AXA Fondation
Prévoyance professionnelle

Prévoyance professionnelle

Règlement relatif à la protection des données

AXA Fondation Prévoyance professionnelle, Winterthur

L1287.002-09.23

Le présent règlement sur la protection des données est édicté par le Conseil de fondation d'AXA Fondation Prévoyance professionnelle, Winterthur («la Fondation») sur la base du chiffre 2 de l'acte de fondation et du chiffre 10 du règlement d'organisation.

But
1

Les collaborateurs et collaboratrices, la clientèle, les personnes assurées, les destinataires de prestations et autres personnes dont la Fondation traite les données personnelles s'attendent à ce qu'elle qu'elle les gère de manière responsable et conforme à la loi.

Lors du traitement de données personnelles, la Fondation respecte les dispositions du droit applicable et du présent règlement sur la protection des données. Ce règlement définit les principes généraux régissant le traitement de données personnelles et est contraignant pour tous les organes de la Fondation ainsi que pour les collaborateurs et collaboratrices délégués au sein de la Fondation ou directement employés par celle-ci («**le personnel**»)

Cadre juridique
2

Les principales lois applicables en matière de traitement de données personnelles sont les suivantes:
- Loi fédérale sur la protection des données (LPD) et l'ordonnance correspondante
- Loi fédérale sur la prévoyance professionnelle vieillesse, survivants et invalidité (LPP) et les ordonnances correspondantes
- Loi fédérale sur le libre passage dans la prévoyance professionnelle vieillesse, survivants et invalidité (LFLP) et les ordonnances correspondantes

Obligation de garder le secret dans le cadre de la prévoyance professionnelle
3

L'obligation de garder le secret s'applique à toutes les informations détenues sur la situation personnelle et financière des personnes assurées et des employeurs. Les exigences spécifiques posées par l'art. 86a LPP sont respectées lors de la communication de données dans le domaine de la prévoyance professionnelle.

Notions et définitions
4

Les données personnelles et le traitement sont des notions centrales de la protection des données. Tout **traitement de données personnelles** est soumis aux prescriptions relatives à la protection des données selon le présent règlement.

Données personnelles
Les données personnelles sont des informations («données») qui se rapportent à une personne physique identifiée ou identifiable («personne concernée»). Elles présupposent donc un lien avec une personne; parfois, celui-ci n'apparaît toutefois clairement que dans le contexte concret. Le mode d'enregistrement des données personnelles, qu'il soit électronique ou sur un support physique, n'est pas important en l'espèce.

Exemples de données personnelles:
- Coordonnées telles que nom, prénom, adresse, adresse e-mail, numéro de téléphone
- Indications sur des caractéristiques, le comportement, les performances, l'état d'esprit, les préférences, les qualités, les opinions ainsi que sur les interactions sociales, familiales ou économiques
- Données d'identification telles qu'adresses IP, numéro de pièce d'identité, numéro AVS, numéro d'assuré ou empreinte digitale
- Images et sons permettant d'établir un lien avec la personne concernée

Traitement
Le traitement de données personnelles désigne au sens très large toute forme d'utilisation desdites données (électronique ou physique). Exemples:
- Conservation, enregistrement et archivage
- Collecte
- Accès
- Transmission/communication à des tiers (p. ex. en cas d'utilisation d'une solution cloud ou d'accès par un fournisseur de services externe)
- Évaluation/analyse
- Publication
- Suppression/destruction
- Anonymisation/pseudonymisation

En ligne, les données personnelles sont principalement traitées au moyen d'des outils de traçage, des médias sociaux et des cookies. Les applications comme les plates-formes de candidature, par exemple pour les élections au Conseil de fondation, contiennent toujours des données personnelles. La conservation de dossiers personnels implique, elle aussi, le traitement de données personnelles.

Données personnelles sensibles
Le traitement des données personnelles qui entrent dans la catégorie (exhaustive) des données personnelles sensibles est régi par des prescriptions plus sévères (voir ci-après).

L1287.002-09.23

Sont considérées comme sensibles les données personnelles qui se rapportent aux domaines suivants:
– Santé
– Religion
– Appartenance à une ethnie/race
– Convictions politiques/philosophiques
– Sphère intime (orientation/vie sexuelle)
– Opinions ou activités syndicales
– Données génétiques/biométriques
– Mesures d'aide sociale
– Poursuites pénales/infractions[1]

Profilage
Par profilage, on entend 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.

Profilage à risque élevé
Un profilage à risque élevé est un profilage qui entraîne un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, dans la mesure où il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique.

Principes 5

Équité
Les données personnelles sont traitées de manière équitable et uniquement comme la personne concernée est en droit de l'attendre.

