PK KVO
PENSIONSKASSE VON KRANKENVERSICHERUNGS-ORGANISATIONEN

Règlement relatif à la protection des données de la CP OAM (caisse de pension des organisations d'assurance-maladie)[1]

Table des matières

[1] *La version originale allemande du règlement fait foi. La version française est une traduction.*

1. Buts du règlement relatif à la protection des données

Le présent règlement relatif à la protection des données doit servir de document principal de référence en la matière et vise à soutenir la mise en œuvre des exigences légales et contractuelles découlant de la nouvelle législation sur la protection des données dans le cadre de la direction et de la gestion de la caisse de pension des organisations d'assurance-maladie (CP OAM). Il régit l'application par la CP OAM de la loi fédérale du 25 septembre 2020 sur la protection des données (LPD; RS 235.1). Outre les dispositions de la LPD, la CP OAM doit également respecter les prescriptions en matière de protection des données prévues à l'art. 85*a* ss de la loi fédérale du 25 juin 1982 sur la prévoyance professionnelle vieillesse, survivants et invalidité (LPP; RS 831.40), qui s'appliquent à titre de règle spéciale (*lex specialis*). Le présent règlement relatif à la protection des données doit servir de document de référence aux personnes responsables de la CP OAM pour respecter et appliquer les prescriptions légales en matière de protection des données.

2. Champ d'application

Le présent règlement relatif à la protection des données s'applique à toutes les personnes chargées de la direction et de la gestion de la CP OAM, ainsi qu'aux assurés, aux bénéficiaires de rente, aux employés affiliés et aux prestataires externes dans la mesure où la LPP ne prime pas.

3. Champ d'application territorial

Le présent règlement relatif à la protection des données s'applique aux états de fait qui déploient des effets en Suisse, même s'ils se sont produits à l'étranger.

Les prétentions de droit privé sont régies par la loi fédérale du 18 décembre 1987 sur le droit international privé (LDIP; RS 291). Sont également réservées les dispositions régissant le champ d'application territorial du code pénal.

4. Définitions

Le présent règlement relatif à la protection des données de la CP OAM se fonde sur les définitions contenues dans la LPD:

4.1 Données personnelles

Toutes les informations concernant une personne physique identifiée ou identifiable.

4.2 Personne concernée

La personne physique dont les données personnelles font l'objet d'un traitement.

4.3 Données personnelles sensibles (données sensibles)

1. les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales;
2. les données sur la santé, la sphère intime ou l'origine raciale ou ethnique;
3. les données génétiques;
4. les données biométriques identifiant une personne physique de manière univoque;
5. les données sur des poursuites ou sanctions pénales et administratives;
6. les données sur des mesures d'aide sociale.

4.4 Traitement

Toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données.

4.5 Communication
Le fait de transmettre des données personnelles ou de les rendre accessibles.

4.6 Profilage
Toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

4.7 Profilage à risque élevé
Tout profilage entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique.

4.8 Violation de la sécurité des données
Toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données.

4.9 Responsable du traitement
La personne privée qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles.

4.10 Sous-traitant
La personne privée qui traite des données personnelles pour le compte du responsable du traitement.

5. Principes généraux du traitement des données (art. 6 LPD[2])

La CP OAM traite les données personnelles selon les principes suivants, lesquels sont régulièrement vérifiés.

5.1 Licéité
La CP OAM traite les données personnelles des assurés et des bénéficiaires de rente de manière licite. Dans ce contexte, elle respecte les prescriptions de la LPD et les dispositions en matière de protection des données prévues par la LPP. Elle traite ces données personnelles avec le consentement des assurés et des bénéficiaires de rente sur la base de formulaires ou d'informations écrites correspondantes.

5.2 Bonne foi
Le traitement est conforme aux principes de la bonne foi et de la proportionnalité.

5.3 Transparence
Les données des assurés et des bénéficiaires de rente sont traitées en tout temps de manière transparente pour la personne concernée. La CP OAM informe cette dernière que ses données sont traitées et lui fournit en tout temps des renseignements sur les données traitées dans ce cadre.

---

[2] ***Les renvois à la LPD portent sur la teneur en vigueur. La numérotation suit celle de la LPD révisée et entrée en vigueur le 1er septembre 2023.***

5.4 Finalité
La CP OAM traite les données personnelles exclusivement aux fins de gestion licite du compte individuel des assurés ou des bénéficiaires de rente.

5.5 Mise à jour et exactitude des données
Lorsqu'elle traite des données, la CP OAM s'assure régulièrement qu'elles sont exactes et à jour. Elle prend les mesures nécessaires pour ce faire. Si elle apprend que des données sont inexactes au regard des finalités et de la gestion du traitement, elle les rectifie après avoir consulté les assurés et les bénéficiaires de rente.

6. Protection des données dès la conception et par défaut (art. 7 LPD)

La gestion technique et donc le traitement des données par la CP OAM sont effectués par le biais d'un logiciel de l'entreprise SwissPension dans l'environnement informatique de Diventa AG. Celui-ci est conçu sur les plans technique et organisationnel de sorte que le traitement respecte les prescriptions de protection des données. Ces mesures sont mises en place dès la conception du traitement (protection des données dès la conception).

