Datenschutz

Versichertendaten gehen den Arbeitgeber nichts an

Es ist datenschutzrechtlich problematisch, dass Arbeitgeber die Vorsorgeausweise zusammen mit den Lohnausweisen versenden. Eine entsprechende Empfehlung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) hat Auswirkungen auf die Verwaltungsorganisation der Vorsorgeeinrichtung.

Beim Datenschutzbeauftragten waren Anzeigen eingegangen, weil eine Vorsorgeeinrichtung die persönlichen Vorsorgeausweise nicht direkt an die versicherte Person, sondern an die Adresse des Arbeitgebers sandte, der sie anschliessend verteilte. Von einer Verletzung des Datenschutzes ausgehend, suchte der EDÖB den Kontakt mit der Vorsorgeeinrichtung, doch kam es nicht zu einer Einigung. Schliesslich erliess der EDÖB die Empfehlung: «Die Einrichtung X stellt die von ihr praktizierte Datenbekanntgabe der Pensionskassenausweise der bei ihr versicherten Personen an den Arbeitgeber unverzüglich ein (…).»[1]

In Kürze

> Wird den datenschutzrechtlichen Normen konsequent nachgelebt, gelangt der Arbeitgeber über die Vorsorgeeinrichtung nicht an ihm nicht zustehende Versichertendaten

> Eine Bekanntgabe spezifischer Personendaten aus konkretem Anlass setzt eine entsprechende Bevollmächtigung voraus

[1] Empfehlung des EDÖB vom 8.7.2009, publiziert auf der Homepage des EDÖB (www.edoeb.admin.ch).

Geschütztes Rechtsgut

Pensionskassenausweise enthalten neben den Stammdaten und dem versicherten Lohn auch Projektionen von Leistungen in den Vorsorgefällen Alter, Invalidität und Tod, Angaben zum vorhandenen Altersguthaben, zu Bezügen zum Erwerb von Wohneigentum, allenfalls auch zu Einkäufen und möglicherweise auch zu gesundheitsbedingten Leistungsvorbehalten. Insbesondere Angaben, die einen Zusammenhang mit der Gesundheit aufweisen oder Rückschlüsse auf diese zulassen, gelten datenschutzrechtlich als besonders schützenswerte Personendaten.[2]

Gemäss Art. 328b OR darf der Arbeitgeber Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrags erforderlich sind. Nicht zu solchen Daten gehören in der Regel Informationen zu persönlichen Verhältnissen, Eigenschaften und Neigungen. Von einer Bearbeitung ausgeschlossen sind auch Lohndaten früherer Arbeitsverhältnisse. Der Arbeitgeber hat kein Anrecht auf Informationen über die persönlichen Vermögensverhältnisse und auf Gesundheitsdaten.[3] Haben der Arbeitgeber und möglicherweise auch der direkte Vorgesetzte Kenntnis von solchen Personendaten, so kann sich dies negativ auf das berufliche Fortkommen auswirken. Denkbar ist zudem, dass die konkreten Vorsorgeverhältnisse als eines der Kriterien dafür herangezogen werden, ob im Rahmen einer Restrukturierungsmassnahme das Arbeitsverhältnis mit einem bestimmten Arbeitnehmer aufgelöst werden soll. Die Datenschutzgesetzgebung will verhindern, dass der Arbeitgeber Zugang zu solchen sachwidrigen Entscheidgrundlagen erhält. Er soll sie sich auch nicht über eine Auswertung von Informationen der Vorsorgeeinrichtung beschaffen können.

[2] Art. 3 lit. c Ziff. 1 Bundesgesetz über den Datenschutz (DSG; SR 235.1).

[3] S. Empfehlung des EDÖP vom 8.7.2009 (FN 1) m.w.H.

Datenbekanntgabe an Dritte

Die Vorsorge wird von einer vom Arbeitgeber unabhängigen, mit eigener Rechtspersönlichkeit ausgestatteten Einrichtung geführt. Ihr gegenüber ist der Arbeitgeber als Dritter zu betrachten.

