisés de données. Si ce devait malgré tout être le cas, il conviendrait alors de veiller au respect des points suivants:

- Lors du traitement automatisé à grande échelle de données sensibles, l'enregistrement, la modification, la lecture, la communication, l'effacement et la destruction des données doivent être consignées par écrit (cf. art. 4 OPDo). Ceci n'est cependant pas obligatoire lorsque des mesures préventives garantissent la protection des données.
- Lorsque l'établissement traite à grande échelle de façon automatisée des données sensibles, un règlement sur les traitements automatisés au sens de l'art. 5 OPDo doit être établi. Le règlement doit en particulier contenir des informations sur l'organisation interne, sur les procédures de traitement des données et de contrôle des données ainsi que sur les mesures visant à garantir la sécurité des données (cf. art. 5 al. 2 OPDo).

17. Profilage

Le profilage désigne l'utilisation de données pour évaluer certains aspects personnels relatifs à une personne physique, tels que son rendement au travail, sa situation économique, sa santé, ses préférences personnelles, ses intérêts, sa fiabilité, son comportement, sa localisation ou ses déplacements (cf. art. 5 let. f LPD). Le profilage présuppose un traitement automatisé des données personnelles.

En pratique, un tel traitement de données automatisé n'est guère entrepris par les établissements. C'est pourquoi les mécanismes de protection spécifiques prévus par la loi en matière de profilage manquent de pertinence dans le présent contexte et ne sont pas décrits plus en détail ici.

18. Annonce de violations de la protection des données

Il est recommandé de prévoir une procédure (sommaire) d'annonce pour permettre à la / au responsable du traitement des données de signaler de manière efficiente au Préposé fédéral à la protection des données et à la transparence (PFPDT) d'éventuelles violations de la protection des données par l'établissement (cf. art. 24 LPD et art. 15 OPDo).

Yann Golay Trechsel / 29.10.2024

ARTISET

Zieglerstrasse 53, 3007 Berne
Tél. +41 31 385 33 33
info@artiset.ch, artiset.ch