

Checklist Conformité à la protection des données - Caisse de pension

Généralités

	Oui	Non
Dans la mesure où le consentement des personnes concernées est nécessaire pour le traitement de données personnelles, ce consentement est-il recueilli et documenté ?	☐	☐
Dans la mesure où le consentement des personnes concernées est nécessaire pour le traitement des données personnelles, celui-ci est-il obtenu pour certains traitements, avec une information appropriée et, le cas échéant, expressément pour le traitement de données personnelles sensibles ?	☐	☐
La caisse de pension tient-elle un registre de traitement contenant toutes les informations nécessaires ?	☐	☐
La caisse de pension a-t-elle communiqué le registre de traitement au PFPDT ?	☐	☐
La caisse de pension effectue-t-elle des traitements de données qui présentent un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées et a-t-elle effectué au préalable une analyse d'impact sur la protection des données pour de tels traitements ?	☐	☐
La caisse de pension conserve-t-elle les analyses d'impact sur la protection des données pendant au moins deux ans après la fin du traitement des données ?	☐	☐
La caisse de pension remplit-elle d'éventuelles exigences cantonales supplémentaires en matière de protection des données ?	☐	☐

Conseiller à la protection des données

Les caisses de pension enveloppantes (enregistrées) actives dans le domaine obligatoire et subobligatoire sont soumises aux dispositions de protection des données applicables aux organes fédéraux et doivent désigner un conseiller à la protection des données conformément à l'art. 25 OLPD.

	Oui	Non
La caisse de pension a-t-elle désigné un conseiller à la protection des données ?	☐	☐
Le conseiller à la protection des données a-t-il pour mission de former et de conseiller la caisse de pension en matière de protection des données ?	☐	☐
Le conseiller à la protection des données dispose-t-il des ressources nécessaires et a-t-il accès à tous les renseignements, documents, registres de traitement et données personnelles dont il a besoin pour accomplir ses tâches ? A-t-il le droit d'informer l'organe supérieur de direction ou d'administration de la caisse de pension dans les cas importants ?	☐	☐

Les coordonnées du conseiller à la protection des données ont-elles été publiées sur le site web de la caisse de pension ?	☐	☐
Les coordonnées du conseiller à la protection des données ont-elles été communiquées au PFPDT ?	☐	☐
Les coordonnées du conseiller à la protection des données ont-elles été communiquées aux employés et ce dernier est-il à la disposition de tous les employés en tant qu'interlocuteur pour les questions de protection des données ?	☐	☐

Procédures

	Oui	Non
Des mesures appropriées ont-elles été prises pour identifier la personne concernée lors d'une demande d'accès ?	☐	☐
Des procédures ont-elles été mises en place pour répondre aux demandes d'accès dans un délai de 30 jours ?	☐	☐
Des procédures ont-elles été mises en place pour que les données personnelles soient transmises dans un format électronique à la demande des personnes concernées ?	☐	☐
Des procédures ont-elles été mises en place pour que les demandes de rectification, d'effacement ou de destruction de données personnelles soient traitées dans les délais impartis ?	☐	☐
Des procédures ont-elles été mises en place pour signaler sans délai au PFPDT toute violation de la protection des données présentant un risque élevé pour la personnalité et les droits fondamentaux des personnes concernées ?	☐	☐
Des procédures ont-elles été mises en place pour documenter les violations de la protection des données et conserver la documentation pendant au moins deux ans ?	☐	☐

Obligations d'information

Conformément à l'art. 19 de la LPD, les personnes concernées doivent être informées en détail sur le traitement de leurs données par la caisse de pension.