Seit 2000 bestehen für alle Sozialversicherer einheitliche Regelungen zur Schweigepflicht.[4] In der beruflichen Vorsorge regelt Art. 86a BVG die Datenbekanntgabe an Dritte. An den Arbeitgeber dürfen Personendaten nur gestützt auf Art. 86a Abs. 5 lit. b BVG weitergegeben werden, wenn die betroffene Person im Einzelfall schriftlich eingewilligt hat oder

[4] Kurt Pärli, in: Jacques-André Schneider/Thomas Geiser/Thomas Gächter (Hrsg.), BVG und FZG, Bern 2010, Art. 86a BVG N 1.

Autor

Kurt C. Schweizer
Dr. iur., Rechtsanwalt, Schweizer Neuenschwander & Partner

wenn eine nicht einholbare Einwilligung vorausgesetzt werden darf. Das Erfordernis der Einwilligung im Einzelfall entspricht der Voraussetzung von Art. 19 Abs. 1 lit. b DSG, unter denen Bundesbehörden Personendaten bekannt geben dürfen. Das ist insofern konsequent, als Vorsorgeeinrichtungen im Obligatoriumsbereich mit einer öffentlichen Aufgabe des Bundes betraut sind und somit als Bundesorgane im Sinne von Art. 3 lit. h DSG gelten.[5] Personendaten danach zu unterscheiden, ob sie das Obligatorium beziehungsweise den überobligatorischen Bereich betreffen, ist nicht praktikabel, und diese strengen Anforderungen sind auch von umhüllenden Vorsorgeeinrichtungen zu beachten.[6]

Für rein überobligatorische Einrichtungen gelangt Art. 86a BVG, da nicht in Art. 89bis Abs. 6 ZGB aufgelistet[7], nicht zur Anwendung, und sie unterstehen den datenschutzrechtlichen Bestimmungen für private Personen. Ihre Datenbearbeitung muss sich auf eine Einwilligung der betroffenen Person, überwiegendes privates oder öffentliches Interesse oder Gesetz abstützen können (Art. 12 Abs. 1 und 13 Abs. 1 DSG). Für eine Weitergabe besteht keine gesetzliche Grundlage. Auch ein überwiegendes Interesse[8] fällt wohl ausser Betracht. Die demnach nötige Einwilligung ist nach Art. 4 Abs. 5 DSG gültig, wenn die betreffende Person sie nach angemessener Information freiwillig sowie für besonders schützenswerte Personendaten ausdrücklich erteilt hat.

Ob aus einer in einem Vorsorgereglement enthaltenen Bestimmung, wonach die Vorsorgeeinrichtung befugt sei, Versichertendaten an den Arbeitgeber weiterzugeben, eine freiwillige, nach angemessener Information erfolgte Einwilligung abgeleitet werden kann, ist zumindest zu bezweifeln.[9] Zudem ist – zumindest für Vorsorgeeinrichtungen, die auch das Obligatorium abdecken – eine Einwilligung im Einzelfall erforderlich, also eine Bevollmächtigung zur Bekanntgabe spezifischer Daten aus einem konkreten Anlass.[10]

Datenbearbeitung durch Dritte

Personendaten dürfen an Dritte nur unter einschränkenden Voraussetzungen zur Bearbeitung übergeben werden: Die Datenbearbeitung durch Dritte bedarf einer Vereinbarung oder einer gesetzlichen Grundlage. Es darf keine über die Befugnisse des Auftraggebers hinausgehende Datenbearbeitung erfolgen, und Geheimhaltungspflichten dürfen ihr nicht entgegenstehen (Art. 10a Abs. 1 DSG). Der Dienstleistungsvertrag zur technischen Verwaltung hat diese Voraussetzungen hinreichend zu konkretisieren.[11]

Nach heute geltendem Recht hat sich die Vorsorgeeinrichtung bei einem Outsourcing zu vergewissern, dass der Dritte die Datensicherheit gewährleistet (Art. 10a Abs. 2 DSG). Damit dürfte der Arbeitgeber als Beauftragter – auch für Einzelaufträge, wie etwa den manchmal in Anschlussverträgen ihm übertragenen Versand der Vorsorgeausweise – ausscheiden. Selbst mit aufwendigen organisatorischen und technischen Massnahmen zu deren Gewährleistung[12] und gegebenenfalls der Vereinbarung eines Audit-Rechts durch den Auftraggeber[13] werden Zweifel nicht ganz auszuräumen sein, dass trotzdem eine gewisse Datendurchlässigkeit bestehen könnte.

