

Umsetzung des revidierten Datenschutzgesetzes (DSG): Fragestellungen aus den Webinaren und Antworten	
Fragen	Antworten
VORSORGEINRICHTUNGEN ALS BUNDESORGANE: WEITERE AUSWIRKUNGEN?	
<p>1. Wie ist vorzugehen, wenn im gleichen System sowohl eine umhüllende Kasse wie auch zwei überobligatorische Kassen des gleichen Arbeitgebers verwaltet werden und die Versicherten der einen überobligatorischen Kasse auch in der umhüllenden Kasse versichert sind?</p> <p>2. Gibt es allfällige Besonderheiten zu beachten, wenn man überobligatorische Kassen wie ein Bundesorgan behandeln will?</p>	<p>1. Lässt sich eine Datenbearbeitung nicht ausschliesslich dem Überobligatorium zuordnen, so muss sich eine umhüllende Pensionskasse an die für Bundesorgane geltenden Regeln des revDSG halten. Nur so weit eine Datenbearbeitung vollständig von der öffentlichen Aufgabe getrennt bzw. ausschliesslich dem Überobligatorium zuzuordnen ist, unterliegt die umhüllende Pensionskasse den für Private geltenden Bestimmungen des revDSG. <i>Siehe ASIP-Fachmitteilung Nr. 130, S. 3 (mit Beispielen).</i> Rein überobligatorische Kassen gelten gemäss revDSG jedoch als private Personen. Sie sind von der Pflicht zur Vornahme einer Datenschutz-Folgenabschätzung befreit. <i>Siehe ASIP-Fachmitteilung Nr. 130, S. 8f.</i></p> <p>2. Nicht registrierten (überobligatorischen) Pensionskassen ist die Ernennung eines Datenschutzberaters freigestellt. Zudem können diese freiwillig ein Bearbeitungsverzeichnis führen. <i>Siehe ASIP-Fachmitteilungen Nr. 130, S. 6, und Nr. 131, S. 1f.</i></p>
DER VERANTWORTLICHE GEMÄSS REVDSG	
<p>Was ist unter dem „Verantwortlichen gemäss revDSG“ zu verstehen?</p>	<p>Als Verantwortlicher gilt jene Person oder jenes Bundesorgan, welche bzw. welches allein oder zusammen mit anderen über den Zweck (Wieso findet eine Datenbearbeitung statt?) und die Mittel (Wie wird der Zweck erreicht?) der Datenbearbeitung entscheidet. Es handelt sich dabei um diejenige Person bzw. um dasjenige Bundesorgan, die/das die wesentlichen datenschutzrechtlichen Parameter einer Datenbearbeitung festlegt (ASIP-Fachmitteilung Nr. 130, S. 6, Anm. 31). Ein Beispiel ist die Gesundheitsprüfung. Sie bezweckt die Durchsetzung der Anzeigepflicht, d.h. der Deklaration einer gesundheitlichen Beeinträchtigung. Der Zweck wird mittels eines durch den Antragsteller (Versicherten) zuhändigen des Verantwortlichen auszufüllenden Fragebogens oder durch sonstiges schriftliches Befragen des Antragstellers durch den Verantwortlichen erreicht (Mittel).</p>

	<i>Dabei empfehlen wir die Anwendung von DSAT (ASIP-Fachmitteilung Nr. 131, S. 5): Formular „Compliance Check II – Anforderungen an eine Datenbearbeitung (für Verantwortliche)“ unter https://dsat.ch/download/.¹</i>
BEARBEITUNGSVERZEICHNISSE	
Sind die Bearbeitungsverzeichnisse, die beim EDÖB aufgeschaltet werden, öffentlich einsehbar?	Ja. Die Meldepflicht beschränkt sich auf die Verzeichnisse von Bundesorganen (Art. 12 Abs. 4 revDSG): https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/unternehmen/anmeldung-einer-datensammlung.html .
