

Bleibt der Datenschutz auf der Strecke?

Problematischer Austausch von Informationen in Versicherungszweigen, die ein Obligatorium und einen privaten Zusatz kennen

In der Krankenversicherung gibt es obligatorische und zusätzliche Versicherungen, die rechtlich völlig getrennt sind und für die nicht dieselben gesetzlichen Bestimmungen gelten. Damit stellt sich die Frage: Wer darf welche Informationen haben, welcher Informationsaustausch ist zwischen der obligatorischen und der zusätzlichen Versicherung zulässig?

Das Bundesgesetz über den Datenschutz ist schon über 13 Jahre alt – es trat am 1. Juli 1993 in Kraft. Es beruht auf den beiden Prinzipien der Transparenz und der Selbstbestimmung. Das heisst: Die Person, deren Daten benötigt werden, soll erstens genau wissen, welche persönlichen Daten wozu verwendet werden, und sie soll zweitens eine Verarbeitung solcher Daten auch verbieten können. Ausgenommen von der Möglichkeit eines solchen Verbots sind Fälle, in denen ein Rechtfertigungsgrund des Datenbearbeiters vorliegt, der höher zu gewichten ist. Als Rechtfertigungsgrund kann insbesondere eine gesetzliche Grundlage gelten.

Im Gesetz sind insbesondere folgende Grundsätze formuliert:

- Rechtmässigkeit der Datenbearbeitung: Diese kann entweder in der Einwilligung der betroffenen Person liegen oder durch überwiegendes privates oder öffentliches Interesse oder durch Gesetz zustande kommen.
- Treu und Glauben: Daten dürfen grundsätzlich nicht heimlich bearbeitet oder mit falschen Angaben bezüglich Zweck und Bearbeitungsart erhoben werden.
- Verhältnismässigkeit: Die Datensparsamkeit ist zu beachten bezüglich Anzahl der Daten, der Aufbewahrungsdauer oder Anzahl der zugriffsberechtigten Personen.
- Zweckbindungsgebot: Daten dürfen nur zum vorgegebenen Zweck genutzt werden, eine Zweckänderung müsste den Betroffenen mitgeteilt werden.
- Richtigkeit der Daten: Daten haben aktuell und richtig zu sein. Falsche Daten sollen berichtigt oder vernichtet werden.

– Informationssicherheit: Zur Informationssicherheit gehören sowohl Datenvertraulichkeit, -verfügbarkeit als auch -integrität. Dafür sind vor allem technische und organisatorische Massnahmen zu treffen.

– Auskunftsrecht über die eigenen Daten: Jede Person kann von einem Datenbearbeiter verlangen, dass dieser sie informiert, ob Daten über sie bearbeitet werden. Falls ja, hat die betroffene Person grundsätzlich ein Recht auf eine Kopie oder einen Ausdruck dieser Daten.

In Kürze

- > Ein Datenaustausch zwischen Trägern der obligatorischen und der zusätzlichen Versicherung dürfte nicht erfolgen
- > In der Praxis finden solche Austausche aber statt. Sie führen nicht zu Nachteilen für die Versicherten

Sozialversicherungsrecht

Sozialversicherungen beruhen auf Bundesgesetzen, in denen auch spezielle Bestimmungen bezüglich Schweigepflicht und Datenweitergabe gelten. Da für die meisten Sozialversicherungen ähnliche Grundsätze gelten, wurde das Bundesgesetz über den allgemeinen Teil des Sozialversicherungsrechts (ATSG) erlassen, das seit 2003 in Kraft ist. Das Gesetz ist auf die Sozialversicherungen anwendbar, wenn dies von den einzelnen Sozialversicherungsgesetzen explizit vorgesehen ist.

Die meisten Sozialversicherungen haben das ATSG in ihrem Art. 1 für anwendbar erklärt. Nicht so das Bundesgesetz über die berufliche Vorsorge (BVG).

