

Stuttgart, den 19.03.2019

An sämtliche
Versicherungsämter, Stadt- und Gemeindeverwaltungen
und Versichertenberaterinnen und -berater im Bereich
der Deutschen Rentenversicherung Baden-Württemberg

I. Gesetz zur Leistungsverbesserung und Stabilisierung in der gesetzlichen Rentenversicherung (RV-Leistungsverbesserungs- und -Stabilisierungsgesetz)

Mit den nachstehenden Ausführungen wollen wir Sie – ergänzend zu unserem Infobrief Nr. 03/18 – über die Gesetzesänderungen zum RV-Leistungsverbesserungs- und -Stabilisierungsgesetz allgemein informieren.

1. Weitere Verbesserungen für Mütter mit vor 1992 geborenen Kindern, sog. „Mütterrente II“

Ausgehend von der Erweiterung der rentenrechtlichen Anerkennung der Erziehungsleistung durch das RV-Leistungsverbesserungsgesetz vom 23.06.2014 (sog. Mütterrente I) verlängert das aktuelle RV-Leistungsverbesserungs- und -Stabilisierungsgesetz die Kindererziehungszeit für vor 1992 geborene Kinder um weitere 6 Monate auf 2,5 Jahre.

Wie schon bei der Mütterrente I werden die Regelungen für Bestandsrentner aus Gründen der Verwaltungspraktikabilität anders ausgestaltet als die Regelungen für Rentenneuzugänge.

a) Erhöhung von Bestandsrenten um einen Zuschlag für Kindererziehung

Sofern bereits am 31.12.2018 ein Anspruch auf Rente bestand, in dem Kindererziehungszeiten für ein vor 1992 geborenes Kind enthalten sind, werden diese Renten um einen Zuschlag in Höhe eines halben persönlichen Entgeltpunkts pro berücksichtigungsfähigem Kind erhöht.

Die Erhöhung der Renten erfolgt rückwirkend anhand eines bundesweit abgestimmten Terminplans im März und April 2019. Die DRV Baden-Württemberg hat die Erhöhung für ihre Rentner durchgeführt, diese haben die Einmalzahlung sowie ihren Bescheid Mitte März erhalten. Die laufende Rentenzahlung wurde ebenfalls entsprechend erhöht.

b) Versicherte und Rentenneuzugänge mit einem Rentenbeginn ab 01.01.2019

Bei Renten mit einem Rentenbeginn ab dem 01.01.2019 werden künftig 30 Kalendermonate Kindererziehung für ein vor 1992 geborenes Kind anerkannt. Bei bereits bewilligten Renten sind die erhöhten Kindererziehungszeiten bereits im Rentenbescheid berücksichtigt.

Für Versicherte, die noch keine Rente beziehen ist auch hier ein gesonderter Antrag auf Anerkennung der zusätzlichen 6 Monate Kindererziehungszeiten grundsätzlich nicht erforderlich, sofern für diese Kinder bereits Berücksichtigungszeiten anerkannt wurden. Versicherte, die ihre Kindererziehungszeiten für vor 1992 geborene Kinder bisher noch nicht beantragt haben, sollten dies, spätestens mit dem Rentenantrag, nachholen.

Für den Personenkreis der bereits vor dem 01.01.2019 die Regelaltersrente erreicht hat und durch die zusätzliche Anerkennung von Kindererziehungszeiten erstmalig die Wartezeit für eine Regelaltersrente erfüllt, ist ein Rentenantrag bis spätestens zum 30.04.2019 zu stellen, damit die Regelaltersrente zum 01.01.2019 beginnen kann.

Sollte trotz zusätzlicher Anerkennung von Kindererziehungszeiten die Wartezeit für die Regelaltersrente immer noch nicht erfüllt sein, besteht die Möglichkeit der Zahlung von freiwilligen Beiträgen. Um die dabei zu berücksichtigenden Antragsfristen einzuhalten, wird eine individuelle Beratung bei einer unserer Auskunft- und Beratungsstellen empfohlen.

Ansprechpartnerin:

Frau Andrea Ziegler-Bochmann
Tel. 0711 848-17223
Fax 0711 825-17099
E-Mail andrea.ziegler-bochmann@drv-bw.de
De-Mail grundsatz@drv-bw.de-mail.de

oder Ihre regional zuständigen
Ansprechpartner

II. "Hochrechnung" durch den Rentenversicherungsträger auf Grundlage der durch den Arbeitgeber abgegebenen "Gesonderten Meldung" (§ 194 SGB VI)

Was ist die Hochrechnung?

Mit der sogenannten Hochrechnung hat der Gesetzgeber die Grundlagen dafür geschaffen, unkompliziert die nahtlose Leistungsgewährung umzusetzen. Sowohl der Rentenantragssteller als auch der Rentenversicherungsträger müssen bei einem bestehenden Beschäftigungsverhältnis nicht bis zur endgültigen Entgeltmeldung des Arbeitgebers warten, bis die Rente bearbeitet und berechnet werden kann. Das Rentenverfahren kann somit regelmäßig verkürzt werden.

Bei der Hochrechnung muss der Arbeitgeber eine gesonderte Meldung abgeben. Diese beinhaltet das bereits erzielte Arbeitsentgelt und wird in der Regel drei Monate vor dem gewünschten Rentenbeginn abgegeben. Die Aufforderung zur Meldung erfolgt grundsätzlich elektronisch durch den Rentenversicherungsträger.

Der Rentenversicherungsträger errechnet für die maximal letzten drei Monate vor Rentenbeginn der Altersrente (Hochrechnungszeitraum) ein voraussichtliches beitragspflichtiges Arbeitsentgelt auf der Grundlage der für die letzten 12 Kalendermonate gemeldeten Entgelte.

Wo liegen die Vorteile?

Die Bescheiderteilung erfolgt regelmäßig vor dem Rentenbeginn. So steht der Bescheid auch frühzeitig für die Beantragung der Betriebsrente zu Verfügung.

Sind die tatsächlichen beitragspflichtigen Einnahmen jedoch höher oder niedriger als die hochgerechneten beitragspflichtigen Einnahmen, verbleibt es bei diesen Beträgen. Es erfolgt später keine Neufeststellung der Rente. Die tatsächlichen Entgelte wirken sich erst bei einer späteren Rente (z. B. Hinterbliebenenrente) aus.

Erwarten Versicherte im Hochrechnungszeitraum Sonderzahlungen (Urlaubsgeld oder Weihnachtsgeld sowie beitragspflichtige Abfindungen), sollte vor der Beantragung der Altersrente ggf. eine Auskunft- und Beratungsstelle aufgesucht werden, um sich hinsichtlich der konkreten Auswirkungen beraten zu lassen.

