

Umsetzung des revidierten Datenschutzgesetzes (DSG): Fragen aus der Datenschutz-Tagung vom 20. März 2023	
Fragen	Antworten
MELDEPLATTFORM EDÖB	
Ist der Inhalt auf der Meldeplattform EDÖB für die Öffentlichkeit jederzeit einsehbar?	Ja. Der EDÖB veröffentlicht die Meldungen der Bundesorgane gemäss Art. 56 revDSG in einem öffentlich zugänglichen Register, dem DataReg (Meldepflicht nur für Verzeichnisse von Bundesorganen [Art. 12 Abs. 4 revDSG]). Siehe https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/unternehmen/anmeldung-einer-datensammlung.html
ORGANISATIONSREGLEMENT	
Muss das Organisations- oder Vorsorgereglement formell per 01.09.2023 genehmigt sein?	Das Organisationsreglement muss per 01.09.2023 formell durch das oberste Organ genehmigt sein. Das Vorsorgereglement allein genügt nicht.
BEARBEITUNGSREGLEMENT	
Ist eine Mehrzahl von Bearbeitungsreglementen möglich?	Ja: Bearbeitungsreglement von Bundesorganen bei automatisierter Bearbeitung u.a. von besonders schützenswerten Personendaten oder bei automatisierter Durchführung eines Profilings (Art. 6 revDSV); Bearbeitungsreglement von privaten Personen, d.h. von nicht registrierten Vorsorgeeinrichtungen, bei automatisierter Bearbeitung besonders schützenswerter Personendaten in grossem Umfang oder bei automatisierter Durchführung eines Profilings mit hohem Risiko (Art. 5 revDSV).
EINWILLIGUNG DER VERSICHERTEN PERSON ODER DES RENTNERS/DER RENTNERIN	
Kann eine Einwilligung generell via PK-Reglement erfolgen?	Grundsätzlich ja, bei Abgabe des PK-Reglements. Die vom Bundesrat noch vorgeschlagene Klarstellung, wonach eine Einwilligung eindeutig erfolgen muss, wurde vom Parlament gestrichen. Somit gilt im neuen Da-

	<p>tenschutzrecht „kein anderer Standard für Einwilligungen [...], wie bisher und sonst im Schweizer Recht für Willenserklärungen.“ Gemäss dem massgebenden Art. 6 Abs. 6 revDSG¹ ist zwar grundsätzlich keine Einwilligung erforderlich, Art. 6 Abs. 7 revDSG fordert jedoch eine ausdrückliche Einwilligung für:</p> <ul style="list-style-type: none">a. die Bearbeitung von besonders schützenswerten Personendaten;b. ein Profiling mit hohem Risiko durch eine private Person; oderc. ein Profiling durch ein Bundesorgan (Art. 6 Abs. 7 revDSG). <p>Besonders schützenswerte Daten i.S. des revDSG sind:</p> <ul 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>In welchen Fällen eine Einwilligung erforderlich ist bzw. als Rechtfertigungsgrund dient, legt das DSG in folgenden Artikeln fest: Art. 17 Abs. 1 lit. a revDSG (Datenexport), Art. 21 Abs. 3 lit. b revDSG (automatisierte Einzelfallentscheide), Art. 25 Abs. 3 revDSG (Auskunftsrecht betreffend Gesundheitsdaten), Art. 31 Abs. 1 revDSG (Rechtfertigungsgründe), Art. 34 Abs. 4 lit. b revDSG (Bearbeitung ohne hinreichende Rechtsgrundlage durch Bundesorgane) und Art. 36 Abs. 2 lit. b revDSG (Bekanntgabe von Personendaten durch Bundesorgane).</p> <p><i>Siehe David Rosenthal, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in: Jusletter 17. Juni 2019, Rz. 30f.</i></p>
DATENTRANSFER INS AUSLAND?	
<p>Wenn Daten in der Cloud gespeichert werden, ist nicht klar, wo diese Daten genau liegen. Ist das dann ein Datentransfer ins Ausland?</p>	<p>Der Cloud-Provider (bei der Speicherung von Daten auf der vom IT-Provider betriebenen Cloud) gilt lediglich als Auftragsbearbeiter gemäss revDSG, die Vorsorgeeinrichtung jedoch ist Verantwortliche. Sie hat sämtliche verwaltungs- und IT-technischen Abläufe vertraglich zu regeln (Auftragsbearbeitungsvertrag oder „Data Processing Agreement“). Es muss die ganze Kette von der Vorsorgeeinrichtung über den/die Software-Anbieter und Cloud-Provider vertraglich abgesichert sein. Im Weiteren darf der Auftragsbearbeiter die Bearbeitung nur mit vorgängiger Genehmigung der Vorsorgeeinrichtung einem Dritten übertragen.</p> <p>Wer beispielsweise Personendaten aus der Schweiz seiner eigenen Zweigniederlassung im Ausland zugäng-</p>

¹ „Ist die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie für eine oder mehrere bestimmte Bearbeitungen nach angemessener Information freiwillig erteilt wird.“

