

Nouvelle loi sur la protection des données

Conséquences sur les institutions de prévoyance

La Suisse révisé sa loi sur la protection des données (LPD) afin de tenir compte des évolutions technologiques et sociétales. Il s'agit d'améliorer la transparence des traitements de données et de renforcer le pouvoir d'autodétermination des personnes concernées sur leurs données.

EN BREF

Les dispositions remaniées sur la protection des données pourraient entrer en vigueur à la mi 2022. Dans le contexte des éventuelles sanctions et d'une atteinte à la réputation en cas de manquements, cette thématique devrait être examinée en temps utile et les adaptations nécessaires devraient être concrétisées.

La révision de la LPD s'explique notamment aussi dans le contexte du Règlement (UE) 2016/679 du 27 avril 2016, à savoir le règlement général sur la protection des données (RGPD). Pour la Suisse, il est capital de continuer à être reconnue par l'UE comme un État tiers offrant un niveau de protection des données approprié, pour qu'à l'avenir la transmission transfrontalière des données reste possible sans être entravée. À cet effet, les dispositions suisses relatives à la protection des données seront alignées sur le RGPD, mais différeront néanmoins des réglementations du RGPD sur certains points («Swiss Finish»).

La révision totale de la LPD a été adoptée par le Parlement le 25 septembre 2020. L'adaptation des dispositions d'exécution et plus particulièrement de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD) est en cours de préparation. La consultation sur la révision de l'OLPD doit s'ouvrir le premier semestre 2021. Les dispositions remaniées sur la protection des données pourraient entrer en vigueur à la mi 2022.

Quelles dispositions en matière de protection des données s'appliquent-elles aux institutions de prévoyance?

Dans la prévoyance professionnelle, il est à noter que les prescriptions des lois spéciales applicables en matière de protection des données telles qu'énoncées dans la LPP et dans la LFLP (art. 85a ss LPP et art. 25 LFLP) évincent parfois les dispositions de la LPD. Les institutions

de prévoyance qui pratiquent la prévoyance professionnelle obligatoire sont soumises aux prescriptions en matière de protection des données du droit de la prévoyance. Les prescriptions de la LPD, notamment les principes régissant le traitement des données (art. 6 LPD^{rév}) s'appliquent à titre complémentaire. Dans le cadre de la LPD, les institutions de prévoyance sont considérées comme des organes fédéraux et ont besoin d'une base légale pour le traitement et la communication de données personnelles, qu'offrent les art. 85a ss LPP.

Dans le domaine de la prévoyance professionnelle étendue, sur- et hors obligatoire, les institutions de prévoyance sont considérées comme des personnes privées et seules les dispositions de la LPD sont applicables (avec les exceptions citées à l'art. 49 al. 2 LPP). En tant que personnes privées, elles peuvent traiter des données personnelles, même sans base légale, pour autant que la personnalité des personnes concernées ne soit pas enfreinte de façon illégale. La LPD entièrement révisée ne change rien à cette systématique.

Qu'est-ce qui change dans la LPD révisée?

La LPD^{rév} s'applique toujours au traitement des données personnelles des personnes physiques, autrement dit des informations qui se réfèrent à une personne physique identifiée ou identifiable. Des règles particulières s'appliquent aux données personnelles sensibles, par exemple les données de santé. Les don-

nées des personnes morales ne sont en revanche plus couvertes par la LPDrév.

Pour l'essentiel, les principes régissant le traitement des données restent inchangés. Un traitement licite et conforme aux principes de la proportionnalité est toujours supposé. Les données ne doivent être collectées et traitées que dans le but indiqué et doivent être détruites dès qu'elles ne sont plus requises aux fins du traitement. Des nouveautés existent notamment dans le domaine des décisions qui sont prises de manière exclusivement automatique (profilage et profilage à risque élevé). La protection des données doit continuer à être garantie également au plan technique. Des réglages par défaut propices à la protection des données («privacy by design and default») sont désormais nécessaires (art. 7 al. 3 LPDrév).