Was passiert, wenn auf die Hochrechnung verzichtet wird?

Bei Verzicht auf die Hochrechnung wird die Altersrente erst nach Eingang der endgültigen Meldung des Arbeitgebers festgesetzt. Da diese Meldung erst nach Beendigung des Beschäftigungsverhältnisses an den Rentenversicherungsträger übermittelt wird, führt dies dazu, dass die Rentenfestsetzung erst nach dem gewünschten Rentenbeginn erfolgen kann und eine Auszahlung der Rente sich dadurch verzögert.

Wo finde ich die Frage im Vordruck R0100?

Im Antragsformular R0100 (Antrag auf Versichertenrente) sind unter der Ziffer 9.4.1, sowie im Antragsformular R0110 (Verkürzter Antrag auf Versichertenrente) unter der Ziffer 7.2.1 ausdrücklich Fragen enthalten, die sich auf die Anforderung der "Gesonderten Meldung" beziehen.

Wie kann die Beratung von Versicherten erfolgen?

Die Versicherten sollen im Rahmen der Rentenanspruchstellung auf die Möglichkeit des Hochrechnungsverfahrens hingewiesen werden, um eine nahtlose Rentengewährung zu ermöglichen. Die Beratung soll dabei anhand der Erläuterungen (R0101) zu der entsprechenden Frage im Rentenanspruchsformular (R0100) erfolgen. In Zweifelsfällen empfehlen wir die persönliche Beratung.

Ansprechpartner:

Herr Martin Branz
Tel. 0711 848-17228
Fax 0711 848-17099
E-Mail martin.branz@drv-bw.de
De-Mail grundsatz@drv-bw.de-mail.de

oder Ihre regional zuständigen
Ansprechpartner

III. Die Grundrente

Die Bundesregierung beabsichtigt, in dieser Legislaturperiode eine sogenannte Grundrente einzuführen. Sie soll all jenen ein regelmäßiges Alterseinkommen zehn Prozent oberhalb des Grundsicherungsbedarfs garantieren, die 35 Jahre an Beitragszeiten oder Zeiten der Erziehung oder Pflege aufweisen.

Aktuell werden verschiedene Modelle einer Umsetzung der von der Koalition geplanten Grundrente in Politik und Medien diskutiert. Die Grundrente kann derzeit noch nicht beantragt werden. Sobald Genaueres, insbesondere zu Zeitpunkten und Gesetzgebungsverfahren, feststeht, werden wir wieder informieren.

Falls Ihren Kunden Rente und ein eventuelles weiteres Einkommen nicht für den Lebensunterhalt ausreichen, besteht möglicherweise Anspruch auf Grundsicherung. Die Broschüren „Die Grundsicherung: Hilfe für Rentner“ und „Tipps für Rentnerinnen und Rentner“ können ausgehändigt werden.

Ansprechpartnerin:

Frau Tatjana Döring
Tel. 0711 848-17221
Fax 0711 848-17099
E-Mail tatjana.doering@drv-bw.de
De-Mail grundatz@drv-bw.de-mail.de

oder Ihre regional zuständigen
Ansprechpartner

IV. Beendigung des Auftragsgeschäfts „Rentenvorverfahren“

Bislang war bei der Aufnahme von Neuanträgen auf

- Rente wegen Erwerbsminderung
- große Witwen- oder Witwerrente aufgrund von Erwerbsminderung

zu beachten, dass die medizinischen Ermittlungen von den Arbeitsbereichen „Rentenvorverfahren“ durchgeführt wurden, weswegen Besonderheiten bei dem Versand des Unterschriftenblattes sowie der weiteren Unterlagen zu beachten waren.

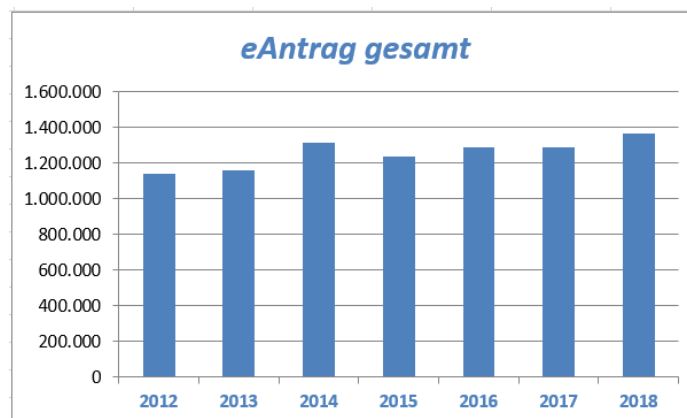
Dieses Auftragsgeschäft „Rentenvorverfahren“ wurde gekündigt. Bei der Antragsaufnahme sind daher die Unterlagen zu den aufgenommenen Rentenansprüchen nun **direkt an die Hauptverwaltung der DRV Bund** zu übersenden.

Ansprechpartnerin:

Frau Stefanie Schuhmacher
Tel. 0711 848-17292
Fax 0711 848-49-17292
E-Mail stefanie.schuhmacher@drv-bw.de
De-Mail grundsatz@drv-bw.de-mail.de
oder Ihre regional zuständigen
Ansprechpartner

V. 20 Jahre elektronische Antragsaufnahme – die DRV Baden-Württemberg sagt „Danke“!

Seit 1998 stellt die Deutsche Rentenversicherung den Gemeinden und Versicherungsämtern (GuV) das Programm „Antrag Online“ sowie „eAntrag/Expertenversion“ in verschiedenen Varianten zur Verfügung. In **über 950 baden-württembergischen Rathäusern** nutzen die Mitarbeiterinnen und Mitarbeiter die elektronische Antragsaufnahme und stellen uns die Anträge digital strukturiert und damit automatisch verarbeitbar zur Verfügung. Auch die Mitarbeiter der DRV sowie die ehrenamtlich tätigen Versichertenberater nutzen tagtäglich die elektronische Antragsaufnahme. Die Zahl der elektronischen Antragsgänge von jährlich mittlerweile 1,35 Mio. steigt weiter.