	<p>lich macht, muss sich an Art. 16f. revDSG und Art. 8-12 revDSV halten. Dies analog auch, wenn eine Vorsorgeeinrichtung Personendaten ihrem sich im Ausland befindenden Cloud-Provider zukommen lässt. Die Vorsorgeeinrichtung hat den betroffenen Personen, d.h. den Versicherten und Rentnern/Rentnerinnen den Staat, in welchem sich der Cloud-Provider befindet, in der Datenschutzerklärung mitzuteilen (Art. 19 Abs. 4 revDSG).</p> <p><i>Siehe David Rosenthal, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in: Jusletter 17. Juni 2019, Rz. 66.</i></p>
<p>a) Handelt es sich beim Versand eines Versicherungsausweises an eine im Ausland wohnhafte versicherte Person um einen Datentransfer ins Ausland gemäss Definition DSG?</p> <p>b) Handelt es sich bei der Benützung eines Mitgliederportals durch eine im Ausland wohnhafte versicherte Person um einen Datentransfer ins Ausland gemäss Definition DSG?</p>	<p>a) Nein. Unter «Bekanntgeben» ist das «Übermitteln oder Zugänglichmachen von Personendaten» (Art. 5 lit. e revDSG) zu verstehen. Das «Bekanntgeben» erfordert begriffslogisch, dass der Kreis der Personen, die über die betreffende Information verfügen, erweitert wird.</p> <p><i>Siehe David Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, Rz. 66.</i></p> <p>b) Nein. Es gilt Antwort unter a). Anders verhält es sich, wenn eine Vorsorgeeinrichtung Personendaten ihrem sich im Ausland befindenden Cloud-Provider zukommen lässt (Art. 16f. revDSG; Art. 8-12 revDSV). Die Vorsorgeeinrichtung hat den betroffenen Personen, d.h. den Versicherten und Rentnern/Rentnerinnen den Staat, in welchem sich der Cloud-Provider befindet, in der Datenschutzerklärung mitzuteilen (Art. 19 Abs. 4 revDSG).</p> <p><i>Siehe David Rosenthal, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in: Jusletter 17. Juni 2019, Rz. 66.</i></p>
<p>EXTERNE PARTNER</p>	
<p>Können externe Partner grundsätzlich als Datenverarbeiter von der Unterstellung unter das revDSG ausgeschlossen werden, wenn diese ausschliesslich nur noch mit anonymen Daten arbeiten? (IT-Provider, Experten, Revisoren, ...)</p>	<p>Ja, wobei die Experten und Revisoren – im Unterschied zu den IT-Providern – als Verantwortliche gelten. Eine Anonymisierung von Personendaten hat 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>LÖSCHUNG ODER ANONYMISIERUNG DER DATEN: UMSETZUNG</p>	

<p>Wie werden Sie die Löschung von Versichertendaten handhaben? Z.B. Informationen über die Zahlung einer FZL-Leistung.</p>	<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.</p> <p>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>Siehe ASIP-Webinare Datenschutz vom 10./14./15. November 2022, Folien 23f.</p>
<p>DATENAUSTAUSCH MIT VERSICHERTEN UND RENTNERINNEN UND RENTNERN</p>	
<p>Datenaustausch mit Versicherten z.B. ausgetretenen Mitarbeiterinnen und Mitarbeitern via Email: Was sind die Anforderungen bezüglich des Versands von persönlichen Versicherungsausweisen etc. Ist ein Email-Versand zulässig und, falls ja, welcher Anforderungen bedarf es?</p>	<p>Nein. Mit dem revidierten DSG wird in der Schweiz erstmals eine Pflicht zur einer sog. Data Breach Notification eingeführt: Wird eine Email falsch versandt oder kommt es anderweitig zu einem Datenverlust oder einem anderen Datensicherheitsvorfall, muss dies neu unter Umständen dem EDÖB gemeldet werden. Eine Verletzung der Datensicherheit ist dem EDÖB so rasch als möglich zu melden, falls die Verletzung voraussichtlich zu einem hohen Risiko für die betroffene Person führt. Die betroffene Person muss ebenfalls informiert werden, falls dies zu ihrem Schutz erforderlich ist oder der EDÖB dies verlangt (Art. 24 revDSG/Art. 15 revDSV).</p> <p><i>Siehe David Rosenthal, Controller oder Processor: datenschutzrechtliche Gretchenfrage, in: Jusletter 17. Juni 2019, Rz. 160.</i></p>
<p>DATENSCHUTZBERATERIN/DATENSCHUTZBERATER</p>	
<p>Ist die Ernennung der Datenschutzberaterin bzw. des Datenschutzberaters (Art. 25 revDSV) zwingend Sache des obersten Or-</p>	<p>Die Ernennung der Datenschutzberaterin bzw. des Datenschutzberaters liegt beim obersten Organ der Vorsorgeeinrichtung. Erstens gehört nämlich der Datenschutz (Umsetzung des revDSG) zur Organisation der Vorsorgeeinrichtung, ist somit Teil einer unentziehbaren und undelegierbaren Aufgabe des obersten Organs (Art. 51a Abs. 1 i.V.m. Art. 49 Abs. 2 Ziff. 7 BVG), und zweitens ergibt sich dieses Erfordernis auch aus den</p>

<p>ganes, oder kann dies auch durch die Geschäftsführung geschehen?</p>	<p>Aufgaben der Datenschutzberaterin bzw. des Datenschutzberaters (Art. 10 Abs. 2 revDSG und Art. 26 Abs. 2 revDSV): 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. <i>Siehe ASIP-Webinare Datenschutz vom 10./14./15. November 2022, Folie 26.</i></p>
---	---