7. Sécurité des données (art. 8 LPD)

Tout en tenant compte des coûts de mise en place, la CP OAM, en collaboration avec santésuisse et Diventa AG, prend des mesures organisationnelles et techniques appropriées au regard de l'état de la technique pour protéger les données personnelles traitées et garantir une sécurité adéquate des données personnelles par rapport au risque encouru. Avec santésuisse et Diventa AG, elle veille notamment à la confidentialité, à la disponibilité et à l'intégrité des données ainsi qu'à la traçabilité du traitement. De plus, elle protège les systèmes contre le risque entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données. La CP OAM vérifie périodiquement ces mesures techniques et organisationnelles avec santésuisse et Diventa AG durant toute la durée de traitement.

En collaboration avec le conseiller à la protection des données, le ressort IT de santésuisse et Diventa AG élaborent des directives en matière de sécurité des données, les vérifient périodiquement et, le cas échéant, les adaptent. Elles concernent notamment des mesures techniques telles qu'un accord de niveau de service informatique (*service-level agreement*), un concept de sécurité informatique et une matrice d'autorisation, ainsi que des mesures organisationnelles telles que des conventions relatives aux devoirs de diligence, à la confidentialité et à l'obligation de garder le secret.

8. Analyse d'impact relative à la protection des données personnelles

Lorsque le traitement des données personnelles est susceptible d'entraîner un risque élevé pour la personne concernée, le responsable du traitement procède au préalable à une analyse d'impact relative à la protection des données personnelles. L'analyse d'impact doit contenir une description du traitement envisagé, une évaluation des risques ainsi que les mesures prévues pour protéger la personnalité. L'examen préalable visant à déterminer si une analyse d'impact relative à la protection des données personnelles est requise doit être effectué une première fois dans un délai de six mois à compter de l'entrée en vigueur du présent règlement. Ensuite, l'analyse d'impact relative à la protection des données personnelles doit être menée à intervalles réguliers.

9. Registre des activités de traitement (art. 12 LPD)

Les responsables du traitement de la CP OAM tiennent un registre des activités de traitement.

Le registre du responsable du traitement contient au moins les indications suivantes:

1. l'identité du responsable du traitement;
2. la finalité du traitement;
3. une description des catégories de personnes concernées et des catégories de données personnelles traitées;
4. les catégories de destinataires;
5. dans la mesure du possible, le délai de conservation des données personnelles ou les critères pour déterminer la durée de conservation;
6. dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données;
7. en cas de communication de données personnelles à l'étranger, le nom de l'État concerné et les garanties prévues à l'art. 16, al. 2, LPD;

Le registre du sous-traitant contient des indications concernant l'identité du sous-traitant et du responsable du traitement, les catégories de traitements effectués pour le compte du responsable du traitement ainsi que les indications prévues aux points 6 et 7. La CP OAM veille à ce que le registre soit toujours à jour.

10. Devoir d'informer de la CP OAM lors de la collecte de données personnelles (art. 19 LPD)

La CP OAM informe la personne concernée de la collecte de données personnelles dans le cadre des exigences légales.

11. Droit d'accès de la personne concernée (art. 25 LPD)

En vertu de la LPD, toute personne peut demander à la CP OAM si des données personnelles la concernant sont traitées. Elle reçoit, le cas échéant, les autres informations sur le traitement des données. En règle générale, les renseignements sont fournis gratuitement dans un délai de 30 jours.

12. Communication de données personnelles à l'étranger

Des données personnelles peuvent être communiquées à l'étranger si le Conseil fédéral a constaté que l'État concerné dispose d'une législation assurant un niveau de protection adéquat ou qu'un organisme international garantit un niveau de protection adéquat. C'est généralement le cas lorsque la Suisse a conclu une convention de sécurité sociale avec un État étranger.

Des données personnelles peuvent aussi être communiquées si la personne concernée a expressément donné son consentement à la communication.

13. Conseiller à la protection des données (art. 10 LPD)

Le conseil de fondation de la CP OAM a nommé l'entreprise Swiss Infosec AG, sise à Sursee, comme conseiller à la protection des données. Il s'agit de l'interlocuteur des personnes et des autorités concernées. Le conseiller à la protection des données forme et conseille le responsable du traitement dans le domaine de la protection des données, et apporte son concours dans l'application des prescriptions relatives à la protection des données. Il est indépendant et dispose au minimum des droits et des tâches prévus par les exigences légales.

Le conseiller à la protection des données exerce sa fonction de manière indépendante par rapport au responsable du traitement et sans recevoir d'instruction de celui-ci.

14. Recours à des sous-traitants

Un contrat garantit que tout sous-traitant respecte les dispositions en matière de protection des données en vigueur. Par ailleurs, la sécurité des données doit également être garantie.