Festhalten der Identität des für die Bearbeitung Verantwortlichen im Bearbeitungsverzeichnis – namentliche Nennung oder reicht Funktionsbezeichnung?	Ja. Das Verzeichnis des Verantwortlichen enthält u.a. mindestens die Identität des Verantwortlichen (Art. 12 Abs. 2 lit. a revDSG). Die für die Bearbeitung verantwortliche Person muss identifizierbar sein, weshalb – neben der Funktionsbezeichnung – deren Name festzuhalten ist. <i>Siehe ASIP-Webinare Datenschutz vom 10./14./15. November 2022, Folien 17f. (Muster eines Bearbeitungsverzeichnisses)</i>
IMPLEMENTIERUNG EINES PROZESSES ZUM FORTLAUFENDEN MONITORING DER DATENSCHUTZ-COMPLIANCE	
Soll das Monitoring an eine bestimmte Rolle geknüpft sein?	Das Monitoring ist Teil des IKS, d.h. Teil der Organisation der Vorsorgeeinrichtung, die zu den undelegierbaren Aufgaben des obersten Organs gehört (Art. 51a Abs. 1 und 2 lit. f BVG/Art. 49 Abs. 2 Ziff. 7 BVG). Dabei wirkt der Datenschutzberater (Art. 10 revDSG/Art. 25ff. revDSV) bei der Anwendung der Datenschutzvorschriften mit. Dieser ist gegenüber dem Verantwortlichen, d.h. dem obersten Organ der Vorsorgeeinrichtung, nicht weisungsgebunden. Die Vorsorgeeinrichtung hat dem Datenschutzberater Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten zu gewähren, die er zur Erfüllung seiner Aufgaben benötigt (Art. 27 Abs. 1 lit. a revDSV), vorausgesetzt, es stehen keine BVG-Bestimmungen entgegen. Mehrere Bundesorgane können auch gemeinsam einen Datenschutzberater ernennen (Art. 25 revDSV). Das IKS ist Gegenstand der Prüfung der Organisation und Geschäftsführung der Vorsorgeeinrichtung durch die Revisionsstelle, welche die Existenz einer angemessenen internen Kontrolle im Prüfbericht bestätigen muss (Art. 35 Abs. 1 BVV2). <i>Siehe Marc Hürzeler/Raffaella Biaggi, Art. 52c BVG, in: Marc Hürzeler/Hans-Ulrich Stauffer (Hgg.), Basler Kommentar. Berufliche Vorsorge, Basel 2021, N. 9.</i>

¹ DSAT ist ein Datenschutz Self Assessment Tool, bestehend aus einem Satz von Formularen, der eine strukturierte Selbstbeurteilung der Datenschutz-Compliance eines Unternehmens erlaubt, d.h. die „Überprüfung, inwieweit die Bestimmungen des Datenschutzes sowohl unter dem revidierten DSG als auch der DSGVO eingehalten sind“ (<https://dsat.ch/einfuehrung/>).

LÖSCHUNG ODER ANONYMISIERUNG DER DATEN: UMSETZUNG	
Wie kann die Anforderung der Löschung oder Anonymisierung der Daten für Vorsorgeeinrichtungen umgesetzt werden?	<p>Beanspruchen die Versicherten bzw. Rentnerinnen und Rentner gegenüber der Vorsorgeeinrichtung das Recht auf „Löschung“ von Vorsorgedaten i.S. des „Rechts auf Vergessen“, hat die Vorsorgeeinrichtung diesen die gesetzlichen Aufbewahrungspflichten der Pensionskassen entgegenzuhalten. Diese gelten sowohl für registrierte als auch für nicht registrierte Vorsorgeeinrichtung gleichermassen. Die Pflicht zur Aufbewahrung von Vorsorgeunterlagen ist in Art. 27i–27k BVV2 geregelt. Die Aufbewahrung von Geschäftsunterlagen richtet sich nach Art. 47 Abs. 4 BVV2 bzw. Art. 958f OR (siehe dazu ASIP-Fachmitteilung Nr. 130, S. 9f.; https://www.datatrust.ch/gesetzesgrundlagen/).</p> <p>„Anonymisiert“ sind Daten, die Personenbezug hatten, bei denen der Personenbezug aber bewusst aufgehoben wurde (z.B. Anonymisierung der Personendaten durch Aggregation derselben). Das Datenschutzrecht gilt für diese Daten deshalb nicht mehr. Datenschutzrechtlich ist die Bearbeitung dieser Daten daher nicht mehr eingeschränkt. Eine Anonymisierung von Personendaten hat demzufolge datenschutzrechtlich dieselbe Wirkung wie eine Löschung derselben. Denn wenn das Datenschutzrecht für anonyme Daten nicht gilt, kann auch nicht ihre Löschung verlangt werden. Somit fallen anonymisierte Personendaten als anonyme Daten nicht unter das „Recht auf Vergessen“.</p> <p><i>Siehe ASIP-Webinare Datenschutz vom 10./14./15. November 2022, Folien 23f.</i></p>
