Was gilt es bei einem Datentransfer ins Ausland zu beachten?

Ein Datentransfer ist nur zulässig:[11]

- in ein Land mit einem vom Bundesrat anerkannten angemessenen Datenschutzniveau,
- wenn durch besondere Schutzmassnahmen ein geeigneter Datenschutz gewährleistet werden kann, oder
- wenn eine gesetzliche Ausnahme vorliegt, z. B. die betroffene Person ausdrücklich in die Bekanntgabe eingewilligt hat.

Ein Datentransfer in Länder der EU ist in der Regel unproblematisch, während bei einem Datentransfer in andere Länder weitere Abklärungen nötig sind. Bei einem Datentransfer ins Ausland sind auch die Versicherten zu informieren.[12]

Schweizer Vorsorgeeinrichtungen dürften ihre Daten regelmässig primär in der Schweiz bearbeiten. Dennoch ist zu prüfen, ob nicht doch (unbeabsichtigt) Personendaten ins Ausland übermittelt werden, z. B. in folgenden Konstellationen:

- Betriebseigene Pensionskassen mit IT-Anbindung an den Arbeitgeber,
- Beauftragung und Bearbeitung von Personendaten durch einen Dienstleister,
- Datenspeicherung in Cloud-Lösungen,
- Erbringen von Vorsorgeleistungen ins Ausland.

Diesfalls wäre zu prüfen, ob die Bekanntgabe im konkreten Fall den Anforderungen des revDSG genügt und zulässig ist.

[11] Art. 16 f. revDSG; Art. 8 ff. DSV; Die Liste der Länder mit angemessenem Datenschutz findet sich in Anhang 1 der DSV.

[12] Art. 19 Abs. 4 DSG.

Relations avec des tiers

Échange de données avec des prestataires de services

Les institutions de prévoyance sont en relation avec un grand nombre de tiers avec lesquels un échange de données a souvent lieu. Nous nous penchons sur la question de savoir à quoi il faut faire attention sous l'angle de la protection des données lors de l'échange de données avec des tiers.

Il convient tout d'abord de déterminer quelles sont les réglementations applicables: dans la prévoyance obligatoire (et enveloppante), il s'agit en premier lieu de respecter l'obligation de garder le secret ancrée à l'art. 86 LPP, avec les exceptions définies aux art. 85a, 85b et 86a et suivants LPP. Selon l'art. 86 LPP, les personnes qui participent à l'application ainsi qu'au contrôle ou à la surveillance de l'application de la LPP sont tenues de garder le secret vis-à-vis des tiers. Cette obligation s'applique également aux tiers mandatés. Dans la prévoyance professionnelle plus étendue, ce sont par contre les moyens de droit civil de la protection de la personnalité[1] et la protection du secret professionnel prévue par le droit de la protection des données qui s'appliquent.[2]

En matière de protection des données, les institutions de prévoyance qui appliquent le régime obligatoire (et donc aussi les institutions de prévoyance enveloppantes) et les institutions de libre passage sont considérées comme des organes fédéraux.[3] Une base légale est nécessaire pour un traitement de données par des organes fédéraux[4], qui existe notamment avec les art. 85a ss LPP et l'art. 25 LFLP. Les dispositions du droit de la protection des données sont applicables à titre complémentaire.

En revanche, les caisses de pensions offrant exclusivement des prestations surobligatoires ou extra-obligatoires, telles que les fondations 1e et les fondations patronales, sont considérées comme des personnes privées. Elles sont soumises aux dispositions du droit de la protection des données et peuvent traiter des données personnelles même sans base légale si la personnalité des personnes concernées n'est pas atteinte ou s'il existe des motifs justificatifs.

Cette distinction existe déjà dans la législation actuelle sur la protection des données. Ce qui est nouveau, c'est par exemple que les organes fédéraux – à la

[1] Art. 28 du Code civil.

[2] Art. 35 LPD; art. 62 nLPD.

[3] Selon l'art. 5 let. i, de la LPD révisée, un organe fédéral est une autorité ou un service de la Confédération ou une personne chargée de tâches publiques de la Confédération.

[4] Art. 34, 1er alinéa, de la loi révisée sur la protection des données.

différence des personnes privées – doivent annoncer leur liste d'activités de traitement au Préposé fédéral à la protection des données et à la transparence (PFPDT)[5] et nommer un conseiller à la protection des données[6].