15. Devoir d'informer de la CP OAM en tant que responsable du traitement

1. Le responsable du traitement informe la personne concernée de manière adéquate de la collecte de données personnelles, que celle-ci soit effectuée auprès d'elle ou non.
2. Lors de la collecte, il communique à la personne concernée les informations nécessaires pour qu'elle puisse faire valoir ses droits selon la LPD et pour que la transparence des traitements soit garantie; il lui communique au moins:

    a. l'identité et les coordonnées du responsable du traitement;
    b. la finalité du traitement;
    c. le cas échéant, les destinataires ou les catégories de destinataires auxquels des données personnelles sont transmises.

3. Si les données personnelles ne sont pas collectées auprès de la personne concernée, il communique en outre les catégories de données traitées à cette personne.
4. Lorsque des données personnelles sont communiquées à l'étranger, il communique également à la personne concernée le nom de l'État ou de l'organisme international auquel elles sont communiquées et, le cas échéant, les garanties prévues à l'art. 16, al. 2, LPD, ou l'application d'une des exceptions prévues à l'art. 17 LPD.

Les exceptions au devoir d'informer sont régies par l'art. 20 LPD.

16. Responsabilités et contrôles internes

L'application des dispositions et mesures en matière de protection des données et le contrôle du respect de ces dernières incombent au conseil de fondation de la CP OAM ainsi qu'au gérant de la CP OAM.

Le respect des dispositions et mesures en matière de protection des données incombe en premier lieu aux collaborateurs de Diventa AG qui traitent des données et au gérant de la CP OAM.

17. Processus de contrôle et d'amélioration, check-lists

Un processus de contrôle et d'amélioration, accompagné d'éventuelles mesures, est effectué au moins une fois par année, et plus si nécessaire. Des entretiens individuels sont également menés.

Ce processus inclut également une vérification des droits d'accès et des mesures prises en matière de protection des données. Les processus de traitement des données et leurs vérifications sont documentés par écrit et peuvent être présentés à tout moment. Les mesures techniques et organisationnelles sont vérifiées au moyen d'un formulaire de contrôle, lequel doit être examiné au moins une fois par année et, le cas échéant, adapté.

18. Audits

Le conseiller à la protection des données procède à des audits relatifs au traitement de données personnelles exigés légalement ou convenus contractuellement. Dans la mesure du possible, les personnes suivantes sont présentes lors de ces audits:

– le gérant de la CP OAM;
– la personne responsable de Diventa AG;
– les personnes responsables des sous-traitants.

Pour procéder à l'examen, la CP OAM autorise l'accès aux systèmes dans lesquels sont traitées des données personnelles, dans la mesure nécessaire et admissible, et sous réserve d'une urgence particulière, après un préavis approprié et pendant les heures de bureau.

Les audits sont documentés par écrit et signés par les personnes responsables des sous-traitants.

La CP OAM est habilitée à mettre les rapports d'audit et d'examen à la disposition d'autres personnes concernées.

19. Annonce des violations de la sécurité des données
En vertu de la LPD, il est obligatoire d'annoncer les violations de la sécurité des données. Si la caisse de pension identifie un tel incident, elle prend immédiatement les mesures adéquates pour y remédier ou en atténuer les conséquences.

Dans ce cas, le gérant de la CP OAM est l'interlocuteur principal. Dans un premier temps, il décide des mesures à prendre immédiatement. Les incidents en lien avec la protection des données et les mesures prises sont documentés.

Conformément aux dispositions légales, les personnes concernées et le Préposé fédéral à la protection des données et à la transparence (PFPDT) sont informés de l'incident.

20. Sensibilisation et formation des collaborateurs
Il est particulièrement important de sensibiliser les collaborateurs qui traitent des données personnelles. Tous les collaborateurs de la caisse de pension et tous les tiers mandatés par celle-ci qui traitent des données personnelles doivent signer une déclaration relative aux devoirs de diligence et respecter les règlements en matière de traitement des données. Le conseiller à la protection des données de la CP OAM est responsable du contenu des formations. Pour ce faire, il s'appuie sur la législation en vigueur et la pratique actuelle, et suit régulièrement des formations continues.

21. Concept d'effacement
Le concept d'effacement est régi par les art. 27*i* à 27*k* et 47 de l'ordonnance du 18 avril 1984 sur la prévoyance professionnelle vieillesse, survivants et invalidité (OPP 2; RS 831.441.1) et l'art. 958*f* de la loi fédérale du 30 mars 1911 complétant le Code civil suisse (livre cinquième: droit des obligations; RS 220).

22. Lacunes dans le règlement relatif à la protection des données de la CP OAM
Les prescriptions de la LPD s'appliquent aux cas pour lesquels le présent règlement relatif à la protection des données ne prévoit pas de dispositions.

Entrée en vigueur du règlement relatif à la protection des données

Le présent règlement relatif à la protection des données entre en vigueur le 25 avril 2025 et remplace toutes les versions antérieures.

Soleure, le 25 avril 2025

Caisse de pension des organisations d'assurance-maladie

Le conseil de fondation

Jean-Pierre Dubois
Président

Dr Reto Flury
Vice-président