Ein institutionelles Datenleck wird auch in der paritätischen Verwaltung erblickt, wenn als Arbeitgebervertreter ein Personalverantwortlicher amtet.[14] Die Möglichkeit, kraft ihrer Befugnisse als Mitglieder des Stiftungsrats in operative Belange Einsicht zu nehmen, haben als Arbeitgebervertreter tätige Personal- und Finanzverantwortliche. Allerdings gehört es zur Good Governance einer Vorsorgeeinrichtung, dass sie einerseits den beiden Kategorien von Mitgliedern des obersten Organs paritätisch, undifferenziert Zugang zu Informationen im Zusammenhang mit operativen Angelegenheiten gewährt. Alle Mitglieder des obersten Organs sind gleichberechtigt. Daten und Informationen Arbeitgebervertretern zugänglich zu machen, vor Arbeitnehmervertretern aber zu verschliessen, ist daher nicht statthaft. Andererseits besteht die Aufgabe des obersten Organs in der Gesamtleitung der Vorsorgeeinrichtung[15], und dafür benötigt es grundsätzlich keine Personendaten. Soweit sie dennoch etwa in einem vom Stiftungsrat zu genehmigenden Teilliquidationsbericht enthalten sind, fallen sie unter die in Art. 86 BVG geregelte Schweigepflicht.

Ebenfalls nicht unkritisch ist die Beauftragung eines externen Anbieters, der nicht nur die technische Verwaltung für die Vorsorgeeinrichtung führt, sondern gleichzeitig für den Arbeitgeber die Saläradministration. Vertraglich muss sichergestellt sein, dass der Beauftragte nur spezifisch den jeweiligen Auftraggeber betreffende Daten für ihn bearbeitet und an ihn weitergibt, dem anderen hingegen nicht zugänglich macht.

Schlussbemerkung

Die geltenden Normen stellen sicher, dass der Arbeitgeber über die Vorsorgeeinrichtung nicht an Daten gelangen darf, in die er keinen Einblick erhalten soll. Wo Datenlecks vorkommen, ist von einer Verletzung geltender Normen auszugehen.

Das Datenschutzgesetz hat die Verselbständigungspflicht von Vorsorgeeinrichtungen konsequent zum Schutz der Arbeitnehmer weitergeführt. Heute gehört es zur Good Governance einer Vorsorgeeinrichtung, dass der Arbeitgeber über sie keinen Zugang zu Personendaten erhält, von denen er nicht ohnehin Kenntnis hat. Gelegentlich, beispielsweise im Zusammenhang mit der finanziellen Verantwortung, besteht Anlass, an diese konsequente Trennung zu erinnern. ■

[5] S. Empfehlung EDÖB (zit. Fn 1), Rz 10 m.w.N; David Rosenthal in David Rosenthal/Yvonne Jöhri (Hrsg.), Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 3 Bst. h, N 99 f., S. 64 f.

[6] S. zum sie ebenfalls erfassenden Anwendungsbereich von Art. 86a BVG Hans Michael Riemer/Gabriela Riemer-Kafka, Das Recht der beruflichen Vorsorge in der Schweiz, 2. A., Bern 2006, S. 21 Rz 51.

[7] S. aber Riemer/Riemer-Kafka (zit. Fn 6), S. 22 Rz 2.

[8] S. dazu Art. 13 Abs. 2 DSG.