Die DRV-Gremien haben beschlossen, die bei wenigen Gemeinden noch eingesetzte **Offline-Variante** zum 31. Dezember 2019 einzustellen. Wir bieten den bisherigen „**Offline-Gemeinden**“ sowie den „**Ortsbehörden ohne eAntrag**“ für den eAntrag-Einstieg eine kompetente fachliche und technische Unterstützung an. Die Rentenversicherungsträger sind darum bemüht, Anwendern bzw. den Antragstellern das Ausfüllen von umfangreichen Papierformularen zu ersparen. Die eAntrag-Verantwortlichen haben für Interessenten die **Teilnahmeerklärung** zur Nutzung der eAntrag-Variante 3 mit Sendefunktion beigefügt.

Deutsche Rentenversicherung - Elektronische Antragstellung

Bei der Nutzung von eAntrag mit einer personenbezogenen Signaturkarte ist es den Rentenversicherungsträgern nach §151 a SGB VI zwischenzeitlich möglich, den Nutzern umfangreiche Daten (z.B. Versicherungslücken, Zeiten der Kindererziehung, Ausbildungszeiten etc.) aus dem jeweiligen Versicherungskonto in eAntrag zur Verfügung zu stellen. Auch diese eAntrag-Variante wird Gemeinden und Versicherungsämtern kostenlos zur Verfügung gestellt. Jährliche Kosten entstehen den Behörde für die Signaturkarte sowie einmalige Aufwendungen für ein Kartenlesegerät. Es können aber auch die gleichen Karten beschafft bzw. genutzt werden, welche bereits im Einwohnermeldeamt im Einsatz sind. Aktuell nutzen bereits ca. 50 Gemeinden und Versicherungsämter diese Variante mit Datenabruf.

Deutsche Rentenversicherung - Hinweise zu Signaturkarten und Kartenlesern

Eine Übersicht zum Datenabruf aus dem jeweiligen Versicherungskonto ist diesem Infobrief beigefügt, ebenso die genehmigten Leit- und Richtlinien. Bei Interesse an einem erweiterten Datenabruf bitten wir Sie, die Verpflichtungserklärung ausgefüllt und unterschrieben an die eAntrag-Ansprechpartner der DRV Baden-Württemberg zurückzusenden. Den Administratoren der Gemeinden und Versicherungsämter übersendet die DRV Baden-Württemberg anschließend weitere Informationen.

Als Anlagen sind beigefügt:

- Teilnahmeerklärung zur Nutzung rveServices –eAntrag/Expertenversion Var. 3
- Übersicht des Datenabrufs nach §151a SGB VI im Feb. 2019
- Leit- und Richtlinien - Datenabruf im Verfahren rveServices –eAntrag/Expertenversion Var. 4
- Registrierungsdaten und Verpflichtungserklärung der Gemeinde bzw. Versicherungsamt Var. 4

Für fachliche Fragen stehen Ihnen die nachstehenden Ansprechpartner zur Verfügung:

<p>Ansprechpartner: Herr Stephan Kuntz Tel. 0721 825-23322 Fax 0721 825-99-23322 E-Mail stephan.kuntz@drv-bw.de De-Mail oeco@drv-bw.de-mail.de oder Ihre regional zuständigen Ansprechpartner</p>	<p>Ansprechpartner: Herr Gert Hiller Tel. 0711 848-23321 Fax 0711 848-49-23321 E-Mail gert.hiller@drv-bw.de De-Mail oeco@drv-bw.de-mail.de oder Ihre regional zuständigen Ansprechpartner</p>
--	--

VI. Versand der Infobriefe per Newsletter

Über das geänderte Versandverfahren zum Infobrief haben wir Sie im Vorfeld schon mehrfach informiert.

Seit vielen Jahren erhalten Sie von der Deutschen Rentenversicherung drei bis vier Mal im Jahr den Infobrief, der Sie aktuell und zuverlässig über alles Wissenswerte zur gesetzlichen Rentenversicherung informiert.

Der Versand erfolgte bisher grundsätzlich per E-Mail. Ab dem Infobrief 01/19 erhalten alle die Stellen und Personen, die sich seit Dezember 2018 schon zum Newsletter angemeldet haben, zusätzlich zum Newsletter den Infobrief auch noch per Mail.

Im Rahmen einer modernen und effizienten Verwaltung werden wir den Versand des Infobriefes auf Newsletter umstellen.

Mit dem Infobrief 03/19 erhalten Sie den Infobrief nicht mehr über die bei uns hinterlegte E-Mail-Adresse oder in wenigen Ausnahmefällen über den Postweg, sondern nur noch als Newsletter.

Hierzu hat die Deutsche Rentenversicherung Baden-Württemberg auf ihrer Internetseite www.deutsche-rentenversicherung-bw.de unter Services\Fachinfos\Newsletter der DRV Baden-Württemberg den [Newsletter-Service](#) für Sie eingerichtet. Dort finden Sie das Newsletter-Anmeldeformular zur Registrierung und können sich ganz **einfach und bequem** für unseren Newsletter für die **Stadt- und Gemeindeverwaltungen sowie die Versichertenberater** anmelden.

Ansprechpartnerin:

Frau Karin Ille
Tel. 0711 848-17314
Fax 0711 848-49-17315
E-Mail karin.ille@drv-bw.de
De-Mail grundsatz@drv-bw.de-mail.de
oder Ihre regional zuständigen
Ansprechpartner

Ansprechpartnerin:

Frau Susanne Gödecke
Tel. 0711 848-17315
Fax 0711 848-49-17315
E-Mail susanne.goedecke@drv-bw.de
De-Mail grundsatz@drv-bw.de-mail.de
oder Ihre regional zuständigen
Ansprechpartner

Mit freundlichen Grüßen
Fachsupport, Zentrale Dienste, Prüfdienste

gez.

Iding

Anlage „Formulare“

Die meisten Papierformulare stellt die Deutsche Rentenversicherung auch in den Programmen zur Online-Antragstellung (eAntrag) zur Verfügung. Für einen schnellen und effizienten Kontakt mit der Rentenversicherung nutzen Sie bitte möglichst diese Anwendung anstelle von Papiervordrucken.