AUTOMATISIERTE DATENVERARBEITUNGSPROZESSE	
Welche Datenverarbeitungsprozesse gelten im Pensionskassenbereich als automatisiert?	<p>Unter „Automatisierung“ sind „automatisierte Einzelentscheide“ zu verstehen. Dabei trifft die Maschine eine Entscheidung aufgrund einer von der Maschine sich antrainierten oder von einem Menschen einprogrammierten Bewertung der der Maschine vorliegenden Personendaten.</p> <p>Im Hinblick auf die Datensicherheit (Art. 8 revDSG) sind geeignete technische und organisatorische Massnahmen für die Gewährleistung einer angemessenen Datensicherheit vorzukehren. Die Datensicherheit zielt auf den Schutz der Vertraulichkeit (keine unbefugten Zugriffe), der Integrität (Korrektheit bzw. Unversehrtheit) sowie der Verfügbarkeit (Zugriff auf Daten) von Daten. Neu sind datenschutzfreundliche Voreinstellungen („privacy by design and default“²) erforderlich (Art. 7 Abs. 3 revDSG).</p> <p>Die Vorsorgeeinrichtung hat mit Blick auf das Profiling bzw. das Profiling mit hohem Risiko abzuklären, welche Datenverarbeitungsprozesse im Pensionskassenbereich als automatisiert gelten, da der Datenschutz auch technisch gewährleistet sein muss.</p> <p>Dabei gibt es beispielsweise folgende Möglichkeiten der Prozessautomatisierung (Entlastung der Mitarbeitenden bei der Bearbeitung: Robotic Process Automation [RPA]): 1. Zahlungseingangsprozess, 2. Eintrittsprozess, 3. Lohn-</p>

² „Privacy by design“ beinhaltet die Pflicht, Prozesse und Projekte so zu gestalten, dass die Einhaltung des Datenschutzes von Anfang an berücksichtigt wird. Im Sinne von „privacy by default“ ist mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt.

	<p>und Beschäftigungsgradänderung, 4. Einkaufsanfrage. Bei der Erstellung von Vorsorgeausweisen empfiehlt es sich, der Informationspflicht gemäss Art. 21 Abs. 4 revDSG nachzukommen und einen Verweis beispielsweise mit "*dieses Dokument wurde automatisch erstellt** anzubringen (ASIP-Fachmitteilungen Nr. 130, S. 4, und Nr. 131, S. 9).</p>
<p>ABLAGE DER PROTOKOLLE</p>	
<p>Wie und in welcher Form sollten die Protokolle getrennt vom System abgelegt werden?</p>	<p>Das ist eine technische Frage, welche die Vorsorgeeinrichtungen mit ihren IT-Unternehmen regeln müssen.</p>
<p>MELDEPROZESS BEIM EDÖB</p>	
<p>Gibt es bereits Detailinformationen zum Meldeprozess beim EDÖB?</p>	<p>Es gibt noch keine Detailinformationen bezüglich der Meldepflichten. Betroffen sind die Meldepflicht der Bearbeitungsverzeichnisse der registrierten Vorsorgeeinrichtungen (Art. 12 Abs. 4 revDSG) und die Meldepflicht des Verantwortlichen von Datenschutzverletzungen, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen (Art. 24 revDSG). <i>Siehe dazu https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news.html#-642810745.</i></p>
<p>UNTERSCHIEDUNG SCHÜTZENSWERTE UND BESONDERS SCHÜTZENSWERTE PERSONENDATEN</p>	
<p>Welche Daten werden als besonders schützenswert erachtet. (z.B. Zivilstand, IV-Grad usw.)</p>	<p>Besonders schützenswerte Daten i.S. des revDSG sind:</p> <ol style="list-style-type: none"> 1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, 2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, 3. genetische Daten, 4. biometrische Daten, die eine natürliche Person eindeutig identifizieren, 5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen, 6. Daten über Massnahmen der sozialen Hilfe (Art. 5 lit. c revDSG).