Quand y a-t-il un traitement pertinent de données personnelles?

Il convient de préciser tout d'abord que les dispositions relatives à la protection des données ne s'appliquent que lorsque des données personnelles sont traitées. Toute manipulation de données personnelles est une opération de traitement pertinente au sens de la loi sur la protection des données.[7]

Les données personnelles sont des données qui se rapportent à une personne physique identifiée ou identifiable[8]. C'est le cas lorsqu'une partie peut identifier une personne individuelle sur la base des données transmises ou avec les données dont elle dispose par ailleurs.

Si des données individuelles sont pseudonymisées, c'est-à-dire que le nom est par exemple remplacé par un numéro, et que le tiers ne dispose pas de la clé permettant d'attribuer les numéros aux différents individus, les données pseudonymisées ne sont pas, du point de vue de ce tiers, des données personnelles au sens du droit de la protection des données. Les explications ci-après s'appliquent au traitement des données personnelles.

Le tiers agit-il en tant que contrôleur ou en tant que processeur?

Du point de vue de la protection des données, les traitements de données sont effectués soit sous sa propre responsabilité (en tant que contrôleur), soit en tant que sous-traitant (processeur). Le responsable est une personne privée ou un organe fédéral qui, seul ou avec d'autres, décide de la finalité (le pourquoi?) et des moyens (le comment?) du traitement[9]. Le sous-traitant est une personne privée ou un organe fédéral qui traite des données personnelles pour le compte du responsable.[10]

[5] Art. 12 al. 4 de la loi révisée sur la protection des données.

[6] Art. 25 et suivants. OPDo.

[7] Art. 5 let. d de la loi révisée sur la protection des données, c'est-à-dire notamment la collecte, la transmission, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données personnelles.

[8] Art. 5 let. a de la loi révisée sur la protection des données.

[9] Art. 5 let. j de la loi révisée sur la protection des données.

[10] Art. 5 let. k de la loi révisée sur la protection des données.

TAKE AWAYS

- Suite à la révision du droit de la protection des données, l'échange de données personnelles avec des tiers requiert une attention particulière.
- La distinction, et donc la qualification du tiers en tant que responsable ou sous-traitant, est importante, car le responsable a des obligations plus étendues.
- Il est recommandé au responsable de vérifier les exigences en matière de sécurité des données avant de faire appel à un sous-traitant et de se faire accorder par contrat le droit de procéder à des contrôles périodiques.
- Un transfert de données vers des pays de l'UE ne pose généralement pas de problème, alors que des clarifications supplémentaires seront nécessaires pour un transfert de données vers d'autres pays.

La délimitation peut être difficile dans certains cas. Tous les rapports de mandat de droit civil ne font pas du tiers un sous-traitant. Ce n'est le cas que si le tiers ne peut pas décider librement de la finalité et des moyens du traitement. Ainsi, par exemple, l'avocat externe travaille certes sur la base d'un rapport de mandat de droit civil, mais il décide néanmoins librement quelles données il traite pour quelle raison et de quelle manière pour

répondre à une question juridique qui se pose. Il en va de même pour l'expert en caisses de pensions et l'organe de révision qui ont leurs propres mandats légaux dans l'exercice desquels ils décident sous leur propre responsabilité du traitement des données.

La situation est différente, par exemple, dans le cas d'un tiers qui exécute la gestion technique de l'institution de prévoyance sur la base d'un mandat. Dans ce cas, le tiers reprend la tâche de l'institution de prévoyance et traite les données en tant que prolongement de l'institution de prévoyance, conformément aux dispositions légales et réglementaires applicables à l'institution de prévoyance et à sa place.

Quelle est la conséquence de cette qualification?

Pourquoi cette distinction, et donc la qualification du tiers en tant que responsable ou sous-traitant, est-elle importante? Les principales différences sont résumées dans le tableau (non exhaustif).

Il en résulte que le responsable a des obligations beaucoup plus étendues et qu'il assume la responsabilité globale du traitement des données, y compris pour le sous-traitant. Il est conseillé au responsable de vérifier les exigences en matière de sécurité des données avant de mandater un sous-traitant (diligence raisonnable, référence à une certification) et de se faire accorder contractuellement le droit de procéder à des contrôles périodiques (droits d'audit).