Formularnummer	Formularbezeichnung	aktuelle Auflage	Auflage vernichten bis
R0815-00	Merkblatt - Krankenversicherung der Rentner (KVdR) und Pflegeversicherung	01.01.2019 (AGRTAQ)	01.01.2018 (AGRTAQ)
R0820-00	Antrag auf Zuschuss zur Krankenversicherung (§ 106 SGB VI)	01.01.2019 (AGRTAQ)	07.06.2018 (AGRTAQ)
V0091-00	Berechnungsgrößen und Beitragswerte	15.11.2018 (AGBGLBE)	07.11.2017 (AGBGLBE)
V0100-00	Antrag auf Kontenklärung (kein Rentenantrag)	27.06.2018 (AGKK)	25.05.2018 (AGKK)
V0110-00	Erläuterungen zum Antrag auf Kontenklärung	27.06.2018 (AGKK)	25.05.2018 (AGKK)
V0800-00	Antrag auf Feststellung von KEZ/BÜZ wegen Kindererziehung	27.06.2018 (AGKK)	15.11.2017 (AGKK) Version 25.05.18 (DSGVO)
V0900-00	Antrag auf Beitragserstattung bei Aufenthalt im Inland	27.06.2018 (AGKK)	25.05.2018 (AGKK)
V0910-00	Erläuterungen zum Antrag auf Beitragserstattung bei Aufenthalt im Inland	27.06.2018 (AGKK)	30.01.2018 (AGKK)

Ansprechpartner:

Ulrike Jung
Telefon 0721 825-17415
Telefax 0721 825-99-17415
E-Mail: ulrike.jung@drv-bw.de

Susanne Gödecke
Telefon 0711 848-17315
Telefax 0711 848-49-17315
E-Mail: susanne.goedecke@drv-bw.de

oder Ihre regional zuständigen Ansprechpartner



Teilnahme am Verfahren eAntrag/Expertenversion

(bitte senden Sie dieses Formular ausgefüllt zurück)

A Registrierungsdaten

Zuständiger Rentenversicherungsträger		Versicherungsamt / Gemeinde	
Name	DRV Baden-Württemberg	Name	
Straße/Postfach	Gartenstraße 105	Straße/Postfach	
PLZ/Ort	76122 Karlsruhe	PLZ/Ort	
		E-Mail	

Ansprechpartner Fachverfahren		weitere Ansprechpartner Fachverfahren	
Vorname		Vorname	
Nachname		Nachname	
Tel.		Tel.	
Fax		Fax	
E-Mail		E-Mail	

Ansprechpartner Technik		Ansprechpartner Datenschutz/IT-Sicherheit	
Vorname		Vorname	
Nachname		Nachname	
Tel.		Tel.	
Fax		Fax	
E-Mail		E-Mail	

Hard- und Software			
Anzahl PC's mit eAntrag/Experten-Version:		Anzahl der Anwender:	
PC-Konfiguration	<input type="checkbox"/> Lokales Netzwerk <input type="checkbox"/> Ausschließlich stand-alone-PC's <input type="checkbox"/> Lokales Netzwerk und stand-alone-PC's	Betriebssystem Client	<input type="checkbox"/> Win NT <input type="checkbox"/> Win XP <input type="checkbox"/> Windows 7 <input type="checkbox"/> anderes:

B Programmversion



mit zentraler Benutzerverwaltung
ohne Signaturkarte
ohne Datenabruf, aber senden des Antrags möglich; ggf. spätere Anwendung mit Signaturkarte

Erläuterungen:

Nach Vorliegen der Teilnahmeerklärung werden Ihnen die Hinweise zur Installation und die erforderlichen Zugangsdaten des Programms zugesendet.
Die Anwender des Programms benötigen eine Internetverbindung

C Erklärung und Unterschrift

1. Für die Teilnahme am Verfahren mit Datenübermittlung an die Deutsche Rentenversicherung ist die Unterzeichnung dieser Erklärung und die Übersendung an die Deutsche Rentenversicherung erforderlich.
2. Die teilnehmende Gemeindebehörde bzw. das teilnehmende Versicherungsamt erklärt, die erforderlichen Maßnahmen zur Gewährleistung der IT-Sicherheit zu beachten und einzuhalten.
3. Ausdrücklich wird erklärt, dass durch die teilnehmende Gemeinde bzw. das teilnehmende Versicherungsamt alle Maßnahmen umgesetzt werden, die den bestimmungsgemäßen Gebrauch der durch die Deutsche Rentenversicherung zur Verfügung gestellten Software sowie die Übermittlung von unverfälschten Sozialdaten gewährleisten.
4. Die Installationsanleitung und die entsprechenden Programmhandbücher für das Verfahren eAntrag werden beachtet.

Die vorstehende Erklärung wird zur Kenntnis genommen und bestätigt.

Ort, Datum

Unterschrift des Behördenleiters/Dienstsiegel

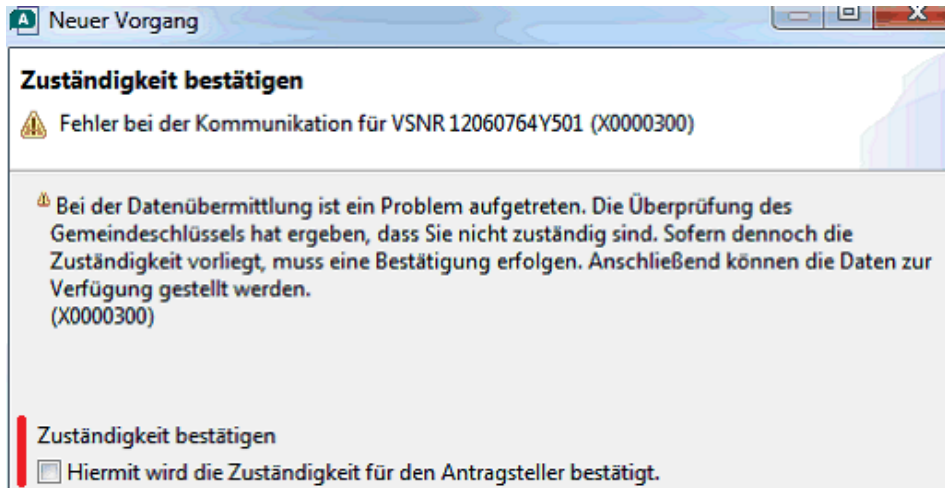
Abruf von Daten aus dem Versicherungskonto

Bitte beachten Sie, dass diese Funktionalität nur für Nutzer der Online-Variante mit Datenabruf zur Verfügung steht.

