Protection des données – Premiers enseignements une année après l'entrée en vigueur de la nouvelle loi

Pension Apéritif SLPS – novembre 2024

Antoine Amiguet

Plan

Introduction

La nouvelle loi fédérale sur la protection des données (LPD) est entrée en vigueur le 1er septembre 2023, sans période transitoire.

La LPD s'applique, sauf exception, à tous les acteurs de l'économie, y compris aux institutions de prévoyance (IP).

Principaux axes de la réforme:

- Amélioration de la transparence des processus de traitement de données personnelles
- Amélioration de la mise en œuvre (*enforcement*) des règles en matière de protection des données en:
- Adaptation aux standards de l'UE (RGPD) et à la Convention 108 du Conseil de l'Europe

DONNÉES PERSONNELLES = **toutes** les **informations** concernant une **personne physique identifiée** ou **identifiable**	DONNÉES SENSIBLES = notamment les informations sur : • **santé**, **sphère intime** ou **origine raciale** ou **ethnique** • **poursuites** ou **sanctions** pénales et administratives • mesures d'**aide sociale**
PERSONNE CONCERNÉE = **personne physique dont les données personnelles font l'objet d'un traitement** (p.ex. assurés actifs et bénéficiaires de rentes, personnes de contact des partenaires commerciaux, membres du Conseil de fondation)	TRAITEMENT = **toute opération relative à des données personnelles** (p.ex. collecte, enregistrement, conservation, utilisation, modification, communication, archivage)

Plan

Régime applicable

Dans son Rapport d'activités 2023/2024, le PFPDT a pris les positions suivantes:

- Caisse de pension participant à la mise en œuvre de la prévoyance professionnelle obligatoire et caisse de pension enveloppante = **organe fédéral au sens de la LPD**
- Caisse de pension dont les activités relèvent exclusivement du régime surobligatoire = **personne privée au sens de la LPD**
- Caisses de pension agissant en tant qu'organes publics cantonaux ou communaux = soumises, dans le cadre de la LPP obligatoire, à la **législation cantonale sur la protection des données** ainsi qu'à la **surveillance cantonale ou municipale**
- Société de services externe à laquelle la caisse de pension confie une partie ou la totalité de leurs activités opérationnelles = **sous-traitant**

Les positions du PFPD ne lient pas les tribunaux mais imposent néanmoins un certain standard.

Régime applicable/ Liste de contrôle

		Organe fédéral	Personne privée
Registre des activités de traitement:	✓ Préparation	●	○
	✓ Communication au PFPDT	●	
Obligation d'information (*privacy notice*):	✓ Préparation ✓ Communication aux personnes concernées (notamment les assurés actifs et les bénéficiaires de rentes)	●	●
Règlement de traitement:	✓ Préparation et adoption par le conseil de la fondation	●	○
Contrats impliquant un transfert de données personnelles:	✓ Conclusion de contrats (s'ils n'existent pas) ou adaptation de contrats existants	●	●
Conseiller à la protection des données (DPO) :	✓ Nomination ✓ Publication des coordonnées et communication au PFPDT	●	

Plan

Registre des activités de traitement (art. 12 LPD et 24 OPDo)

De quoi s’agit-il:

- Cartographie des traitements de données personnelles effectuées par l’IP
- Se présente généralement sous la forme d’un tableau Excel
- Plusieurs façon de faire possibles

Préparation:

- Obligatoire pour les organes fédéraux
- Facultative (mais vivement conseillée) pour les personnes privées

Déclaration au PFPDT:

- Obligatoire pour les organes fédéraux
- Conseillé de le faire par le biais de la plateforme du PFPDT dans les trois langues officielles (allemand, français et italien)
- Entre le 1er avril 2023 et le 31 mars 2024, les institutions de prévoyance ont procédé à plus de 1'000 inscriptions dans le registre des activités de traitement des organes fédéraux du PFPDT (*Datareg*) (cf. Rapport d'activités 2023/2024 du PFPDT, p. 45)

Plan

Notice d'information (art. 19 ss et 60 LPD, 13 OPDo)

L'assuré a le droit d'être informé de manière adéquate de toute collecte de données personnelles.

Pas d'obligation d'informer lorsque le traitement de données personnelles est prévu par la loi.

→ Il est toutefois conseillé à toutes les caisses de pension de rédiger une notice d'information.

Contenu minimal:

- Identité et coordonnées du responsable de traitement (*i.e.* la caisse de pension)
- Finalités des traitements de données personnelles
- Le cas échéant, destinataires auxquels les données personnelles sont transmises
- Lorsque les données personnelles sont communiquées à l'étranger, nom de l'Etat concerné et, le cas échéant, garanties mises en place

Plan

Règlement de traitement (art. 5 et 6 OPDo)

Ce document est obligatoire pour les organes fédéraux mais il ne doit en principe pas être soumis à l'autorité de surveillance.

Ce document comprend généralement des dispositions sur:

- Les rôles essentiels du point de la protection des données pour assurer la conformité à la législation applicable
- La procédure de réponse aux requêtes des personnes concernées
- La procédure applicable en cas d'incident de sécurité:
  - Personnes en charge de l'analyse de l'incident, des prises de décision, de la communication, du contact avec les autorités
  - Définition de la marche à suivre
  - Annonce au PFPDT / aux personnes concernées (art. 24 LPD et 15 OPDo)
- Les règles relatives à l'archivage
- Les mesures visant à garantir la sécurité des données

Plan

Contrats impliquant un transfert de données personnelles (art. 9 et 61 LPD, 7 nODPo)

Revue des dispositions en matière de protection des données (description du traitement, instructions, etc.):

- Mesures de sécurité appropriées et adéquates
- Procédure d'information en cas de fuite de données
- Procédure d'information et autorisation préalable pour le recours à des sous-sous-traitants
- Garanties appropriées (p. ex: clauses contractuelles standards) en cas de transfert de données personnelles vers des Etats non-adéquats

Un avenant peut venir modifier / compléter le contrat principal existant.