A quoi faut-il faire attention lors d'un transfert de données à l'étranger?

Un transfert de données n'est autorisé que[11]

- vers un pays dont le niveau de protection des données est reconnu comme adéquat par le Conseil fédéral,
- lorsqu'une protection appropriée des données peut être assurée par des mesures de protection particulières, ou
- lorsqu'il existe une exception légale, par exemple lorsque la personne concernée a expressément consenti à la communication.

[11] Art. 16s. nLPD; art. 8ss. OPDo; la liste des pays disposant d'une protection des données adéquate se trouve à l'annexe 1 de l'OPDo.

Un transfert de données dans les pays de l'UE ne pose généralement pas de problème, tandis qu'un transfert de données dans d'autres pays nécessite des clarifications supplémentaires. En cas de transfert de données à l'étranger, les assurés doivent également être informés.[12]

En règle générale, les institutions de prévoyance suisses vont sans doute traiter leurs données en premier lieu en Suisse. Il convient néanmoins de vérifier si des données personnelles ne sont pas (involontairement) transmises à l'étranger, par exemple dans les cas de figure suivants:

- caisses de pensions propres à l'entreprise avec connexion informatique à l'employeur,
- la délégation et le traitement des données personnelles par un prestataire de services,
- stockage des données dans des solutions en nuage,
- fourniture de prestations de prévoyance à l'étranger.

Dans ce cas, il faudrait vérifier si la communication répond aux exigences de la LPD révisée et si elle est autorisée dans le cas concret.

Evelyn Schilter
Estelle Caveng

[12] Art. 19 al. 4 LPD.

Délimitation entre responsable et sous-traitant

Responsable	– Reste responsable du traitement des données, même s'il le confie à un sous-traitant. Le transfert doit se faire sur la base d'un contrat («Controller to Processor Agreement») ou d'une loi.[1] – En cas de transfert des données à un responsable, la responsabilité du cédant concernant le traitement par le tiers prend fin au moment du transfert au tiers. Le tiers repreneur est lui-même responsable du traitement correct. – Le traitement des données doit être conçu sur le plan technique et organisationnel de manière à respecter les prescriptions en matière de protection des données. Le tiers repreneur doit: – procéder à des préréglages favorables à la protection des données (art. 7 nLPD). – s'assurer que le sous-traitant est en mesure de garantir la sécurité des données (art. 9 al. 2 nLPD). – informer les personnes concernées sur le traitement, en particulier aussi sur une communication à l'étranger (art. 19 ss. nLPD). – réaliser des analyses d'impact sur la protection des données (art. 22 et suivants de la loi révisée sur la protection des données). – informer le PFPDT et/ou les personnes concernées d'une violation de la sécurité des données (art. 24 nLPD). – sur demande d'une personne concernée: renseigner sur le traitement des données ou sur la remise/transmission des données (art. 25 ss. nLPD).
Responsable et responsable du traitement des commandes	– Liste des activités de traitement. Il existe des différences en ce qui concerne les contenus qui doivent figurer dans le registre.[2] – Garantir une sécurité des données adaptée au risque par des mesures techniques et organisationnelles appropriées. Les mesures doivent permettre d'éviter toute violation de la sécurité des données.[3]
Responsable du traitement de la commande	– Ne peut traiter les données que comme le responsable serait lui-même autorisé à le faire et seulement si aucune obligation légale ou contractuelle de confidentialité n'interdit la transmission. – Ne peut, pour sa part, confier le traitement à un tiers qu'avec l'autorisation préalable du responsable (art. 9 al. 3 LPD révisée, art. 7 OPDo). – Annonce au responsable une violation de la sécurité des données (art. 24 al. 3 nLPD).

[1] Art. 9 al. 1 nLPD: en cas de transfert à un responsable, la conclusion d'une convention (Controller to Controller Agreement) n'est pas obligatoire, mais recommandée.

[2] Art. 12 nLPD: l'art. 12 al. 2 nLPD prescrit le contenu minimal pour le registre des traitements d'un responsable, l'art. 12 al. 3 nLPD prescrit le contenu du registre des traitements du sous-traitant.

[3] Art. 8 nLPD et art. 1ss. OPDo: des exigences accrues s'appliquent aux traitements automatisés (cf. obligations de journalisation et d'édiction d'un règlement de traitement selon les art. 4 ss. OPDo).