Mit Erweiterung des Datenkataloges nach § 151a SGB VI wurden für rveServices - eAntrag/Expertenversion die Voraussetzungen geschaffen, Daten aus dem Versicherungskonto in einem größeren Umfang als bisher abzurufen. Konkret bestehen mit Einsatz der Version 4.2.1 folgende weitere Abrufmöglichkeiten aus dem Rentenversicherungskonto:

- Vorbelegung der Anschrift des Versicherten.
- Übermittlung des aktuellen Kontoführers und dessen Vorbelegung im R0810 sowie in den allgemeinen Druckvorgaben in der Anwendung.
- Übermittlung und Vorbelegung des Datums des letzten Zuzuges aus dem Ausland des Versicherten.
- Datum der letzten Kontenklärung.
- Übermittlung und Vorbelegung des Datums des Eintritts in die Versicherung.
- Übermittlung von Informationen zu den im Konto bereits gespeicherten Kindern.
- Übermittlung von Informationen zum Umfang der im Konto vorhandenen ungeklärten Erziehungszeiten.
- Übermittlung von bereits im Versicherungskonto erfassten Berufsausbildungszeiten.
- Automatische Vorbelegung der im Versicherungskonto bereits erfassten Vorversicherungszeiten im R0810.
- Abruf von Informationen hinsichtlich bestehender Versicherungslücken im Konto.
- Anzeige von Wartezeitmonaten aus dem Versicherungskonto.

- Bei vollmaschineller Feststellung, dass der Wohnort eines Versicherten / Hinterbliebenen außerhalb des Bezirks des Versicherungsamtes liegt, wird der Datenabruf trotzdem freigegeben, sofern Sie die örtliche Zuständigkeit des Versicherungsamtes in rveServices - eAntrag/Expertenversion ausdrücklich bestätigen.



- Übermittlung des aktuellen Kontoführers und Vorbelegung im R0810 (Ziffer 8.3) sowie in den allgemeinen Druckvorgaben in rveServices - eAntrag/Expertenversion.
- Übermittlung des Datums des Eintritts in die Versicherung zur Vorbelegung der Frage ‚Wann wurde erstmalig eine Erwerbstätigkeit aufgenommen -ggf. auch im Ausland- ?‘ (Frage 4.2 bzw. 5.3) im R0810.
- Es werden Informationen zum Umfang der im Konto vorhandenen ungeklärten Erziehungszeiten übermittelt. Die Kontodaten können mittels der neuen Schaltfläche „Zeiten der Kindererziehung im Versicherungskonto“ an den relevanten Fragen (z.B. V0100 Ziffer 6.1) zur Anzeige gebracht werden.

Angaben zu Kindern

Haben Sie Kinder innerhalb der ersten 10 Lebensjahre erzogen, für die Zeiten der Kindererziehung bisher nicht bei Ihnen angerechnet wurden?

unbeantwortet nein ja

- Im Konto vorhandene Kinder können im V0800 bei der Frage ‚Angaben zu den Kindern‘ sowie im Rentenantrag bei der Frage ‚Elterneigenschaft für die Pflegeversicherung‘ vorbelegt werden.
- Es werden die Berufsausbildungszeiten aus dem Versicherungskonto übermittelt. Konkret werden inländische Berufsausbildungszeiten (Beitragszeiten) übermittelt. Die Kontodaten können mittels der neuen Schaltfläche ‚Berufsausbildungszeiten im

Versicherungskonto' an den relevanten Fragen (z.B. R0100 Ziffer 5.3) zur Anzeige gebracht werden.

Haben Sie Zeiten der **Berufsausbildung** (auch ohne Abschluss) zurückgelegt?

unbeantwortet nein ja

- Die Informationen zu den zuständigen Einzugsstellen werden übermittelt und in der Frage zu den Vorversicherungszeiten im R0810, sowie der Frage nach der gesetzlichen Krankenkasse im R0100 vorbelegt bzw. als Vorbelegungsauswahl angeboten.

Solange keine Kontodaten übermittelt werden, sind die neuen Schaltflächen zur Anzeige der Kontodaten insensitiv.

Angaben zu Kindern

Haben Sie Kinder innerhalb der ersten 10 Lebensjahre erzogen, für die Zeiten der Kindererziehung bisher nicht bei Ihnen angerechnet wurden?

unbeantwortet nein ja

Sobald die Daten aus dem Konto geliefert werden können, erfolgen weitere Informationen.

Die ab Juli 2017 zur Verfügung stehende Version 3.10 von rveServices - eAntrag/Expertenversion enthält die Funktionalitäten für die Verarbeitung des mit Inkrafttreten des 6. SGB IV-Änderungsgesetzes erweiterten Datenkatalog des § 151a SGB VI und die Erweiterung auf alle Leistungsberechtigte. Allerdings können die Informationen über die Erfüllung der Wartezeiten und die Lücken im Versicherungsverlauf seitens der Deutschen Rentenversicherung voraussichtlich erst mit der nächsten Version von rveServices – eAntrag/Expertenversion aus dem Versicherungskonto zur Verfügung gestellt werden.

Die vorbereitenden Maßnahmen zur Anzeige in rveServices - eAntrag/Expertenversion wurden in der Version 3.10 bereits getroffen:

Beantragte Rente(n)

Beantragte Rente(n)

Beantragte Rente	Die Antragstellung erfolgt wegen eines Hinweises des Re

Hinzufügen

Bearbeiten

Entfernen

Erweiterung des Abrufs von Daten aus dem Versicherungskonto

In rveServices - eAntrag/Expertenversion wurden die Voraussetzungen geschaffen weitere Daten aus dem Versicherungskonto abzurufen und anzuzeigen. Konkret wurden zur Version 01/2019 folgende weitere Abrufmöglichkeiten umgesetzt:

1. Übermittlung der Lücken im Versicherungskonto

Zur Klärung / Überprüfung des Versicherungskontos werden die Lücken im Versicherungsverlauf übermittelt, an deren Klärung der Versicherte noch nicht mitgewirkt hat.

Voraussetzung hierfür ist, dass der Auftrag zur Ermittlung der Lücken im Konto verarbeitet werden kann (-> fehlerfreies Konto).

Die Lücken im Versicherungsverlauf werden mittels der Schaltfläche „Ungeklärte Lücken im Versicherungsverlauf“ an folgenden Fragen zur Verfügung gestellt:

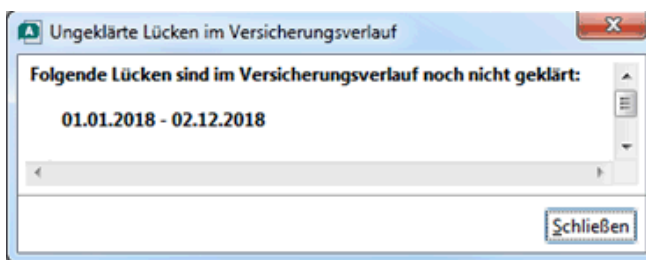
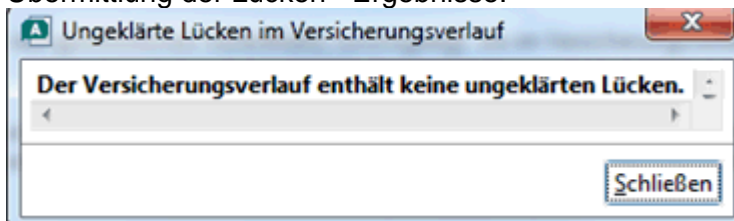
- „Beitragszeiten oder Beschäftigungszeiten im Inland“ für die Anträge R0100, R0110, R0500, V0100 und V0900 zur Verfügung gestellt.
- „Beantragte Rente(n)“ im R0100 und R0110.

