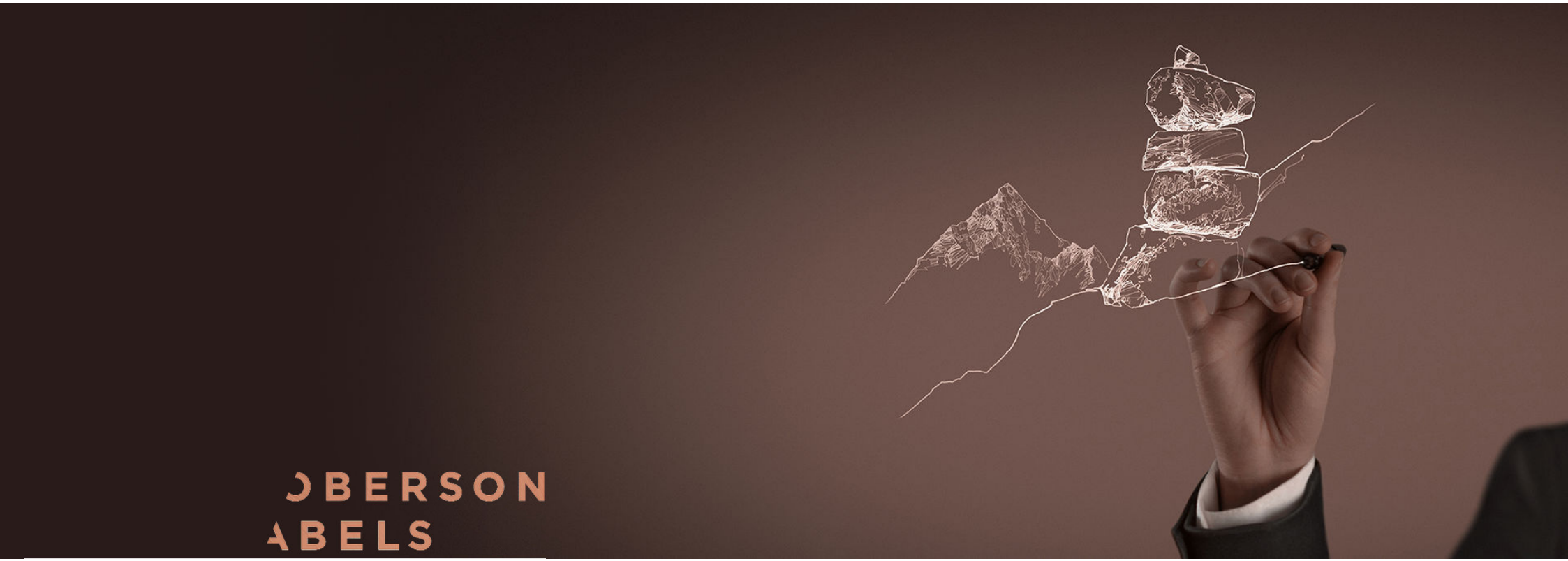


Protection des données – Nouvelles règles applicables aux caisses de pension

Pension Apéritif – septembre 2023

Antoine Amiguet

Plan

Introduction

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

La LPD s'applique en principe 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:
  - accordant des nouveaux droits aux personnes concernées
  - imposant la divulgation d'incidents de la sécurité en matière de données personnelles
  - renforçant les pouvoirs du Préposé fédéral à la protection des données (PFPDT)
  - prévoyant des sanctions plus sévères
- Adaptation aux standards de l'UE (RGPD) et à la Convention 108 du Conseil de l'Europe

Absence de disposition transitoire: les institutions de prévoyance doivent respecter ces règles dès à présent

Plan

Régime applicable

La LPD prévoit des règles différentes selon que l'acteur concerné est une « personne privée » ou un « organe fédéral »

De manière générale, les règles sont plus strictes pour les organes fédéraux que pour les personnes privées

Dans le domaine de la prévoyance:

- Les caisses de pension actives dans le domaine de la prévoyance obligatoire et les fondations de libre passage sont considérées comme des organes fédéraux
- Les institutions actives exclusivement dans le domaine sur- ou hors- obligatoire sont soumises aux règles applicables aux personnes privées
- Les caisses de pension cantonales ou communales organisées sous la forme d'une institution de droit public sont en principe soumises aux règles du droit cantonal en matière de protection des données

Régime applicable

IP	Domaine de la prévoyance	Régime applicable
Caisses de pension enregistrées	Prévoyance obligatoire Prévoyance obligatoire et sur-obligatoire	Régime de la LPD applicable aux organes fédéraux
Fondations de libre passage	Libre passage	Régime de la LPD applicable aux organes fédéraux
Caisses de pension non enregistrées	Prévoyance sur- ou hors-obligatoire	Régime de la LPD applicable aux personnes privées
Caisses de pension cantonales ou communales organisées sous la forme d'une institution de droit public	Prévoyance obligatoire et/ou surobligatoire	Droit cantonal sur la protection des données

Plan

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

De quoi s'agit-il:

- Mapping des traitements de données personnelles effectuées par l'IP
- Se présente généralement sous forme d'un tableau Excel
- Plusieurs façons de faire possibles (p. ex. modèle ASIP)

Catégories de données personnelles traitées	Catégories de données personnelles traitées	Catégories de données personnelles traitées	Données sensibles	Données sensibles	Données sensibles	Données sensibles
Horaires de travail	Données de connexion	Données de localisation	Données de santé	Orientation ou vie sexuelle	Condamnations pénales	Poursuites ou sanctions pénales et administratives

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

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
- Environ 700 IP ont déclaré leur registre des activités de traitement sur la plateforme du PFPDT à ce jour

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

Modèle proposé par l'ASIP

Déclaration de confidentialité Caisse de pension XY

Principe

La déclaration de confidentialité[1] s'applique à toutes les données personnelles[2] que nous traitons dans le cadre de l'exécution de la prévoyance professionnelle et des activités y afférentes, y compris les locations.