Transparence
Lorsque des données personnelles sont fournies par la personne concernée elle-même ou recueillies auprès d'autres sources, la personne concernée est informée en temps utile et de manière active, détaillée et compréhensible sur le traitement de ses données personnelles.

Finalité
Les données personnelles ne peuvent être collectées que pour des finalités déterminées et reconnaissables pour la personne concernée. Elles ne doivent être traitées qu'en accord avec ces finalités. (Exemple: l'adresse e-mail indiquée dans un formulaire de contact ne doit pas être utilisée pour l'envoi d'une newsletter.)

Limitation des données
La collecte de données personnelles doit être limitée à ce qui est nécessaire. En outre, les données personnelles doivent être autant que possible anonymisées ou pseudonymisées. (Exemple: l'indication du nom et du prénom des personnes assurées n'est normalement pas nécessaire pour répondre à un courtier qui demande une offre pour le compte d'un employeur.)

Limitation de la conservation
La conservation des données personnelles doit se limiter à la durée nécessaire au regard des finalités pour lesquelles elles sont traitées. (Exemple: un module d'effacement garantit que les données personnelles sont supprimées après un certain temps.)

Exactitude
Les données personnelles doivent être exactes et tenues à jour.

Sécurité
Les données personnelles doivent être traitées de manière confidentielle et être protégées par des mesures techniques et organisationnelles adéquates contre la destruction non autorisée, la perte, la modification ou la divulgation non autorisée. (Exemples: journalisation, cryptage matériel d'appareils mobiles)

Base juridique
Une base juridique spécifique est requise pour le traitement de données dans les cas suivants: violation de l'un des principes énumérés ci-dessus, communication de données personnelles sensibles à des tiers ou traitement de données personnelles contre la volonté expresse de la personne concernée.

L1287.002-09.23

[1] Y c. poursuites ou sanctions administratives

Exemples de bases juridiques:
– Prescription légale, p. ex. délai de conservation légal pour les justificatifs comptables
– Relation directe avec la conclusion ou l'exécution d'un contrat avec une personne concernée par un traitement de données
– Intérêt prépondérant de la Fondation au traitement des données, c'est-à-dire intérêt de la Fondation si important qu'il prime les intérêts opposés de la personne concernée
– Consentement de la personne concernée

Dans le domaine de la prévoyance professionnelle, le traitement de données personnelles n'est autorisé que s'il existe une base légale correspondante. Une exception à cette règle est possible dans les situations où la personne concernée, en l'espèce, a consenti au traitement ou a rendu ses données accessibles à tout un chacun et ne s'est pas opposée formellement à leur traitement. Le consentement doit être explicite pour (i) tout traitement de données personnelles sensibles; (ii) un profilage à risque élevé hors du domaine de la prévoyance obligatoire; et (iii) tout profilage dans le domaine de la prévoyance obligatoire.

Il faut faire appel au conseiller ou à la conseillère à la protection des données de la Fondation dès lors qu'il n'est pas clair si les données doivent être traitées d'après une base légale ou juridique précise ou si une telle base est nécessaire au traitement de ces données.

Déclaration relative à la protection des données

6

Les personnes concernées doivent être informées de manière compréhensible et aisément accessible sur le traitement de leurs données personnelles, sauf par exemple lorsque le traitement est prévu par la loi.

L'information communiquée à la personne concernée doit au moins contenir les indications suivantes:
– Coordonnées de l'entité juridique responsable des données
– Finalité du traitement
– Destinataires ou catégories de destinataires
– État(s) destinataire(s) en cas de transmission de données à l'étranger
– Catégories de données en cas de collecte indirecte (pas auprès de la personne concernée)
– Modalités des décisions importantes prises de manière entièrement automatisée

Traitement de données personnelles sur mandat

7

Le traitement de données personnelles peut être confié à un prestataire en tant que gestionnaire de mandat. La Fondation continue de répondre du traitement des données personnelles à l'égard de la personne concernée. Le recours à un gestionnaire de mandat est soumis aux conditions suivantes:
– La personne choisie comme gestionnaire de mandat est en mesure de garantir la protection des données et la sécurité des données en particulier.
– La transmission de données personnelles à cette personne ne viole aucune obligation de garder le secret légale ou contractuelle.
– Avant toute transmission de données personnelles à la personne choisie comme gestionnaire de mandat, une convention ad hoc est conclue avec cette personne par écrit ou sous toute autre forme textuelle.
– En cas de mandat confié à un gestionnaire ayant son siège à l'étranger, les conditions du chiffre 8 doivent en outre être remplies.