Beitragszeiten im Inland

Haben Sie Beitragszeiten oder Beschäftigungszeiten zurückgelegt, die im Versicherungsverlauf nicht erwerbsmäßig tätige Pflegeperson)?

un beantwortet nein ja

Übermittlung der Lücken - Ergebnisse:



Der Zeitraum der Lückenprüfung endet grundsätzlich mit dem Tag vor der Verarbeitung. Sofern bereits ein Todestag vorhanden ist, endet der Zeitraum an diesem Tag.

2. Übermittlung der Wartezeit

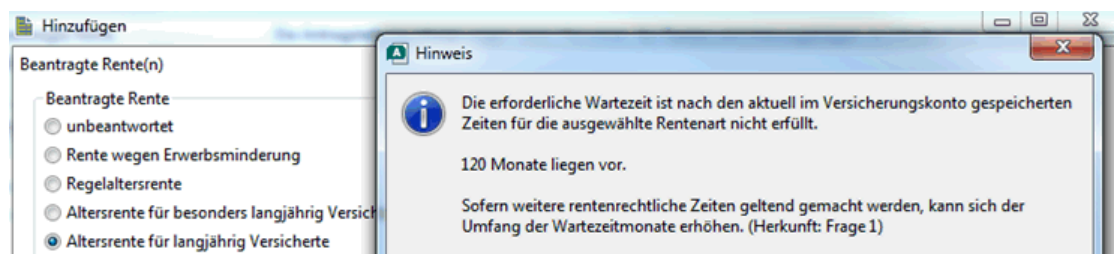
Aus dem Versicherungskonto wird die Auskunft übermittelt in welchem Umfang Wartezeitmonate (einschließlich der Wartezeiterfüllung nach § 52 SGB VI) vorhanden sind.

Voraussetzung hierfür ist, dass der Auftrag zur Ermittlung der Wartezeitmonate im Konto verarbeitet werden kann (-> fehlerfreies Konto, Wartezeitaufstellung möglich).

Die Information über den Umfang der vorhandenen Wartezeitmonate wird für die jeweilige Rentenart mittels eines dynamischen Hinweises angezeigt.

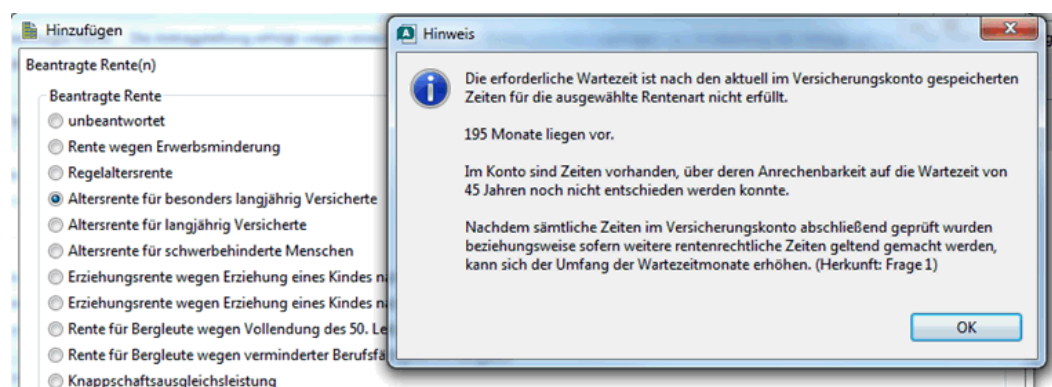
Ein Hinweis erfolgt nur, sofern Wartezeitmonate übermittelt wurden und die Wartezeit für die ausgewählte Rentenart nicht erfüllt ist.

Übermittlung der Wartezeit – Ergebnisse



Übermittlung der Wartezeit -> **Besonderheit "Altersrente für besonders langjährig Versicherte"**

Ein besonderer Hinweis für die "Altersrente für besonders langjährig Versicherte" erfolgt, sofern das Versicherungskonto Zeiten enthält, deren Anrechenbarkeit auf die Wartezeit von 45 Jahren nicht maschinell geprüft werden kann.



Leitlinie und Richtlinien zur IT- Sicherheit

**bei Nutzung des Verfahrens
eAntrag der
Deutschen Rentenversicherung in den
Gemeindebehörden und
Versicherungsämtern**

003.00.00

Autor

Michael Vogel

Deutsche Rentenversicherung Rheinland-Pfalz

Tel.:+49 (0)6232 17-2747

E-Mail: michael.vogel@drv-rlp.de

Inhaltsverzeichnis

Präambel	5
1	Leitlinie zur IT-Sicherheit für den Einsatz des Verfahrens "eAntrag"7
1.1	Verantwortung für die IT-Sicherheit.....7
1.2	Geltungsbereich.....7
1.3	Sicherheitsziele.....7
1.4	Definition des Schutzbedarfs.....8
1.5	Genehmigung und Änderung9
1.6	Ansprechpartner für das Verfahren „eAntrag“ bei der Deutschen Rentenversicherung..... 10
1.7	Verantwortliche für das Verfahren „eAntrag“ bei den Gemeindebehörden und Versicherungsämtern 10
2	Richtlinien11
2.1	IT-Sicherheitskoordinator 11
2.2	Benutzer- und Zugangsverwaltung..... 12
2.2.1	Einrichten und Ändern von Zugriffen 12
2.2.2	Umgang und Regelungen mit Signaturkarten..... 13
2.2.3	Umgang und Regelungen mit PINs der Signaturkarten 13
2.3	Personal 15
2.3.1	Einarbeitung/Einweisung neuer Mitarbeiter 15
2.3.2	Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen 15
2.3.3	Vertretungsregeln 15
2.3.4	Ausscheiden eines Mitarbeiters 16
2.4	Behandlung von Sicherheitsvorfällen 17
2.4.1	Sicherheitsvorfälle..... 17
2.4.2	Eskalationsstufen/Behandlung von Sicherheitsvorfällen..... 17
2.4.3	Konsequenzen bei Verstößen 18
2.4.4	Reaktion auf Störungen oder Alarmierungen 18
2.4.5	Evaluierung der Eskalationsstrategie 19
2.5	Wartungs- und Reparaturarbeiten..... 19
2.5.1	Interne Wartungs- und Reparaturarbeiten 20
2.5.2	Externe Wartungs- und Reparaturarbeiten..... 20
2.5.3	Ordnungsgemäße Entsorgung von Betriebsmitteln 20
3	Alarmierungsplan bei Sicherheitsvorfällen.....21
4	Erforderliche Sicherheitsmaßnahmen für Hardware und Betriebssysteme24
4.1	Generelle Maßnahmen für obligatorische IT-Komponenten und Ressourcen..... 24
	Baustein B 1.13 Sensibilisierung und Schulung zur Informationssicherheit 25
	Baustein B 1.14 Patch und Änderungsmanagement 25

