Revision des Datenschutzgesetzes (DSG)

Handlungsbedarf für die berufliche Vorsorge

Der Gesetzgeber ist durch die Revision des Datenschutzgesetzes (DSG) und dessen Harmonisierung mit den Datenschutzbestimmungen des BVG gefordert.

IN KÜRZE

Eine gesetzliche Grundlage für das Bearbeiten von Personendaten, wie in Art. 85a E-BVG vorgesehen, ist auch für die Träger der weitergehenden, über- und ausserobligatorischen beruflichen Vorsorge nötig.

Yolanda Müller
Rechtsanwältin,
CAS Berufliche Vorsorge (IRP-HSG), Basel

Am 25. Mai 2018 ist die Datenschutzgrundverordnung (DSGVO) in der EU in Kraft getreten.[1] Der Schweizerische Pensionskassenverband ASIP erachtet die Auswirkungen der DSGVO auf schweizerische Pensionskassen als gering, auch wenn vereinzelt ein Handlungsbedarf zu prüfen ist.[2]

Einschneidender für die Einrichtungen der beruflichen Vorsorge ist dagegen die laufende Revision des Datenschutzgesetzes des Bundes (DSG).[3] Hintergrund der Revision ist mitunter, dass die EU die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau für künftige grenzüberschreitende Datenübermittlungen anzuerkennen hat.

Viele Fragen zur Revision sind noch unklar. Das E-DSG sieht unter anderem erhöhte Informationspflichten und Anforderungen an die Datenbeschaffung, -bearbeitung, -aufbewahrung und Dokumentationspflichten vor. Auch eine Datenschutzfolgeabschätzung und eine Meldepflicht bei unbefugter Datenbearbeitung beziehungsweise bei Datenverlust an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) sollen eingeführt werden. Verstösse sollen mit einer Busse bis zu 250 000 Franken mit einer persönlichen Haftung der verantwortlichen Personen sanktioniert werden.

Verhältnis der Datenschutzbestimmungen des BVG zum DSG

Das DSG ist auf Vorsorgeeinrichtungen soweit anwendbar, als es nicht durch die spezifischen Datenschutznormen des BVG (Art. 85a ff. BVG) und FZG (Art. 25) verdrängt wird.

Die Art. 85a ff. BVG regeln das Bearbeiten von Personendaten, die Akteneinsicht, die Schweigepflicht, die Datenbekanntgabe, die Information der Versicherten und die Amts- und Verwaltungshilfe. Diese spezifischen Datenschutzbestimmungen des BVG gelten für die obligatorische berufliche Vorsorge, nicht jedoch für die weitergehende, über- und ausserobligatorische berufliche Vorsorge.[4] Letztere unterstehen «nur» den

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutze natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 96/46/EG (Datenschutz-Grundverordnung).

[2] Zum Beispiel bei IT-Anbieter/Server in der EU oder Gesundheitsdaten von Grenzgängern. Fachmitteilung Nr. 111 vom 22. Mai 2018 des ASIP; Basile Cardinaux, Revision des Datenschutzes, Bedeutung für die Schweizer Vorsorgeeinrichtungen, SPV 8/17, S. 88 f.

[3] Botschaft des Bundesrats zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941 (abrufbar unter https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html). Das Parlament teilte die Vorlage auf. Die Revision des Bundesgesetzes über den Datenschutz (DSG) wird zurzeit in den vorberatenden parlamentarischen Kommissionen behandelt.

[4] Kein Verweis in den Katalogen von Art. 49 Abs. 2 BVG (umhüllende Kassen) und Art. 89a Abs. 6 und 7 ZGB (Personalfürsorgestiftungen mit und ohne reglementarische Leistungen) mit Ausnahme von Verweisen auf die Verwendung, Bearbeitung und Bekanntgabe der AHV-Versichertennummer und die Information der Versicherten; Basile Cardinaux, a.a.O., S. 89; OFK-Vetter, BVG 86a N 3 ff.

Bestimmungen des DSG. Zur über- und ausserobligatorischen Vorsorge zählen zum Beispiel Einrichtungen mit 1e- oder Kaderplänen, die Stiftung FAR, Wohlfahrtsfonds mit Ermessensleistungen oder Einrichtungen der Säule 3a.

Sie alle sind für ihre vielfältigen Aufgaben auf das Bearbeiten von besonders schützenswerten Personendaten angewiesen. Der Umgang mit Daten über die Gesundheit, Löhne, Ersatzeinkommen gehört zu ihrem Alltag. Sie müssen Leistungsfälle beurteilen und reglementarische oder Ermessensleistungen ausrichten, Verteilpläne erstellen, die Gebote der Gleichbehandlung und der Angemessenheit gegenüber ihren Versicherten beachten, Beiträge erheben, den Informationsverkehr mit ihren Organen (Experte, Revisionsstelle), der Aufsichtsbehörde und anderen Sozialversicherungsträgern sicherstellen. Nicht immer können sie sich dabei auf eine bestehende klare gesetzliche Grundlage stützen[5] oder vorgängig eine Einwilligung des Versicherten/Destinatärs einholen.