Bezüglich Schweigepflicht wird aber sowohl im ATSG als auch im BVG dieselbe Formulierung gewählt: «Personen, die an der Durchführung sowie der Kontrolle oder der Beaufsichtigung der Durchführung die-



Ursula Uttinger

lic. iur., MBA HSG, Präsidentin Datenschutz-Forum Schweiz, leitende Auditorin SQS, Mitglied Stiftungsrat Personalvorsorgestiftung SQS

Matthias Vögeli

lic. iur., Rechtsanwalt, Vorstand Datenschutz-Forum Schweiz, Datenschutzbeauftragter einer Krankenversicherung, Rothenburg

ses Gesetzes (BVG)/der Sozialversicherungsgesetze (ATSG) beteiligt sind, haben gegenüber Dritten Verschwiegenheit zu bewahren.» Auch bezüglich Datenbekanntgabe wird ähnlich vorgegangen: Es wird eine abschliessende Liste der Auskunftsberechtigten im Gesetz definiert.

Krankenversicherung

Im Bereich der Krankenversicherung gibt es eine obligatorische Versicherung (obligatorische Krankenpflegeversicherung) und freiwillige Zusatzversicherungen. Für diese beiden Zweige gelten unterschiedliche Bestimmungen, wie der Datenaustausch zu erfolgen hat. Komplizierter wird der Datenaustausch zusätzlich dann, wenn die beiden Versicherungsarten von zwei rechtlich selbständigen Gesellschaften durchgeführt werden. In der Praxis haben sich die Mehrheit der Krankenversicherer eine Holdingstruktur gegeben, mit einer oder mehreren Gesellschaften für die obligatorische Krankenversicherung und einer Gesellschaft für die Zusatzversicherungen, wobei diese rechtlich zwar selbständig sind, organisatorisch und wirtschaftlich aber eine enge Verflechtung besteht. Wie kann der Informationsaustausch zwischen zwei solchen Unternehmungen erfolgen? Wie lassen sich die unterschiedlichen Bedürfnisse des Kunden nach verhältnismässiger Datenweitergabe einerseits und speditiver Leistungsabrechnung andererseits befriedigen? Schnittpunkte ergeben sich insbesondere bei folgenden Situationen:

Vertragsabschluss

Im Gegensatz zur obligatorischen Krankenpflegeversicherung sind bei den Zusatzversicherungen Fragen nach dem Gesundheitszustand zulässig. Die entspre-

chenden Antworten und die meist gleichzeitig erteilte Ermächtigung, bei Dritten zusätzliche Auskünfte einzuholen, sind aber ausschliesslich für die Zusatzversicherungen zu verwenden und dürfen nicht für eine Risikoselektion in der obligatorischen Grundversicherung verwendet werden.

Prüfung von Leistungsansprüchen

Im Leistungsfall besteht eine Leistungspflicht aus den Zusatzversicherungen erst, wenn keine Leistungen aus der obligatorischen Krankenpflegeversicherung geschuldet sind. Streng rechtlich genommen hätten die Versicherer eine strikte Trennung des Datenzugriffs zu beachten: Wäre für die Beurteilung der Leistungspflicht in der Zusatzversicherung ein Rückgriff auf Daten der obligatorischen Versicherung notwendig, so müsste somit zuerst die Einwilligung der versicherten Person eingeholt werden. Dies ist weder verhältnismässig, noch kann dies im Interesse der versicherten Person liegen, sodass diese Einwilligung vorausgesetzt werden kann. Man geht in diesem Fall davon aus, dass für die versicherte Person eine rasche Leistungsaurichtung wichtiger ist als datenschutzrechtliche Bedenken. Dies unabhängig davon, ob die obligatorische Krankenpflegeversicherung und die Zusatzversicherung in getrennten juristischen Personen betrieben werden.