En vertu de la convention correspondante, le gestionnaire de mandat doit notamment s'engager à traiter les données personnelles uniquement selon son mandat et les instructions de la Fondation, à ne pas les utiliser à d'autres fins et à garantir la sécurité du traitement des données. Le gestionnaire de mandat ne peut faire appel à des sous-traitants qu'avec l'accord de la Fondation.

Transmission à l'étranger

8

Des données personnelles ne peuvent être transmises à l'étranger que si l'État destinataire présente un niveau de protection des données adéquat ou si des mesures de protection particulières telles que des garanties contractuelles ont été prises.

Privacy by Design: annonce de traitements de données nouveaux, supprimés ou considérablement modifiés

9

Afin de garantir la conformité en matière de protection des données d'un processus, d'une application, d'un projet ou de toute autre activité ainsi que la mise en place des mesures nécessaires, la gérance de la Fondation doit impliquer le conseiller ou la conseillère à la protection des données le plus tôt possible en complétant la check-list «Analyse d'impact relative à la protection des données».

Exemples de traitements de données nouveaux ou considérablement modifiés:
– Utilisation d'un nouveau logiciel, d'une nouvelle application ou de certaines de ses fonctionnalités
– Mesures de marketing adaptées
– Analyse/évaluation/appariement nouveaux ou modifiés de données existantes pouvant être reliées à une personne
– Utilisation d'un logiciel ou d'une application pour collecter des données personnelles supplémentaires ou à de nouvelles fins

L1287.002-09.23

– Création de nouveaux fichiers
– Octroi d'un droit d'accès à distance à des données personnelles

Déclaration d'incidents

10

Tout soupçon ou cas avéré de violation de la protection des données doit être annoncé sans délai au conseiller ou à la conseillère à la protection des données de la Fondation (exemples: perte d'un smartphone ou d'un ordinateur portable sans cryptage matériel, envoi d'e-mails à des destinataires erronés). Le conseiller ou la conseillère à la protection des données décide de l'information des autorités et des personnes concernées et de la mise en œuvre d'autres mesures.

Conseiller à la protection des données de la Fondation:
Swiss Infosec AG
Centralstrasse 8A
6210 Sursee
Tél.: +41 (0)41 984 12 12
E-mail: datenschutzberater@infosec.ch

Transmission de demandes de personnes concernées

11

Les requêtes de personnes concernées souhaitant exercer leurs droits d'accès, à la rectification des données, d'opposition ou à la portabilité des données ou demandant la vérification de décisions individuelles automatisées ayant un lien avec leurs données personnelles doivent être transmises immédiatement au conseiller ou à la conseillère à la protection des données de la Fondation, qui coordonne la collecte des données dans les différents services et se charge de la communication avec les personnes concernées.

Organisation

12

Organes et collaborateurs et collaboratrices
Les organes et les collaborateurs et collaboratrices répondent, dans leurs domaines de compétence et d'activité respectifs, du respect des principes relatifs au traitement des données personnelles définis dans le présent règlement.

Maîtres des fichiers
Les maîtres des fichiers assument la responsabilité principale pour l'application des dispositions du droit de la protection des données et du présent règlement dans le cadre de leur fichier et du traitement des données. Ils veillent à la bonne documentation du traitement des données et, si nécessaire, à la réalisation d'une analyse d'impact relative à la protection des données.

Service informatique
Le service informatique prend les mesures techniques et organisationnelles nécessaires pour garantir la sécurité des données personnelles dans les systèmes d'information.

Conseiller ou conseillère à la protection des données
Le conseiller ou la conseillère à la protection des données de la Fondation a pour mission de donner des conseils impartiaux et de coordonner le respect de la protection des données à l'échelle de l'organisation. Afin de garantir que les obligations relevant du droit de la protection des données puissent être remplies dans les délais, parfois contraignants, il ou elle dépend de la transmission rapide et fluide des informations par tous les organes, collaborateurs et collaboratrices.

Le conseiller ou la conseillère à la protection des données apporte son soutien à la réalisation de l'analyse d'impact relative à la protection des données exigée par la loi, donne des conseils pour la tenue du registre des activités de traitement et l'établissement du règlement de traitement et coordonne les déclarations d'incidents et le respect des droits des personnes concernées. En outre, il ou elle s'assure que les personnes concernées soient suffisamment informées, comme l'exige le principe de la transparence dans le cadre du traitement des données. Si nécessaire, il ou elle met à jour et complète les informations sur la protection des données.

Sanctions

13

Le non-respect du présent règlement peut entraîner des conséquences disciplinaires, civiles ou pénales.

Disposition finale

14

Le présent règlement peut être complété par d'autres prescriptions ou règlements relatifs au traitement de données personnelles (p. ex. l'instruction applicable aux utilisateurs des services informatiques). Il entre en vigueur le 1er septembre 2023.

L1287.002-09.23