Baustein B 1.4 Datensicherungskonzept	26
Baustein B 1.6 Schutz vor Schadprogrammen	26
Baustein B 2.3 Büroraum	28
Baustein B 3.201 Allgemeiner Client	29
Baustein B 3.208 Internet-PC.....	30
Baustein B 3.301 Sicherheitsgateway (Firewall).....	32
Baustein B 3.406 Drucker, Kopierer und Multifunktionsgeräte.....	33
Baustein B 4.2 Netz- und Systemmanagement	34
4.2 Erweiterte Maßnahmen zu Hard- und Software.....	35
4.3 Empfohlene Maßnahmen zum IT-Sicherheitsmanagement.....	36
Baustein B 1.0 Sicherheitsmanagement.....	36
5 Verpflichtungserklärung.....	37
Glossar 39	

Präambel

Die Deutsche Rentenversicherung (DRV) bietet den Gemeindebehörden und Versicherungsämtern eine Softwarelösung zur computerunterstützten Antragserfassung (kurz "eAntrag") an.

Das Verfahren „eAntrag“ beinhaltet die Übertragung, Speicherung und Verarbeitung personenbezogener (Sozial-)Daten. Daher müssen technische und organisatorische Maßnahmen (z.B. Firewall, Virens Scanner etc.) getroffen werden, die erforderlich sind, um die Einhaltung der datenschutzrechtlichen Vorschriften zu gewährleisten (§ 78a SGB X).

Dies sind Maßnahmen mit dem Ziel,

- den Verlust der Vertraulichkeit,
- den Verlust der Transparenz,
- den Verlust der Revisionsfähigkeit,
- den Verlust der Integrität und
- den Verlust der Authentizität zu verhindern sowie
- die Verfügbarkeit der Verfahren und der Daten sicherzustellen.

Insoweit ist ein hoher Anspruch an die IT-Sicherheit besonders im Hinblick auf Integrität und Vertraulichkeit gegeben.

Durch die Deutsche Rentenversicherung Bund wurde daher für den IT-Verbund eAntrag ein IT-Sicherheitskonzept nach den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) 100-2 und 100-3 mit einer entsprechenden Risikoanalyse erstellt und umgesetzt.

Für den sicheren Einsatz des Verfahrens bei Gemeindebehörden und Versicherungsämtern sind bestimmte Mindestanforderungen bzw. Rahmenbedingungen erforderlich, die in der vorliegenden Leitlinie und den zugehörigen Richtlinien auf Grundlage der IT-Grundsicherungsstandards des Bundesamtes für Sicherheit in der Informationstechnik für den Einsatz des Verfahrens erstellt wurden. Dies entspricht auch den Anforderungen des § 151 a SGB VI für eine Onlineanbindung im Verfahren „eAntrag“.

Eine Vielzahl der erforderlichen Sicherheitsvorkehrungen beim Zugang zum Programm sowie für die Datenspeicherung und die Datenübermittlung sind bereits in den IT-Komponenten der Deutschen Rentenversicherung und in der Software selbst implementiert. Weitere Sicherheitsmaßnahmen sind für die sichere Nutzung von „eAntrag“ aber auch bei den eingesetzten IT-Komponenten der Gemeindebehörden bzw. Versicherungsämtern erforderlich.

Da die IT-Strukturen in den am Verfahren beteiligten Gemeindebehörden bzw. Versicherungsämtern sehr vielfältig sind, wurden zunächst alle in Frage kommenden IT-Komponenten ermittelt. Für IT-Komponenten definiert der BSI-Standard im Rahmen des IT-Grundschutzes sogenannte Bausteine, welche die Gefährdungen und entsprechende Gegenmaßnahmen beim Einsatz solcher Systeme beschreiben. Durch die Deutsche Rentenversicherung sind im Einvernehmen mit dem BSI zutreffende Maßnahmen für die Gemeindebehörden bzw. Versicherungsämter auf der Grundlage der 15. Ergänzungslieferung identifiziert und festgelegt worden. Sie sind nun Bestandteil dieses Dokuments. Die Einhaltung und Umsetzung dieser Maßnahmen obliegt den Gemeindebehörden bzw. Versicherungsämtern.

Einige der Maßnahmen betreffen direkt den Umgang mit dem Programm „eAntrag“ insbesondere sind organisatorische Maßnahmen hinsichtlich Personal, Behandlung von Sicherheitsvorfällen umzusetzen. Diese Maßnahmen sind im Teil 3 und Teil 4 des vorliegenden Dokumentes in den Richtlinien bzw. in den Handlungsanweisungen in Form eines Alarmierungsplanes beschrieben.

Neben diesen organisatorischen Regelungen muss gewährleistet sein, dass die für das Verfahren eingesetzte Hardware und Betriebssysteme sowie deren Handhabung den Sicherheitsanforderungen genügen. Dafür sind die Maßnahmen umzusetzen, welche im Teil 5 "Erforderliche Sicherheitsmaßnahmen für Hardware und Betriebssysteme" aufgelistet sind.

1 Leitlinie zur IT-Sicherheit für den Einsatz des Verfahrens "eAntrag"

1.1 Verantwortung für die IT-Sicherheit

Im Verfahren „eAntrag“ werden sensible, personenbezogene Antragsdaten von Bürgerinnen und Bürgern erfasst, übertragen und verarbeitet. Die Deutsche Rentenversicherung sieht sich direkt in der Verantwortung, umfassend für deren gesetzmäßige und korrekte Nutzung Sorge zu tragen.