Avec cette déclaration de confidentialité, nous aimerions vous expliquer comment nous collectons et traitons vos données personnelles lorsque vous consultez notre site web ou utilisez nos services en ligne; et comment nous les retraitons, les stockons et les transmettons à des tiers, lorsque nous vous fournissons des prestations de service.

Nous ne collectons et traitons vos données personnelles que pour les objectifs décrits dans la déclaration de confidentialité et dans la quantité nécessaire à cet effet, ainsi que dans le cadre des prescriptions légales en vigueur. Ce faisant, nous ne conservons vos données personnelles que dans la mesure où cela est nécessaire et aussi longtemps que le requièrent nos prestations de service. Nous veillons à garantir la protection de nos bases de données contre toute intrusion extérieure, perte, utilisation abusive ou falsification.

Pour garantir la sécurité de vos données personnelles et leur protection contre des traitements non autorisés, voire illicites, nous prenons des mesures appropriées sur le plan technique (p. ex. cryptage ou pseudonymisation des données personnelles, procès-verbaux, restrictions d'accès et stockage de copies de sauvegarde) et organisationnel (p. ex. consignes données aux collaboratrices et collaborateurs, clauses de confidentialité et contrôles).

Plan

Règlement de traitement (art. 5 et 6 OPDo)

Ce document est obligatoire pour les organes fédéraux

Il ne doit en principe pas être soumis à l'autorité de surveillance (raison pour laquelle il est généralement désigné sous le terme de directive)

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

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

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

Exigences applicables au DPO:

- doit disposer des connaissances professionnelles nécessaires
- doit exercer sa fonction de manière indépendante par rapport à la caisse de pension et sans recevoir d'instruction de celle-ci
  - Le DPO ne devrait pas être un membre du Conseil de fondation
  - La désignation d'un employé de l'employeur affilié est envisageable, mais nécessite la mise en place de mesures de séparation strictes
  - Le DPO peut être un externe (souvent la meilleure solution)
- peut être une personne physique ou morale

La caisse de pension doit:

- donner au conseiller à la protection des données accès à tous les renseignements, les documents, les registres des activités de traitement et à toutes les données personnelles dont celui-ci a besoin pour l'accomplissement de ses tâches
- veiller à ce que le conseiller à la protection des données soit informé de toute violation de 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 addendum peut venir modifier / compléter le contrat principal existant.

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

Externalisation	Destinataire	Statut au regard de la LPD
Gestion technique et administrative	Administration externe	Sous-traitant (ASIP) ou responsable selon le degré d'indépendance du prestataire de services
Stockage et gestion des données	Fournisseur de services IT	Sous-traitant: le fournisseur de services IT agit sur instruction de l'IP. Le but et les moyens du traitement sont définis par l'IP en tant que responsable de traitement.
Expertise en matière de prévoyance	Expert en matière de prévoyance professionnelle	Sous-traitant (CHS PP) ou responsable indépendant
Révision des états financiers	Organe de révision	Responsable indépendant / tiers (en principe, ne traite pas de données personnelles de l'IP)
Dépôt et/ou gestion des actifs	Banque dépositaire / Gestionnaire de fortune	Responsable indépendant / tiers (en principe, ne traite pas de données personnelles de l'IP)
Réassurance	Compagnie d'assurance	Responsable indépendant
Courtier (intermédiaire d'assurance non lié)	Courtage pour le compte de l'employeur	Responsable indépendant (ASIP)

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

Exemple d'avenant relatif au traitement de données personnelles

Addendum relatif au transfert de données personnelles

entre
Caisse de pension XY, ayant son siège à Genève

("**Exportateur**")

et
[<Nom>], [<Adresse>]

("**Importateur**")

(individuellement, une "**Partie**", et collectivement, les "**Parties**")

[...]

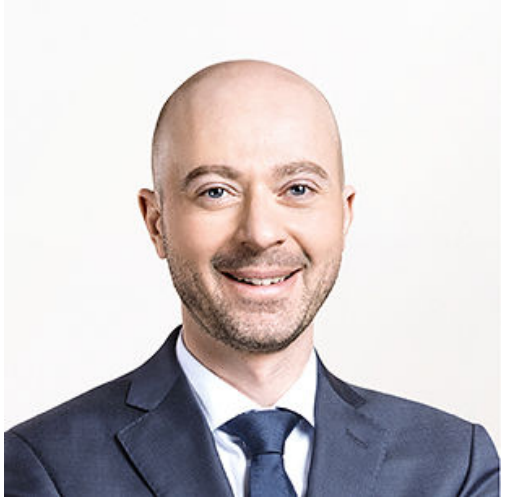
4. Traitement des Données Personnelles

4.1 L'Importateur s'engage à :

a) mettre en œuvre et maintenir à tout moment les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque du Traitement, en tenant compte des standards de l'industrie, des coûts de mise en œuvre et de la nature, de la portée, du contexte, des finalités du Traitement, ainsi que des risques liés au Traitement pour les droits et libertés des Personnes Concernées, y compris, le cas échéant :

i. la pseudonymisation et le cryptage des Données Personnelles ;
ii. la capacité de garantir en permanence la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de Traitement ;
iii. la capacité de restaurer en temps utile la disponibilité et l'accès aux Données Personnelles en cas d'incident physique ou technique ; et
iv. un processus permettant de tester, d'apprécier et d'évaluer régulièrement l'efficacité des mesures techniques et organisationnelles visant à garantir la sécurité du Traitement ;

Merci pour votre attention



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