Datenbearbeitung

bei Anzeigepflichtverletzung

Stellt sich noch die in letzter Zeit an Aktualität gewonnene Frage, wie die Daten-

beschaffung bei Vermutung einer Anzeigepflichtverletzung¹ erfolgen darf. Da der Versicherer das ihm zustehende Rücktrittsrecht innert vier Wochen geltend machen muss, ist er unter Umständen auf Daten aus der Grundversicherung angewiesen. In Versicherungsanträgen regelmässig enthaltene Einwilligungsklauseln können wohl bei der Aufnahme in die Zusatzversicherung eine ausreichende Grundlage für einen Beizug der Daten aus der obligatorischen Krankenpflegeversicherung darstellen. Eine Anzeigepflichtverletzung kann aber unter Umständen erst nach Jahren aktuell werden. Zwar erstreckt sich die auf dem Antrag erteilte Einwilligung ausschliesslich auf den Vertragsabschluss, dennoch wäre es rechtsmissbräuchlich, sich bei einem Versicherungsbetrug auf das Recht auf Datenschutz zu berufen, sodass der Versicherer sich in einem solchen Fall die Daten aus der obligatorischen Krankenpflegeversicherung zunutze machen dürfte.

Besonderheiten Pensionskasse

Bei Pensionskassen wird unterschieden in einen obligatorischen und einen überobligatorischen Teil der Vorsorge. In der heutigen Praxis ist für die Durchführung dieser beiden Zweige in aller Regel nur eine einzige Vorsorgeeinrichtung und

¹ Eine solche liegt vor, wenn etwa im Rahmen eines Versicherungsantrags der Gesundheitsfragebogen nicht oder nicht wahrheitsgemäss ausgefüllt wird.

nur ein einziges Vorsorgereglement zuständig. Man spricht deshalb von «umhüllendem Vorsorgewerk», in dem die Ansprüche gemäss den gesetzlichen Mindestvorschriften vollständig enthalten sein müssen. Welche Detailvorschriften nicht nur für den obligatorischen, sondern ausdrücklich auch für den überobligatorischen Teil gelten, wird in Art. 49 BVG mit einer Aufzählung genannt. Bestimmungen über Datenschutz sind in dieser Aufzählung – auch nach der 1. BVG-Revision – erstaunlicherweise nicht enthalten. Carl Helbling bejaht trotzdem klar eine Anwendung der Datenschutzartikel im BVG auch für den überobligatorischen Teil der Vorsorge.²

Von grosser praktischer Bedeutung sind die Datenschutzbestimmungen dann, wenn die ausserobligatorische Vorsorge über einen separaten Versicherungsträger abgewickelt wird, also bei einem Verzicht auf die Umhüllung: Eine direkte Kommunikation beider Einrichtungen ohne Wissen der betroffenen Personen ist grundsätzlich nicht korrekt, die Kommunikation der beiden Einrichtungen muss immer und ausschliesslich über die versicherte Person erfolgen. Nur wenn beide Teile der Versicherung durch den gleichen Versicherungsträger durchgeführt werden, kann davon ausgegangen werden, dass eine direkte Kommunikation stattfindet. Eine solche ist denn auch nicht zum Nachteil der Versicherten.

Grosse Herausforderung

Sobald ein obligatorischer und ein überobligatorischer Teil einer Versicherung besteht, ist der Datenschutz eine Herausforderung. Denn ein Datentransfer dürfte zwischen den entsprechenden Trägern eigentlich nicht erfolgen. Dennoch werden Daten oft ohne Wissen der betroffenen Personen ausgetauscht. Dies führt jedoch kaum zu Nachteilen für die betroffenen Personen.

Grundsätzlich kann festgehalten werden: Die Einhaltung des Datenschutzes ist nicht immer und überall eine Selbstverständlichkeit. Ein relativ kleiner Kreis von Datenschutzespezialisten setzt sich mit dem Thema intensiv auseinander, der Grossteil der Bevölkerung ist unbeeindruckt. ■

² Carl Helbling: Personalvorsorge und BVG, 8. Auflage 2006, Seite 302.

La protection des données est-elle sacrifiée?

Problèmes d'échange d'informations dans les secteurs d'assurance qui connaissent un régime obligatoire et un complément privé

Dans l'assurance maladie, il existe des assurances obligatoires et des assurances complémentaires qui forment des entités juridiques totalement séparées et ne sont pas régies par les mêmes dispositions légales. D'où la question de savoir qui a le droit d'obtenir quelles informations, quel échange d'informations est admissible entre l'assurance obligatoire et l'assurance complémentaire.