<p>DATENSCHUTZBERATER</p>	
<p>Ist es mit Blick auf die fachliche Unabhängigkeit und Weisungsungebundenheit des Datenschutzberaters</p>	<p>1. Es ist für eine Vorsorgeeinrichtung möglich, den Datenschutzberater des Arbeitgebers als eigenen Datenschutzberater zu ernennen. Auch können mehrere Bundesorgane (registrierte Vorsorgeeinrichtungen) gemeinsam einen Datenschutzberater ernennen (Art. 25 revDSV). Nicht registrierten Vorsorgeeinrichtungen ist die Ernennung eines Datenschutzberaters freigestellt.</p>

<p>gemäss Art. 10 Abs. 3 lit. a revDSG denkbar, dass die Pensionskasse den Datenschutzberater des Arbeitgebers ernennt, oder sind da Interessenskonflikte zu befürchten, die einer solchen Ernennung entgegenstehen?</p>	<p>2. Die fachliche Unabhängigkeit und Weisungsungebundenheit sind vertraglich sicherzustellen. Dabei ist zu beachten, dass Personen, welche pensionskassenintern als für den Datenschutz zuständig erklärt werden, nicht automatisch als Datenschutzberater im Sinne von Art. 10 revDSG gelten. Die Datenschutzberater müssen als solche bezeichnet werden.</p> <p><i>Siehe ASIP-Webinare Datenschutz vom 10./14./15. November 2022, Folie 26.</i></p>
<p>Sind mit der in der ASIP-Fachmitteilung Nr. 131, S. 8 unten, angekündigten IT-basierten Plattform die Anforderungen des neuen DSG an ein Bundesorgan abgedeckt, oder muss man parallel zur IT-basierten Plattform noch andere Aufgaben beachten?</p>	<p>Durch die vom ASIP für seine Mitglieder zur Verfügung gestellte IT-basierte Plattform (verbunden mit regelmässiger Begleitung und entsprechenden Schulungsangeboten) soll den Vorsorgeeinrichtungen die Suche eines Datenschutzberaters teilweise erleichtert werden. Die Ernennung desselben muss jedoch durch die jeweilige Vorsorgeeinrichtung selbst vorgenommen werden (zwingende Weisungsungebundenheit des Datenschutzberaters). Allerdings besteht für die registrierten Vorsorgeeinrichtungen die Möglichkeit, dass mehrere Bundesorgane gemeinsam einen Datenschutzberater bzw. eine Datenschutzberaterin ernennen können (Art. 25 revDSV). Mit dessen Ernennung ist das Erfordernis des revDSG erfüllt. Die Aufgaben des Datenschutzberaters (Art. 10 Abs. 2 revDSG und Art. 26 Abs. 2 revDSV) sind: a. Schulung und Beratung des obersten Organs im Bereich des Datenschutzes, b. Mitwirkung bei der Anwendung der Datenschutzvorschriften (Prüfung der Bearbeitung von Personendaten, Empfehlung von Korrekturmassnahmen nach Feststellung einer Verletzung der Datenschutzvorschriften, c. Beratung der Verantwortlichen bei der Erstellung der Datenschutz-Folgenabschätzung und Überprüfung von deren Ausführung) und d. Ansprechpartner für die versicherten Personen und die Datenschutzbehörden.</p> <p><i>Siehe ASIP-Webinare Datenschutz vom 10./14./15. November 2022, Folie 26.</i></p>
<p>Nach Art. 27 Abs. 2 DSV muss der/die Datenschutzberater/in auf dem Internet publiziert werden. Als firmeneigene Pensionskasse betreiben wir keine öffentlich-zugängliche Website. Muss extra für diese Information eine solche erstellt werden?</p>	<p>Ja, grundsätzlich schon. Allenfalls besteht die Möglichkeit einer Veröffentlichung auf der Website des Arbeitgebers (Firma).</p>

OUTSOURCING-VERHÄLTNISSE	