Aber auch Einrichtungen, welche die obligatorische Vorsorge betreiben, müssen das DSG beachten. So hielt das Bundesverwaltungsgericht fest, dass die Bestimmungen des DSG ergänzend zum BVG anwendbar sind. Es beurteilte den Versand von unverschlossenen Vorsorgeausweisen an den Arbeitgeber zur Verteilung an die Versicherten als Verstoss gegen das geltende DSG.[6]

Gesetzliche Grundlage für die Bearbeitung von Personendaten

Das DSG unterscheidet zwischen Vorschriften für Bundesorgane und solchen für private Personen. Soweit privatrechtliche Vorsorgeeinrichtungen die obligatorische Vorsorge und damit zwingendes Recht durchführen, gelten sie als Bundesorgane. Sie benötigen damit eine gesetzliche Grundlage für ihr Handeln.[7]

Private Personen, das heisst auch Einrichtungen der über- und ausserobligatorischen Vorsorge, dürfen Persönlichkeitsdaten ohne widerrechtliche Verletzung bearbeiten. Keine widerrechtliche Verletzung liegt unter anderem vor, wenn diese durch eine Einwilligung der betroffenen Person oder durch das Gesetz gerechtfertigt ist.[8]

Auch die Informationspflicht bei der Beschaffung von Personendaten entfällt, wenn die Bearbeitung gesetzlich vorgesehen ist.[9]

Die Datenfolge-Abschätzung ist neu bei der Bearbeitung von besonders schützenswerten Personendaten vorgesehen. Von ihr wird bei Erfüllung einer gesetzlichen Pflicht abgesehen.[10]

Umso mehr ist künftig für Einrichtungen der über- und ausserobligatorischen Vorsorge eine klare gesetzliche Grundlage für die Bearbeitung von Personendaten im Sinne der Rechtssicherheit unumgänglich.[11] Diskussionen wären damit aus datenschutzrechtlicher Optik vom Tisch, ob die jetzigen gesetzlich oder reglementarisch normierten oder gar im Ermessen des Stiftungsrats stehenden Aufgaben dieser Einrichtungen dafür ausreichend sind.

Bedauerlicherweise wurde im E-DSG die gesetzliche Grundlage nur für das BVG-Obligatorium angepasst, jedoch keine für den weitergehenden, über- und ausserobligatorischen Bereich geschaffen. Die zuständigen Organe werden im Obligatorium zur Erfüllung ihrer Aufgaben neu explizit befugt, Personendaten, die namentlich die Beurteilung der Gesundheit, der Schwere des physischen oder psychischen Leidens, der Bedürfnisse und der wirtschaftlichen Situation der versicherten Person erlauben, zu bearbeiten oder bearbeiten zu lassen.[12] Solche Datenbearbeitungen könnten einen schwerwiegenden Eingriff in die Grundrechte der betroffenen Person mit sich bringen. Auch dies zeigt, dass Einrichtungen der weitergehenden, über- und ausserobligatorischen Vorsorge über eine entsprechende gesetzliche Grundlage für die reibungslose Bewältigung ihrer Arbeiten verfügen sollten.

Gesetzessystematik überdenken

Es ist im Rahmen der Revision des DSG sicherzustellen, dass die Abwicklung und Verwaltung der beruflichen Vorsorge wie bisher reibungslos und rationell vorgenommen werden kann. Verschiedene Bestimmungen des E-DSG erscheinen diesbezüglich hinderlich und sind im Gesetzgebungsprozess zu überprüfen.

Für die Erfüllung ihrer Kernaufgaben sollten sich auch Einrichtungen der weitergehenden, über- und ausserobligatorischen Vorsorge auf die datenschutzrechtlichen Bestimmungen des BVG als lex specialis stützen können, wie von verschiedenen Branchenverbänden in der Vernehmlassung zum VE-DSG angeregt wurde.[13] Eine Ausdehnung der Datenschutzbestimmungen des BVG auf alle Träger der beruflichen Vorsorge ist zu prüfen. Sie könnten durch entsprechende Verweise in den Scharnierbestimmungen von Art. 49 Abs. 2 BVG und Art. 89a Abs. 6 und 7 ZGB beziehungsweise Art. 82 BVG relativ einfach bewerkstelligt werden.