La loi fédérale sur la protection des données est déjà vieille de plus de 13 ans – elle est entrée en vigueur le 1er juillet 1993. Elle se fonde sur les deux principes de la transparence et de l'autodétermination. Ce qui signifie: la personne dont les données sont demandées doit savoir exactement lesquelles de ses données personnelles sont utilisées et ce qu'il en advient, mais elle doit aussi pouvoir refuser un traitement de ces données. Seuls ne peuvent pas être interdits les traitements pour lesquels celui qui les effectue peut justifier d'un motif plus important que la protection des données personnelles. Une base légale constitue par exemple un tel motif.

Dans la loi sont notamment formulés les principes suivants:

Légalité du traitement de données: elle peut être fondée par l'autorisation de la personne concernée, ou par un intérêt public ou privé prépondérant, ou découler d'une loi.

– Bonne foi: il est interdit par principe de traiter des données en secret ou sous un faux prétexte concernant leur but et le mode de traitement.

– Adéquation: la parcimonie est de rigueur concernant la quantité des données, la durée de conservation ou le nombre des personnes autorisées à y accéder.

– Obligation de lien à un but: L'utilisation des données est seulement autorisée en relation avec le but indiqué, un changement de but devrait être signalé aux personnes concernées.

– Exactitude des données: les données doivent être actuelles et correctes. Des données inexactes devront être corrigées ou détruites.

– Sécurité de l'information: en font partie la confidentialité des données, la disponibilité et l'intégrité. A cet effet, il faudra surtout prendre des mesures d'ordre technique et organisationnel.

En bref

> Il ne devrait pas y avoir d'échange de données entre les organismes d'assurance obligatoires et complémentaires

> Dans la pratique, de tels échanges ont pourtant lieu, mais il n'en résulte aucun désavantage pour les assurés

– Droit de demander des renseignements sur ses données personnelles: toute personne peut demander à celui qui traite ses données de lui dire si ses données sont effectivement en voie de traitement ou non. Le cas échéant, la personne peut en principe demander une copie ou un imprimé de ces données.

Droit relatif aux assurances sociales

La plupart des assurances ont déclaré la LPGA applicable dans leur article 1er. Ce n'est pas le cas de la loi fédérale sur la prévoyance professionnelle (LPP).

Mais en matière d'obligation de secret, la LPGA et la LPP utilisent une formulation identique: «Les personnes qui participent à l'exécution, ainsi qu'au contrôle ou à la surveillance de l'exécution de cette loi (LLP)/des lois relatives aux assurances sociales (LPGA) sont tenues de garder le secret vis-à-vis de tiers». Concernant la divulgation de données, la manière de procéder est similaire: une liste exhaustive



Ursula Uttinger

lic. en droit, MBA HESG, Présidente du Forum suisse de la protection des données, auditrice responsable SQS, membre du conseil de fondation de la fondation en faveur du personnel SQS

Matthias Vögeli

lic. en droit, avocat, comité du Forum suisse de la protection des données, préposé à la protection des données d'une caisse maladie, Rothenburg

des personnes autorisées à donner des renseignements est définie dans la loi.

Assurance maladie

Dans le domaine de l'assurance maladie, il existe une assurance obligatoire (assurance de soins de base) et des assurances complémentaires facultatives. Les dispositions régissant l'échange de données divergent pour ces deux branches. L'échange de données devient encore plus compliqué lorsque les deux types d'assurances sont exécutés par deux sociétés juridiquement autonomes. Dans la pratique, la plupart des assureurs maladie se sont donné une structure de holding, avec une ou plusieurs compagnies pour l'assurance maladie obligatoire et une compagnie pour les assurances complémentaires, toutes constituant des entités morales autonomes, mais étroitement liées au niveau organisationnel et économique. Comment peut se dérouler l'échange d'informations entre deux entreprises de ce type? Comment concilier les besoins conflictuels du client qui souhaite une transmission adéquate de ses données et de l'administration qui doit pouvoir procéder au décompte des prestations de manière expéditive? Ces besoins se recoupent en particulier dans les situations suivantes:

Conclusion d'un contrat

A l'inverse de l'assurance de soins obligatoire, il est admis de poser des questions sur l'état de santé lors de la conclusion d'assurances complémentaires. Cependant, les réponses correspondantes et l'autorisation de se procurer des informations complémentaires auprès de tiers qui est généralement octroyée en même

temps doivent être utilisées aux seules fins des assurances complémentaires et non à une sélection des risques dans l'assurance de base obligatoire.