<p>Vereinbarungen zur Datenverarbeitung sind mit Dienstleistern und IT-Providern abzuschliessen:</p> <p>1. Was bedeutet dies im Outsourcing-Verhältnis (Auslagerung der Verwaltung)? Reicht die Bestätigung des Outsourcing-Partners für ihre IT-Provider (Cloud, PK-Software)</p> <p>2. Subdelegation vom Processor an Sub-Processor ist nur mit vorgängiger Genehmigung des Verantwortlichen zulässig. Wie sehen Sie das in der Praxis? Sind namentliche Nennungen notwendig?</p> <p>3. Gilt die Post als Verantwortliche oder als Datenbearbeiterin gemäss revDSG?</p>	<p>1. Hat die Vorsorgeeinrichtung ihre Verwaltung an einen Dritten ausgelagert, so erfolgt die Datenbearbeitung durch die (technische) Verwaltung (als Auftragsbearbeiter) im Auftrag der Vorsorgeeinrichtung (Art. 9 revDSG). Letztere muss dann insbesondere sicherstellen, dass die Verwaltung in der Lage ist, die Datensicherheit zu gewährleisten, da die Vorsorgeeinrichtung weiterhin verantwortlich ist. Ein weiteres Beispiel eines Auftragsbearbeiters ist der Cloud-Provider (Cloud-Software). In diesem Fall muss die ganze Kette von der Vorsorgeeinrichtung über den/die Software-Anbieter und Cloud-Provider vertraglich abgesichert sein. Des Weiteren darf der Auftragsbearbeiter die Bearbeitung nur mit vorgängiger Genehmigung der Vorsorgeeinrichtung einem Dritten übertragen. In allen Fällen ist ein entsprechender Vertrag abzuschliessen (Auftragsbearbeitungsvertrag oder „Data Processing Agreement“). Dabei gilt der Cloud-Provider (bei der Speicherung von Daten auf der vom IT-Provider betriebenen Cloud) lediglich als Auftragsbearbeiter gemäss revDSG, die Vorsorgeeinrichtung jedoch ist Verantwortliche. Sie hat sämtliche verwaltungs- und IT-technischen Abläufe vertraglich zu regeln.</p> <p>2. Ja. Die Vorsorgeeinrichtung hat als Verantwortliche gemäss revDSG auch das Verhältnis vom Processor zum Sub-Processor vertraglich mit dem Outsourcing-Partner zu regeln. Dabei sind namentliche Nennungen nicht notwendig (Ausnahme: Bearbeitungsverzeichnis; <i>siehe oben</i>).</p> <p>3. Für die Datenbearbeitung auf der Transportebene – wozu auch die Adressen auf den Postsendungen gehören – ist die Post verantwortlich (= Verantwortliche nach revDSG); die Datenbearbeitung auf der Inhaltsebene – was die Kunden in ihren Briefen oder auf ihren Postkarten schreiben – ist Sache der Postkunden, hier also der Vorsorgeeinrichtung (Vorsorgeeinrichtung = Verantwortliche nach revDSG). Es liegt keine gemeinsame Verantwortlichkeit der Vorsorgeeinrichtung und der Post vor, sondern diese sind je auf ihrer Tätigkeitsebene Verantwortliche gemäss revDSG. Deshalb tangiert ein von der Post fehlzugestellter Brief nicht die datenschutzrechtliche Verantwortlichkeit der Vorsorgeeinrichtung, hier der Vorsorgeeinrichtung, während ein falschadressierter Brief einzig die Verantwortlichkeit der Vorsorgeeinrichtung ist mit entsprechenden Folgen etwa für die Meldepflichten bei Datenschutzverstößen.</p> <p><i>Siehe David Rosenthal, Controller oder Processor: Die datenschutzrechtliche Grechtenfrage, in: Jusletter 17. Juni 2019, Rz. 87.</i></p>
<p>Wie gestaltet sich das Verhältnis der Vorsorgeeinrichtung als Verantwortliche zu anderen Verantwortlichen gemäss revDSG?</p>	<p>Wenn eine Vorsorgeeinrichtung im Bereich ihrer Tätigkeit als Bundesorgan Dienstleistungen an einen Datenschutzverantwortlichen (wie PK-Experte, Anwalt, etc.) outsourced, dann muss der externe Dienstleister ebenfalls über einen Datenschutzberater verfügen.</p> <p>Als Verantwortlicher muss er wie die Vorsorgeeinrichtung selbst alle gesetzlichen Anforderungen erfüllen, dies im Unterschied zum Auftragsbearbeiter.</p>

	<p>Im Verhältnis der Vorsorgeeinrichtung (Verantwortliche) zu einem Dritten, der ebenfalls Verantwortlicher ist (insbesondere zu Organen gemäss Art. 52 BVG), empfiehlt sich eine vertragliche Regelung für den Datentransfer von der Vorsorgeeinrichtung zu diesem Dritten (Abgrenzung der Verantwortlichkeiten gemäss revDSG und Art. 52 BVG) (ASIP-Fachmitteilung Nr. 131, S. 8).</p>
UNTERSTELLUNG DER KANTONALEN ÖFFENTL.-RECHTL. VORSORGEINRICHTUNGEN UNTER DAS REVDSG?	