[5] Zum Beispiel bei der Verteilung von freien Mitteln oder Härtefallleistungen.
[6] BVGer A-4467/2011 vom 10. April 2012, E. 4.3, 4.4. und 11.
[7] Art. 30 E-DSG.
[8] Art. 26 und 27 E-DSG.
[9] Art. 18 Abs. 1 lit. b E-DSG.
[10] Art. 20 Abs. 4 E-DSG.
[11] So für Wohlfahrtsfonds mit Ergänzungsleistungen (mittels neuem Verweis in Art. 89a Abs. 7 ZGB).
[12] Art. 85a E-DSG; BBl 2017 7145.
[13] Art. 85a–87 BVG.

Révision de la loi sur la protection des données (LPD)

La prévoyance professionnelle doit réagir

Le législateur a fort à faire avec la révision de la loi sur la protection des données (LPD) et son harmonisation avec les dispositions de la LPP relatives à la protection des données.

EN BREF

Un cadre légal pour le traitement des données personnelles, tel qu'il est prévu à l'art. 85a P-LPP, est également nécessaire pour les organes de la prévoyance professionnelle plus étendue, sur- et extra-obligatoire.

Le Règlement général sur la protection des données (RGPD) est entré en vigueur dans l'UE le 25 mai 2018.[1] L'Association suisse des institutions de prévoyance (ASIP) estime que l'impact du RGPD sur les caisses de pension suisses est faible, même si certaines actions isolées doivent être examinées.[2]

La révision en cours de la loi fédérale sur la protection des données (LPD) est en revanche plus déterminante pour les institutions de prévoyance professionnelle.[3] Cette révision a notamment pour objectif que l'UE continue de reconnaître la Suisse comme un État tiers ayant un niveau adéquat de protection des données pour les futurs transferts transfrontaliers de données.

De nombreuses questions concernant la révision n'ont pas encore été tranchées. Le P-LPD prévoit notamment des devoirs d'information accrus et des exigences concernant la collecte, le traitement et la conservation des données et les obligations de documentation. Une analyse d'impact relative à la protection des données et une obligation de déclarer au Préposé fédéral à la protection des données et à la transparence (PFPDT) en cas de traitement non autorisé de données ou de perte de données doivent également être introduites. Les infractions doivent être sanctionnées par une amende jusqu'à 250 000 francs et une responsabilité personnelle des personnes responsables.

Rapport entre les dispositions en matière de protection des données de la LPP et la LPD

La LPD est applicable aux institutions de prévoyance dans la mesure où elle n'est pas supplantée par des normes spécifiques en matière de protection des données de la LPP (art. 85a ss LPP) et de la LFLP (art. 25).

Les art. 85a ss LPP règlent le traitement de données personnelles, la consultation du dossier, l'obligation de garder le secret, la communication de données, l'information des assurés et l'entraide administrative. Ces dispositions spécifiques en matière de protection des données de la LPP s'appliquent à la prévoyance professionnelle obligatoire, mais non à la prévoyance professionnelle plus étendue,

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[2] Par exemple, en cas de prestataires/serveurs informatiques dans l'UE ou concernant les données en matière de santé des frontaliers. Circulaire d'information n° 111 de l'ASIP du 22 mai 2018; Basile Cardinaux, Revision des Datenschutzes, Bedeutung für die Schweizer Vorsorgeeinrichtungen, SPV 8/17, pp. 88 s.

[3] Message du Conseil fédéral concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, FF 2017 6565 (consultable sur https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html). Le Parlement a scindé le projet. La révision de la loi fédérale sur la protection des données (LPD) est actuellement examinée dans les commissions parlementaires chargées de l'examen préalable.

sur- et extra-obligatoire.[4] Ces dernières sont «uniquement» soumises aux dispositions de la LPD. La prévoyance sur- et extra-obligatoire inclut par exemple les institutions avec des plans 1e ou pour cadres, la fondation FAR, les fonds de bienfaisance fournissant des prestations facultatives ou les institutions du pilier 3a.

Tous ces organismes doivent traiter des données personnelles sensibles pour mener à bien leurs multiples tâches. Ils gèrent quotidiennement des données sur la santé, les salaires ou les revenus de substitution. Ils doivent apprécier des cas de prestations et verser des prestations réglementaires ou facultatives, établir des plans de répartition, respecter les principes de l'égalité de traitement et du caractère approprié vis-à-vis de leurs assurés, percevoir des cotisations, assurer l'échange d'informations avec leurs organes (experts, organe de révision), l'autorité de surveillance et d'autres organismes d'assurance sociale. Ils ne peuvent pas toujours s'appuyer sur une base légale explicite existante[5] ou demander préalablement le consentement de l'assuré/du destinataire.