[9] S. Beispiele gültiger bzw. ungültiger Einwilligungen bei David Rosenthal (zit. Fn 5), Art. 4 Abs. 5 N 97 f., S. 114 ff.

[10] Eine solche ist nicht erforderlich für die Information des Arbeitgebers über das Bestehen einer Teilinvalidität, s. Kurt Pärli, Datenaustausch zwischen Arbeitgeber und Versicherung, Diss. Bern 2003 (ASR 678), S. 98 f.

[11] Im Einzelnen David Rosenthal (zit. Fn 5), Art. 10a Abs. 1 Bst. a N 71 ff., S. 244 ff.

[12] S. zu den zu überbindenden technischen und organisatorischen Massnahmen Art. 8 ff. der Verordnung zum Bundesgesetz über den Datenschutz (VDSG; SR 235.11).

[13] S. David Rosenthal (zit. Fn 5), Art. 10a Abs. 2 N 129, S. 264 f.

[14] Hans Michael Riemer, Berührungspunkte zwischen beruflicher Vorsorge und Arbeitsrecht, in SZS 2009, S. 119 f.

[15] S. dazu Art. 51a BVG (Inkrafttreten 1.1.2012).

Protection des données

Les données des assurés ne regardent pas l'employeur

Il est problématique, au plan du droit de la protection des données, que les employeurs notifient les certificats de prévoyance conjointement avec les certificats de salaire. Une recommandation afférente du Préposé fédéral à la protection des données et à la transparence (PFPDT) a des répercussions sur l'organisation administrative de l'institution de prévoyance.

Des avis étaient parvenus au préposé à la protection des données, parce qu'une institution de prévoyance envoyait les certificats personnels de prévoyance non pas directement à la personne assurée, mais à l'adresse de l'employeur, lequel en effectuait ensuite la distribution. Procédant d'une violation de la protection des données, le PFPDT a recherché le contact avec l'institution de prévoyance, sans toutefois aboutir à un accord. Finalement, le PFPDT a émis une recommandation, selon laquelle l'institution de prévoyance X. cesse immédiatement la communication, pratiquée par elle à l'employeur, de données des certificats de caisses de pensions des personnes qu'elle assure.[1]

Bien juridique protégé

Outre les données fixes et le salaire assuré, les certificats de caisse de pensions contiennent également des projections de prestations dans les cas de prévoyance de la vieillesse, de l'invalidité et du décès, des indications concernant l'avoir de vieillesse existant, les versements en vue de l'acquisition de la propriété du logement, le cas échéant aussi sur des rachats et, probablement, sur des réserves de prestations dues à l'état de santé. Au plan du droit de la protection des données, ce sont notamment des indications présentant un lien avec la santé ou permettant des déductions quant à celle-ci qui sont considérées comme des données sensibles.[2]

Selon l'art. 328b CO, l'employeur ne peut traiter des données concernant le travailleur que dans la mesure où celles-ci portent sur les aptitudes du travailleur à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail. En règle générale, ne font pas partie de ces données les informations sur des rapports personnels, des qualités et des tendances. Sont également exclues d'un traitement les données relatives au salaire dans le cadre de précédents rapports de services. L'employeur n'a pas droit à des informations sur la situation patrimoniale personnelle et à des données portant sur la santé.[3]

Communication des données à des tiers

La prévoyance est gérée par une institution dotée de sa personnalité juridique propre et indépendante de l'employeur. Par rapport à celle-ci, l'employeur est à considérer comme un tiers.