	Oui	Non
Au moment de la collecte des données personnelles, les personnes concernées (assurés, collaborateurs, etc.) sont-elles informées de l'étendue et des finalités des traitements de données de manière précise, transparente, compréhensible et facilement accessible ? Ces informations sont-elles complètes ?	☐	☐

Checklist Conformité à la protection des données - Caisse de pension

Les personnes concernées sont-elles informées des décisions individuelles automatisées et ont-elles la possibilité de faire valoir leur point de vue ?	☐	☐
--	--------------------------	--------------------------

Suppression des données

La législation en matière de protection des données exige que les données personnelles ne soient traitées qu'aussi longtemps que nécessaire pour atteindre les objectifs fixés et respecter les éventuels délais de conservation légaux.

	Oui	Non
L'enregistrement, la modification, la lecture, la communication, l'effacement et la destruction de données personnelles sensibles traitées de manière automatisée à grande échelle ou faisant l'objet d'un profilage à haut risque, et pour lesquelles des mesures préventives ne peuvent pas garantir la protection des données, sont-ils consignés ?	☐	☐

Sous-traitance et communication de données à l'étranger

Le traitement des données personnelles par des prestataires de services sur la base de directives doit être effectué dans le cadre d'un contrat. Lorsque des prestataires de services traitent des données personnelles sur mandat, le respect de certaines normes de sécurité doit être fixé conformément à l'article 9 LPD. Les données personnelles peuvent être communiquées à l'étranger si une protection adéquate est garantie.

	Oui	Non
Tous les sous-traitants ont-ils été identifiés ?	☐	☐
Des dispositions contractuelles ont-elles été prises avec tous les sous-traitants pour le traitement des données ?	☐	☐
La caisse de pension s'est-elle assurée auprès de chaque sous-traitant que celui-ci est en mesure de garantir la sécurité des données ?	☐	☐
Les sous-traitants ne peuvent-ils transférer des données personnelles à un tiers qu'avec l'autorisation préalable spécifique ou générale de la caisse de pension ?	☐	☐
En cas de communication de données personnelles à l'étranger, une protection des données appropriée est-elle garantie et la communication n'a-t-elle lieu que vers un pays offrant un niveau de protection adéquat, en application de clauses contractuelles standard ou conformément aux exceptions prévues à l'article 17 de la LPD ?	☐	☐
En cas de communication de données à l'étranger sur la base de clauses contractuelles standard, la caisse de pension utilise-t-elle les clauses contractuelles approuvées du PFPDT avec les adaptations prescrites ?	☐	☐

La caisse de pension a-t-elle pris des mesures appropriées pour s'assurer que les destinataires respectent également les clauses contractuelles standard en cas de communication de données à l'étranger au moyen de ces clauses ?	☐	☐
--	--------------------------	--------------------------

Sécurité technique

	Oui	Non
La caisse de pension a-t-elle déterminé les risques pour la personnalité et les droits fondamentaux des personnes concernées ainsi que les besoins de protection des données personnelles et défini les mesures techniques et organisationnelles appropriées en fonction du risque ?	☐	☐
Des mesures appropriées ont-elles été prises pour garantir la confidentialité, la disponibilité, l'intégrité et la traçabilité du traitement des données en fonction de leurs besoins de protection ?	☐	☐
Les données personnelles sont-elles détruites ou anonymisées dès qu'elles ne sont plus nécessaires aux fins du traitement ?	☐	☐
Le traitement des données a-t-il fait l'objet de réglages préalables favorables à la protection des données ?	☐	☐

Sécurité organisationnelle

	Oui	Non
La caisse de pension a-t-elle établi une directive et un concept de protection des données ?	☐	☐
Si nécessaire, la caisse de pension a-t-elle établi un règlement de traitement contenant des indications sur l'organisation interne, les procédures de traitement et de contrôle des données, les responsabilités des personnes impliquées ainsi que les mesures visant à garantir la sécurité des données ? Ce règlement a-t-il été porté à la connaissance du conseil d'administration ?	☐	☐
Si nécessaire, le règlement de protection des données selon la LPP a-t-il été soumis à l'organe de révision cantonal pour examen ?	☐	☐
Les personnes internes et externes ayant accès à des données personnelles sont-elles tenues de respecter le secret professionnel en matière de protection des données ?	☐	☐