Mais les institutions qui pratiquent la prévoyance obligatoire doivent également respecter la LPD. Ainsi, le Tribunal administratif fédéral a retenu que les dispositions de la LPD étaient applicables en complément à la LPP. Il a considéré l'envoi de certificats de prévoyance sous pli non fermé à l'employeur en vue de la distribution aux assurés comme une infraction à la LPD en vigueur.[6]

Base légale pour le traitement des données personnelles

La LPD distingue entre prescriptions ciblant les organes fédéraux et les personnes privées. Dans la mesure où des institutions de prévoyance de droit privé exécutent la prévoyance obligatoire et donc le droit impératif, elles sont considérées comme des organes fédéraux. Elles ont par conséquent besoin d'une base légale pour leur action.[7]

Les personnes privées, c'est-à-dire également les institutions de prévoyance sur- et extra-obligatoire, peuvent traiter les données à caractère personnel sans atteinte illicite. Il n'y a notamment pas d'atteinte illicite quand celle-ci est justifiée par le consentement de la personne concernée ou par la loi.[8]

L'obligation d'informer lors de la collecte de données personnelles est également annulée lorsque le traitement est prévu par la loi.[9]

L'analyse d'impact relative à la protection des données est désormais prévue lors du traitement de données personnelles sensibles. Elle ne s'applique pas en cas d'exécution d'une obligation légale.[10]

Une base légale claire pour le traitement des données personnelles dans le sens d'une sécurité juridique sera d'autant plus indispensable à l'avenir pour les institutions de la prévoyance sur- et extra-obligatoire.[11]

Les discussions visant à savoir si les tâches actuelles de ces institutions normalisées par la loi ou le règlement, voire laissées à la discrétion du conseil de fondation, sont suffisantes à cet égard seraient ainsi balayées dans l'optique de la protection des données.

Malheureusement, le cadre légal n'a été adapté que pour le régime LPP obligatoire dans le P-LPD et aucune base légale n'a été créée pour le domaine plus étendu, sur- et extra-obligatoire. Pour l'accomplissement de leurs missions, les organes compétents dans le régime obligatoire sont désormais explicitement autorisés à traiter ou à faire traiter les données personnelles qui permettent notamment d'évaluer la santé, la gravité d'une atteinte physique ou psychique, des besoins et de la situation économique de la personne assurée.[12] De tels traitements de données peuvent entraîner une atteinte grave aux droits fondamentaux de la personne concernée. Cela montre aussi que les institutions de la prévoyance plus étendue, sur- et extra-obligatoire devraient disposer d'un cadre légal correspondant pour accomplir leur travail à la perfection.

Revoir la systématique de la loi

Dans le cadre de la révision de la LPD, il faut s'assurer que l'exécution et la gestion de la prévoyance professionnelle puissent être réalisées sans problème et de façon rationnelle comme précédemment. Différentes dispositions du P-LPD semblent constituer un obstacle à cet égard et doivent être vérifiées dans le cadre du processus législatif.

Pour l'exécution de leurs missions de base, les institutions de la prévoyance plus étendue, sur- et extra-obligatoire, devraient également pouvoir s'appuyer sur les dispositions en matière de protection des données de la LPP en qualité de lex specialis, comme l'ont suggéré différentes associations de branche dans le cadre de la consultation sur l'AP-LPD.[13] Une extension des dispositions en matière de protection des données de la LPP à tous les organes de la prévoyance professionnelle doit être examinée. Elle serait assez facile à mettre en œuvre grâce à des renvois correspondants dans les dispositions charnières de l'art. 49 al. 2 LPP, de l'art. 89a al. 6 et 7 CC et de l'art. 82 LPP.

Yolanda Müller

[4] Aucun renvoi dans les catalogues de l'art. 49 al. 2 LPP (caisses enveloppantes) et de l'art. 89a al. 6 et 7 CC (institutions de prévoyance en faveur du personnel avec et sans prestations réglementaires), à l'exception de renvois à l'utilisation, au traitement et à la communication du numéro d'assuré AVS et de l'information des assurés; Basile Cardinaux, op. cit., p. 89; OFK-Vetter, BVG 86a N 3 ss.

[5] Par exemple, lors de la distribution de fonds libres ou de prestations en cas de rigueur.

[6] TAF A-4467/2011 du 10 avril 2012, consid. 4.3, 4.4. et 11.

[7] Art. 30 P-LPD.

[8] Art. 26 et 27 P-LPD.

[9] Art. 18 al. 1 let. b P-LPD.

[10] Art. 20 al. 4 P-LPD.

[11] C'est le cas pour les fonds de bienfaisance avec prestations complémentaires (grâce au nouveau renvoi à l'art. 89a al. 7 CC).

[12] Art. 85a P-LPD; FF 2017 6759.

[13] Art. 85a à 87 LPP.