Depuis 2000, il existe, pour tous les assureurs sociaux, des règles uniformes concernant l'obligation de garder le secret.[4] Dans la prévoyance professionnelle, l'art. 86a LPP régit la communication des données aux tiers. Des données personnelles ne peuvent être transmises à l'employeur, sur la base de l'art. 86a, al. 5, let. b, LPP, que si la personne concernée y a, en l'espèce, consenti par écrit ou si un consentement qu'il n'est pas possible d'obtenir peut être présupposé. L'exigence du consentement dans le cas d'espèce correspond à la condition de l'art. 19, al. 1er, let. b, LPD, sous laquelle les autorités fédérales peuvent communiquer des données personnelles, ce qui est logique dans la mesure où les institutions de prévoyance dans le régime obligatoire sont chargées d'une tâche publique de la Confédération et donc considérées comme organes fédéraux au sens de l'art. 3, let. h, LPD[5]. Une distinction des

En bref

> Si l'on observe résolument les règles relatives à la protection des données, l'employeur n'a pas accès, par l'intermédiaire de l'institution de prévoyance, à des données de personnes assurées auxquelles il n'a pas droit

> Une communication de données personnelles spécifiques pour un motif concret suppose l'octroi de pouvoirs afférents

[1] Recommandation du PFPDT du 08.07.2009, publiée sur le site web du PFPDT (www.edoeb.admin.ch).

[2] Art. 3, let. c, ch. 1er, de la loi fédérale sur la protection des données (LPD; RS 235.1).

[3] Voir Recommandation du PFPDT du 08.07.2009 (note 1 en bas de page) avec références additionnelles.

[4] Kurt Pärli, in: Jacques-André Schneider/Thomas Geiser/Thomas Gächter (éd.), BVG und FZG, Berne 2010, Art. 86a LPP, N. 1.

[5] Voir Recommandation du PFPDT (citée dans la note 1 en bas de page), ch. 10 avec notes additionnelles; David Rosenthal, in: David Rosenthal/Yvonne Jöhri (éd.), Handkommentar zum Datenschutzgesetz, Zurich 2008, Art. 3, let. h, N. 99 s., p. 64 s.

données personnelles quant à savoir si elles concernent le régime obligatoire ou le régime surobligatoire n'est pas praticable; de plus, ces exigences rigoureuses doivent aussi être observées par des institutions de prévoyance enveloppantes.[6]

L'art. 86a LPP ne s'applique pas aux institutions purement sur-obligatoires, car il n'est pas énuméré dans l'art. 89bis, al. 6, CC[7]; en outre, celles-ci sont soumises aux dispositions relatives à la protection des données pour les personnes privées. Leur traitement de données doit pouvoir se fonder sur un consentement de la personne concernée, un intérêt privé ou public prépondérant ou la loi (art. 12, al. 1er, et art. 13, al. 1er, LPD). Il n'existe pas de base légale pour une transmission. De même, un intérêt prépondérant[8] n'entre sans doute pas en considération. Le consentement dès lors requis est valable, conformément à l'art. 4, al. 5, LPD, si la personne concernée a exprimé sa volonté librement après avoir été dûment informée et si, lorsqu'il s'agit de données sensibles, elle a donné son consentement explicitement.

Il y a lieu de douter, à tout le moins, qu'il soit possible de déduire d'une disposition contenue dans un règlement de prévoyance – selon laquelle l'institution de prévoyance est autorisée à transmettre des données de personnes assurées à l'employeur – un consentement librement formé et donné après due information.[9] En outre, au moins pour les institutions de prévoyance couvrant également le régime obligatoire, un consentement est requis dans le cas d'espèce, soit l'octroi d'un pouvoir en vue de la communication de données spécifiques pour un motif concret.[10]

Traitement des données par des tiers

En vue de leur traitement, les données personnelles ne doivent être remises à des tiers qu'à des conditions restrictives: le traitement des données par des tiers nécessite une convention ou une base légale. Aucun traitement de données dépassant les pouvoirs du mandant ne doit avoir lieu et aucune obligation de garder le secret ne doit s'y opposer (art. 10a, al. 1er, LPD). Le contrat de prestation de services concernant la gestion administrative doit concrétiser ces conditions dans une mesure suffisante.[11]

D'après le droit actuellement en vigueur, l'institution de prévoyance doit s'assurer, lors d'une externalisation, que le tiers garantisse la sécurité des données (art. 10a, al. 2, LPD). Partant, l'employeur ne devrait pas entrer en ligne de compte en tant que mandataire. Même à l'aide de mesures organisationnelles et techni-ques coûteuses en vue de cette garantie[12] et, le cas échéant, d'une convention pour un droit d'audit par le mandant[13], il ne sera pas possible d'écarter entièrement des doutes qu'une certaine perméabilité des données puisse néanmoins exister.