<p>1. Was muss eine kantonale öffentlich-rechtliche Vorsorgeeinrichtung betreffend revDSG unternehmen? 2. Untersteht eine öffentlich-rechtliche Vorsorgeeinrichtung nach der Verselbstständigung dem kantonalen DSG? 3. Muss eine kantonale öffentlich-rechtliche Vorsorgeeinrichtung einen Datenschutzberater gemäss revDSG ernennen? 4. Würden Sie öffentlich-rechtlichen Vorsorgeeinrichtungen trotzdem anraten – im Sinne des Vorsichtsprinzips – die grundsätzlichen Bestimmungen und Vorgaben (z.B. Erstellung Bearbeitungsverzeichnis) des revDSG für registrierte Pensionskassen zu implementieren? Oder wäre Ihre Empfehlung für das weitere Vorgehen für öffentlich-</p>	<p>1./2. Es kann in verschiedenen Rechtsbereichen zu Abgrenzungsschwierigkeiten zwischen Datenschutzvorschriften des Bundes und der Kantone kommen. Insbesondere stellen sich diese Fragen z.B. dann, wenn kantonale Behörden Bundesrecht vollziehen. Als Beispiel mag der angehängte Datenschutzleitfaden des SECO für den Bereich AVIG und AVG dienen (siehe Abschnitt „Geltungsbereiche“, Randziffern 2 bis 5 des Leitfadens). Das eidgenössische Recht i.S.v. Art. 3 Abs. 1 Datenschutzgesetz (bGS 146.1) kann daher das (n)DSG des Bundes, aber namentlich auch sektorielle Datenschutzvorschriften auf eidgenössischer Ebene meinen. 3./4. Es können Konstellationen vorkommen, in denen Datenschutzvorschriften aus der Gesetzgebung des Bundes z.B. im Bereich der beruflichen Vorsorge oder aus weiteren Sozialversicherungszweigen auf Datenbearbeitungen Anwendung finden, welche eine kantonale öffentlich-rechtliche Vorsorgeeinrichtung vornimmt. Es ist im Grundsatz aber so, dass eine öffentlich-rechtliche Vorsorgeeinrichtung als öffentliches Organ des Kantons dem kantonalen DSG untersteht. Es handelt sich bei einer kantonalen öffentlich-rechtlichen Vorsorgeeinrichtung weder um ein Bundesorgan noch um eine private Person gemäss revDSG, weshalb sie prinzipiell nicht in den Geltungsbereich der Datenschutzgesetzgebung des Bundes fällt. Punktuell kann es jedoch Ausnahmen geben. Für die kantonalen öffentlich-rechtlichen Vorsorgeeinrichtungen besteht im Hinblick auf das Inkrafttreten des totalrevidierten Datenschutzgesetzes des Bundes kein dringender, zwingender Handlungsbedarf; insbesondere sind sie nicht verpflichtet, einen Datenschutzberater zu ernennen. Angesichts ihrer Aufgaben, die regelmässig das Bearbeiten von besonders schützenswerten Personendaten beinhalten, ist es trotzdem geboten, dass die kantonalen öffentlich-rechtlichen Vorsorgeeinrichtungen die Compliance im Bereich Datenschutz sicherstellen.</p>

rechtliche Pensionskassen?	