Le PFPDT considère que les sociétés de services externes auxquelles les institutions de prévoyance confient une partie ou la totalité de leurs activités opérationnelles sont des sous-traitants.

Certains gestionnaires contestent cette approche.

Plan

Conseiller à la protection des données (art. 10 LPD, 23 et 25 ss OPDo)

La désignation d'un conseiller à la protection des données (*Data Protection Officer;* DPO) est:

- Obligatoire pour les organes fédéraux
- Facultative pour les personnes privées (présente un intérêt restreint)

Rôle du DPO:

- Former et conseiller les collaborateurs de l'IP en matière de protection des données
- Participer à l'application des dispositions relatives à la protection des données
- Servir d'interlocuteur pour les personnes concernées et le PFPDT

Plan

Préposé fédéral à la protection des données (art. 4 et 43 ss LPD, 36 ss OPDo)

Le Préposé fédéral à la protection des données et à la transparence (PFPDT) est chargé de surveiller la bonne application des dispositions fédérales de protection des données (art. 4 LPD).

Le PFPDT:

- Peut ouvrir une enquête contre un organe fédéral ou une personne privée si des indices suffisants font penser qu'un traitement de données pourrait être contraire à des dispositions de protection des données (art. 49 LPD)
- Peut prendre des mesures administratives (art. 51 LPD), telles que:
  - Ordonner la modification, la suspension ou la cessation de tout ou partie du traitement ainsi que l'effacement ou la destruction de tout ou partie des données personnelles
  - Suspendre ou interdire la communication de données personnelles à l'étranger
- Doit être informé des cas de violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité (art. 24 LPD)

Le PFPDT ne peut pas prononcer de sanctions pénales.

Plan

Dispositions pénales (art. 60 ss LPD)

Approche retenue par la Suisse:

- Les infractions à la LPD sont susceptibles de sanctions pénales
- Les personnes physiques sont visées en première ligne

Approche différente en droit européen: amendes administratives contre les personnes morales:

- Les auteur des infractions = "Personnes privées"
- La plupart des dispositions pénales LPD visent les "personnes privées" au sens de la LPD, et non pas les organes fédéraux
- Risque qu'elles s'appliquent aux membres du Conseil de fondation et collaborateurs d'une caisse de pensions, notamment lorsque l'institution de prévoyance est enveloppante et agit donc au-delà du régime obligatoire LPP?

Dispositions pénales (art. 60 ss LPD)

LPD	Infraction	Auteur	Poursuite
Art. 60 (1)	Fourniture intentionnelle de renseignements inexacts ou incomplets aux personnes concernées ou omission intentionnelle d'informer	Personnes privées	Sur plainte
Art. 60 (2)	Fourniture intentionnelle de renseignements inexacts ou refus intentionnel de collaborer dans le cadre d'une enquête	Personnes privées	D'office
Art. 61	Violation intentionnelle des devoirs de diligence (communication à l'étranger, respect des conditions de l'art. 9 LPD en cas de sous-traitance, exigences minimales en matière de sécurité des données)	Personnes privées	Sur plainte
Art. 62	Violation intentionnelle du devoir de discrétion	Quiconque	Sur plainte
Art. 63	Insoumission à une décision du PFPDT ou d'une autorité de recours	Personnes privées	D'office

Dispositions pénales (art. 60 ss LPD)

Toutes les infractions sont:

- Punies de l'amende de CHF 250'000 au plus
- Intentionnelles
- Des contraventions (art. 333 al. 3 CP) – tentative et complicité non punissables (art. 105 al. 2 CP)

Les violations des règles suivantes ne constituent pas une infraction pénale:

- Annonce des violations de la sécurité des données (*data breach notifications*) (art. 24 LPD)
- Registre des activités de traitement (art. 12 LPD)
- Analyse d'impact en cas de risque élevé pour la personnalité (art. 22 LPD)

Prescription de l'action pénale = 5 ans (art. 66 LPD)

Dispositions pénales (art. 60 ss LPD)

Volonté claire du législateur de sanctionner les personnes physiques:

- Exception: "*Lorsque l'amende entrant en ligne de compte ne dépasse pas CHF 50'000 et que l'enquête rendrait nécessaires à l'égard des personnes punissables selon l'art. 6 DPA des mesures d'instruction hors de proportion avec la peine encourue, l'autorité peut renoncer à poursuivre ces personnes et condamner l'entreprise (art. 7 DPA) au paiement de l'amende à leur place*" (art. 64 al. 2 LPD)
- L'employeur peut-il payer l'amende à la place de la personne physique?
  - Controversé en doctrine
  - Risqué: "*Celui qui aura soustrait une personne à (…) l'exécution d'une peine (…) sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire*" (art. 305 CP)
  - Amende = hautement personnelle
- Peut-on s'assurer?
  - Accord aux termes duquel une personne s'engage à payer une amende infligée à un tiers est en principe nul
  - En pratique: les assurances excluent les amendes de la couverture

Merci pour votre attention!

Antoine Amiguet
Associé, LL.M. (NYU)
aamiguet@obersonabels.com
T +41 58 258 88 88