Il existe différentes nouveautés concernant les processus et la documentation: désormais, il faut notamment établir un registre des activités de traitement, informer de la collecte des données personnelles, introduire un processus d'analyse d'impact relative à la protection des données et d'annonce des manquements à la sécurité des données, mais aussi adapter le processus de fourniture de renseignements et introduire un nouveau processus pour la communication ou le transfert de données sur demande.

Concernant l'exécution de la LPDrév, rappelons que le Préposé fédéral à la protection des données et à la transparence (PFPDT) se voit doter de compétences d'investigation et d'action étendues et peut prendre des mesures administratives (art. 49 ss LPDrév). Le PFPDT peut percevoir des émoluments de personnes privées pour certaines prestations dans le cadre de la LPDrév (art. 59 LPDrév). Le champ d'application des sanctions est par ailleurs élargi et les amendes éventuelles qui peuvent désormais s'élever à

250 000 francs ont été significativement augmentées.

La rédaction de la base légale du traitement des données personnelles dans la prévoyance professionnelle obligatoire est en outre adaptée et une base légale expresse pour le traitement des données personnelles dans le but d'évaluer la santé, les besoins et la situation économique de la personne assurée est introduite (art. 85a LPDrév), autrement dit pour le traitement des données personnelles sensibles selon l'art. 5 let. c LPDrév.

Dans quels domaines les institutions de prévoyance doivent-elles agir?

Sachant que les dispositions d'exécution du Conseil fédéral pourraient encore nécessiter d'autres adaptations, une action est notamment requise dans les domaines suivants, dans une perspective actuelle:

- adaptation des documents relatifs à la protection des données (nouvelle terminologie; art. 5 LPDrév) et des contrats de protection des données (notamment en ce qui concerne le traitement sur mandat; art. 9 LPDrév);
- implémentation de réglages par défaut propices à la protection des données («privacy by design and default»; art. 7 al. 3 LPDrév);
- établissement d'un registre des activités de traitement (art. 12 LPDrév);
- vérification de l'existence de transferts de données à l'étranger et de leur protection suffisante au regard de la protection des données (art. 16 LPDrév);
- implémentation d'une déclaration relative à la protection des données lors de la collecte de données personnelles (nouveau devoir d'information; art. 19 s. LPDrév);
- détermination de la nécessité d'une analyse d'impact relative à la protection des données et de la possibilité correspondante d'élaborer un proces-

sus défini (art. 22 LPDrév) ainsi que, le cas échéant, implémentation d'un processus pour la consultation du PFPDT (art. 23 LPDrév);

- implémentation de processus relatifs à l'annonce de violations de la sécurité des données (art. 24 LPDrév), sur l'information sur les traitements de données conformément à la LPD révisée (art. 25 LPDrév) et sur la communication et le transfert de données (art. 28 s. LPDrév).

Mise en œuvre

Dans la perspective de la loi révisée sur la protection des données, les institutions de prévoyance doivent notamment analyser, documenter et adapter leurs processus de traitement des données, vérifier et adapter les documents et les conventions relatifs à la protection des données, garantir la protection des données grâce à des précautions techniques et garantir des réglages par défaut propices à la protection des données ainsi que garantir les droits et les devoirs d'information. Les institutions enveloppantes devraient rechercher une solution permettant de concilier les différentes exigences à l'égard des organes fédéraux et des personnes privées.

Grâce à une approche systématique et à un projet de mise en œuvre rigoureux, les adaptations nécessaires devraient généralement pouvoir être appliquées assez facilement. Dans le contexte des éventuelles sanctions et d'une atteinte à la réputation en cas de manquements, cette thématique devrait être examinée en temps utile et les adaptations nécessaires devraient être concrétisées. **I**

Evelyn Schilter
Estelle Caveng