BEKANNTGABE VON PERSONENDATEN INS AUSLAND	
Was ist unter der „Gewährleistung eines angemessenen Schutzes durch die Gesetzgebung des betreffenden Staates oder das internationale Organ“ (Art. 16 Abs. 1 revDSG/Art. 8 revDSV) zu verstehen?	<p>Es bedeutet, dass Personendaten ins Ausland nur dann bekannt gegeben werden dürfen, wenn der betreffende Staat einen angemessenen Datenschutz gewährleistet. Falls sich der Staat nicht auf der Liste befindet, muss ein geeigneter Datenschutz anders gewährleistet werden, beispielsweise mittels der Verwendung von Standardvertragsklauseln (Art. 9-12 revDSV). Siehe zu dieser Thematik die Ausführungen des EDÖB zu Datenübermittlungen ins Ausland: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html#-741117193: „Die Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau gestützt auf anerkannte Standardvertragsklauseln und Musterverträge“ vom 27. August 2021.</p> <p>Sowohl registrierte als auch nicht-registrierte Pensionskassen müssen überprüfen, ob Datentransfers ins Ausland stattfinden und – falls dies der Fall ist – ob die Grundsätze von Art. 16 revDSG eingehalten werden oder die Datenbekanntgabe ins Ausland allenfalls gestützt auf eine Ausnahme nach Art. 17 revDSG erfolgen darf. Dabei dürfen Personendaten ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet (Art. 16 Abs. 1 revDSG). Liegt kein Entscheid des Bundesrates nach Absatz 1 vor, so dürfen Personendaten ins Ausland bekanntgegeben werden, wenn ein geeigneter Datenschutz gewährleistet wird durch: a. einen völkerrechtlichen Vertrag; b. Datenschutzklauseln in einem Vertrag zwischen dem Verantwortlichen oder dem Auftragsbearbeiter und seiner Vertragspartnerin oder seinem Vertragspartner, die dem EDÖB vorgängig mitgeteilt wurden; c. spezifische Garantien, die das zuständige Bundesorgan erarbeitet und dem EDÖB vorgängig mitgeteilt hat; d. Standarddatenschutzklauseln, die der EDÖB vorgängig genehmigt, ausgestellt oder anerkannt hat; oder e. verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig vom EDÖB oder von einer für den Datenschutz zuständigen Behörde eines Staates, der einen angemessenen Schutz gewährleistet, genehmigt wurden (Art. 16 Abs. 2 revDSG). Der Bundesrat kann andere geeignete Garantien im Sinne von Absatz 2 vorsehen (Art. 16 Abs. 3 revDSG). Ausnahmen in Art. 17 revDSG.</p>
ABGRENZUNG REVDSG/INFORMATIONSSICHERHEITSGESETZ (ISG)	
Neu werden die Vorsorgeeinrichtungen als Bundesorgan eingestuft. Hat dies neben den höheren Anforder-	Die DSG-Revision hat keine direkten Auswirkungen auf das geltende DSG und das revDSG. Der ASIP befürwortete – angesichts der Tatsache, dass Cyberrisiken schon seit etlichen Jahren auch für Pensionskassen und deren Versicherte bzw. Rentnerinnen und Rentner ein grosses Risiko darstellen – in seiner Vernehmlassung vom 14.04.2022 grundsätzlich das neue ISG. Wir begrüßten dabei die im Erläuterungsbericht, S. 18f., erwähnte Möglichkeit der

rungen im DSG auch noch weitere Auswirkungen (z.B. Unterstellung ISG) falls ja, welche?	Einschränkung der Meldepflicht aller registrierten und nicht registrierten Vorsorge- und Freizügigkeitseinrichtungen gemäss Art. 74a i.V.m. Art. 74b lit. j E-ISG. ³
-----------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

³ <https://www.inter-pension.ch/uploads/1/1/8/3/118397790/informationssicherheitsgesetz.pdf>; https://www.inter-pension.ch/uploads/1/1/8/3/118397790/erlaeuternder_bericht.pdf.