Examen de demandes de prestations

Lors de la réalisation d'un cas déclenchant des prestations, l'obligation des assurances complémentaires de servir des prestations débute seulement lorsqu'il n'y a pas de prestations échues de la part de l'assurance de soins obligatoire. D'un point de vue strictement juridique, les assureurs devraient séparer rigoureusement l'accès aux données: pour consulter les données de l'assurance obligatoire afin de décider si l'assurance complémentaire est tenue de fournir des prestations, il faudrait donc demander l'autorisation de la personne assurée au préalable. Mais il en résulterait un travail déraisonnable et qui en plus ne servirait pas les intérêts de la personne assurée, de sorte que l'on peut supposer une autorisation d'office. On admet donc dans ce cas qu'il est plus important que la personne assurée bénéficie rapidement de ses prestations que de respecter les impératifs de la protection des données. Et ce indépendamment du fait que l'assurance de soins obligatoire et l'assurance complémentaire soient exécutées dans des personnes morales séparées.

Traitement des données en cas de violation de l'obligation d'informer

Reste une question qui gagne en actualité depuis quelque temps, à savoir, de quelle manière on peut se procurer les

données lorsqu'on soupçonne une violation de l'obligation d'informer.¹ Comme l'assureur doit exercer en l'espace de quatre semaines le droit de résiliation dont il dispose, il se peut qu'il dépende de données de l'assurance de base. Les clauses de consentement régulièrement contenues dans les demandes d'assurance peuvent certes servir de base pour consulter les données d'une assurance de soins obligatoire avant d'avaliser l'adhésion à une assurance complémentaire. Mais selon les circonstances, il est possible qu'une violation de l'obligation d'informer passe inaperçue pendant plusieurs années. Il est vrai que le consentement donné sur la demande se limite à la conclusion du contrat, mais il serait quand même abusif que l'on puisse se prévaloir du droit à la protection des données en cas d'escroquerie à l'assurance, de sorte que l'assureur pourrait, le cas échéant, se servir des données de l'assurance de soins obligatoire.

Les particularités d'une caisse de pensions

Dans les caisses de pensions, on fait la différence entre une partie obligatoire et une partie surobligatoire de la prévoyance. Dans la pratique actuelle, l'exécution de ces deux secteurs relève généralement d'une seule institution de prévoyance et d'un seul règlement de

prévoyance. On parle dans ces cas d'une «œuvre de prévoyance enveloppante» dans laquelle toutes les exigences minimales stipulées par la loi doivent être entièrement satisfaites. Les prescriptions détaillées qui s'appliquent non seulement à la partie obligatoire, mais aussi et explicitement à la partie surobligatoire, sont énumérées à l'art. 49 de la LPP. Ce qui surprend, c'est que cette liste ne comprend pas de dispositions sur la protection des données – et la 1^{re} révision de la LPP n'y a rien changé. Carl Helbling est néanmoins catégorique: l'article sur la protection des données est également applicable dans la partie surobligatoire de la prévoyance.²

Dans la pratique, les dispositions relatives à la protection des données revêtent une grande importance lorsque la prévoyance hors obligatoire est exécutée par un organe d'assurance tiers, que la caisse n'est donc pas enveloppante. Une communication directe entre les deux institutions qui passe outre aux personnes concernées ne serait en principe pas correcte, la communication des deux institutions doit toujours et exclusivement passer par la personne assurée. La communication directe ne peut paraître admissible que lorsque les deux parties de l'assurance sont exécutées par le même organe d'assurance. Dans ce cas, elle ne se fait pas non plus au détriment de l'assuré. ■

¹ Elle existe dans les faits, par exemple au cas où le questionnaire sur la santé n'est pas rempli ou pas de façon véridique.

² Helbling, Carl: Personalvorsorge und BVG, 8e tirage 2006, page 302.