Une fuite institutionnelle de données est également perçue dans la gestion paritaire lorsqu'un responsable du personnel exerce la fonction de représentant de l'employeur[14]. Les responsables du personnel et des finances agissant en qualité de représentants de l'employeur ont la possibilité, en vertu de leurs pouvoirs de membres du conseil de fondation, d'avoir un droit de regard dans les affaires de nature opérative. Toutefois, il appartient à la bonne gouvernance d'une institution de prévoyance qu'elle accorde, d'une part, aux deux catégories de membres de l'organe suprême, de façon paritaire et sans différenciation, un accès aux informations liées aux affaires opératives. D'autre part, la tâche de l'organe suprême consiste en la direction globale de l'institution de prévoyance[15]; à cet effet, il n'a en principe pas besoin de données personnelles. Dans la mesure où celles-ci font néanmoins partie, par exemple, d'un rapport de liquidation partielle à approuver par le conseil de fondation, elles tombent sous le coup de l'obligation de garder le secret régi par l'art. 86 LPP.

L'octroi d'un mandat à un prestataire externe, qui gère non seulement l'administration technique pour l'institution de prévoyance, mais aussi – et simultanément – l'administration des salaires pour l'employeur, est également délicat. Il y a lieu d'assurer, par contrat, que le mandataire traite pour le mandant uniquement des données concernant spécifiquement ce dernier et les lui remette, mais ne les rende pas accessibles à l'autre.

Observation finale

Les normes en vigueur garantissent que l'employeur ne peut accéder, par le biais de l'institution de prévoyance, à des données qu'il ne doit pas consulter. Lorsque des fuites de données surviennent, il convient de procéder d'une violation de normes applicables.

La loi sur la protection des données a poursuivi de manière conséquente l'obligation d'autonomisation des institutions de prévoyance dans le but de protéger les travailleurs. Aujourd'hui, la bonne gouvernance d'une institution de prévoyance implique que l'employeur n'obtienne, par le biais de celle-ci, aucun accès à des données personnelles dont il n'a pas de toute façon connaissance. ■

Kurt C. Schweizer

[6] Voir, à propos du champ d'application de l'art. 86a LPP qui les concerne aussi, Hans Michael Riemer/Gabriela Riemer-Kafka, Das Recht der beruflichen Vorsorge in der Schweiz, 2e éd., Berne 2006, p. 21 ch. 51.

[7] Voir cependant Riemer/Riemer-Kafka (cité dans la note 6 en bas de page), p. 22 ch. 2.

[8] Voir à ce propos art. 13, al. 2, LPD.

[9] Voir les exemples de consentements valables et non valables dans David Rosenthal (cité dans la note 5 en bas de page), Art. 4, al. 5, N. 97 s., p. 114 ss.

[10] Un tel consentement n'est pas requis pour l'information de l'employeur sur l'existence d'une invalidité partielle; voir Kurt Pärli, Datenaustausch zwischen Arbeitgeber und Versicherung, thèse Berne 2003 (ASR 678), p. 98 s.

[11] Pour les détails, David Rosenthal (cité dans la note 5 en bas de page), Art. 10a, al. 1er, let. a, N. 71 ss., p. 244 ss.

[12] Concernant les mesures techniques et organisationnelles à reporter, voir art. 8 ss. de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD; RS 235.11).

[13] Voir David Rosenthal (cité dans la note 5 en bas de page), Art. 10a, al. 2, N. 129, p. 264 s.

[14] Hans Michael Riemer, Berührungspunkte zwischen beruflicher Vorsorge und Arbeitsrecht, in: RSAS 2009, p. 119 s.

[15] Voir à ce propos art. 51a LPP (entrée en vigueur: 01.01.2012).