Zur Wahrnehmung der Verantwortung durch die Deutsche Rentenversicherung finden die gültigen BSI-Standards 100-1 bis 100-3 hinsichtlich der Informationssicherheit bei Planung, Implementation und Betrieb des Verfahrens „eAntrag“ Anwendung.

Die Deutsche Rentenversicherung geht davon aus, dass bei konsequenter und durchgängiger Einhaltung dieser Standards, von der Erfassung der Daten bis hin zur Verarbeitung, ein sicherer Regelbetrieb und ein wirksames Risikomanagement gewährleistet sind und so dem Anspruch an die sichere Handhabung der Daten Genüge getan wird.

1.2 Geltungsbereich

Die vorliegende Leitlinie und die Richtlinien sind auf der Grundlage des im Einvernehmen mit dem BSI erstellten Sicherheitskonzepts gemäß § 151a SGB VI im Geltungsbereich der Gemeindebehörden und Versicherungsämter einzuhalten.

Der Geltungsbereich dieses Dokuments erstreckt sich auf alle Daten, Systeme und Netzwerkkomponenten, die im Zusammenhang mit dem Verfahren "eAntrag" stehen.

Dieses Dokument ist für alle Mitarbeiter der Gemeinden und der Versicherungsämter, die "eAntrag" bedienen, benutzen oder damit zu tun haben, bindend.

1.3 Sicherheitsziele

Für das Verfahren „eAntrag“ setzt sich die Deutsche Rentenversicherung folgende konkrete IT-Sicherheitsziele:

- Schutz von Sozialdaten bzw. personenbezogenen Daten nach den einschlägigen Rechtsvorschriften
- Sensibilisierung der Mitarbeiter für die Aufgabe IT-Sicherheit
- Sicherstellung einer hohen Verfügbarkeit für die Nutzer des Verfahrens

- Schutz von Hardware, Software und Daten vor Zerstörung, Verlust und Manipulation sowie Schutz vor Schadsoftware
- Gewährleistung des guten Rufes der Deutschen Rentenversicherung

1.4 Definition des Schutzbedarfs

Dieses Dokument dient der Realisierung und der Aufrechterhaltung eines hohen Schutzbedarfs im Hinblick auf Integrität und Vertraulichkeit der Daten gemäß Empfehlungen des BSI zum IT-Grundschutz.

Die Grundwerte der IT-Sicherheit sind beeinträchtigt, wenn

- vertrauliche Daten unberechtigt zur Kenntnis genommen oder weitergegeben werden (Verletzung der Vertraulichkeit).
- die Korrektheit der Daten und die Funktionsweise von Systemen nicht mehr gegeben ist (Verletzung der Integrität).
- berechnete Benutzer am Zugriff auf Daten und Systeme gehindert werden (Verletzung der Verfügbarkeit).

Die möglichen Schadensszenarien für diese Grundwerte wurden bewertet und im Rahmen des Sicherheitskonzeptes über sogenannte Schutzbedarfskategorien bewertet.

Die Deutsche Rentenversicherung hat im Verfahren „eAntrag“ folgende Einstufung mit der folgenden Begründung verbindlich festgelegt.

Grundwert Vertraulichkeit „Hoch“

Die Gemeindebehörden und Versicherungsämter sind nach § 35 Abs. 1 des Ersten Buches des Sozialgesetzbuches (SGB I) zur Einhaltung des Sozialdatenschutzes verpflichtet. Die über eAntrag/Expertenversion aufgenommenen Antragsdaten sind Sozialdaten. Sie unterliegen dem § 35 SGB I (Sozialgeheimnis). Erhoben werden dürfen die Daten nur mit dem Einverständnis des Antragstellers und ausschließlich für die Antragsaufnahme verarbeitet und genutzt werden. Sobald diese abgeschlossen ist, sind die Daten von den Gemeindebehörden und Versicherungsämtern zu löschen. Es ist § 78a SGB X (technische und organisatorische Maßnahmen) zum Schutz der Sozialdaten zu beachten. Unzulässige Datenerhebung, -verarbeitung und -nutzung führen zu Schadenersatzansprüchen nach § 82 SGB X. Der Imageschaden bei nicht sachgemäßer Erhebung, Verarbeitung und Nutzung ist als „beträchtlich“ einzustufen.

Für die Online-Abfrage von Daten für die Antragsaufnahme ist § 151a SGB VI zu beachten. Hier wird unter Abs. 1 die Zulässigkeit des Datenabrufs und unter Abs. 2 der abrufbare Datenumfang beschrieben. Die Beschreibung der Kategorie "sehr hoch" trifft allerdings nicht zu. Insgesamt ergibt sich aus dem Vorgenannten ein hoher Schutzbedarf.

Grundwert Integrität „Hoch“

Der Zugriff darf nur durch Berechtigte im Sinne des § 151a Abs. 1 SGB VI. erfolgen. Das bedeutet, nichtautorisierte Veränderung zwischengespeicherter Daten und unbefugte Veränderung der Bestandsdaten der Rentenversicherung sind zu verhindern. Der Imageschaden bei nicht sachgemäßer Erhebung, Verarbeitung und Nutzung ist als beträchtlich einzustufen. Insgesamt ergibt sich aus dem Vorgenannten ein hoher Schutzbedarf, die Beschreibung der Kategorie "sehr hoch" trifft nicht zu.

Grundwert Verfügbarkeit „Normal“

Die Erfassung von Rentenanträgen kann jederzeit über das übliche Papierverfahren erfolgen. Daher können bei Ausfall des automatisierten Verfahrens keine Fristversäumnisse ausgelöst werden und kein Schaden entstehen. Der Schutzbedarf für die Verfügbarkeit wird daher mit "gering bis mittel" eingestuft.

Aus der Einordnung in eine bestimmte Schutzbedarfskategorie ergeben sich organisatorische, personelle, infrastrukturelle und technische Maßnahmen, die in den folgenden Richtlinien und dem Alarmierungsplan beschrieben sind und die auf die eigenen beteiligten Systeme und die eigene Infrastruktur bei den Gemeinden und Versicherungsämtern angewendet und umgesetzt werden müssen.

Ein Unterschreiten, Abschwächen oder Missachten der festgelegten Maßnahmen führt direkt zu einem höheren Risiko der Verfahrenskompromittierung und ist damit nicht statthaft. Es ist erklärte Aufgabe und Verpflichtung eines jeden Beteiligten, seinen Beitrag zum sicheren Betrieb des Verfahrens „eAntrag“ zu leisten.

Die Einhaltung der festgelegten Richtlinien und Handlungsanweisungen sowie der Maßnahmen für Hardware und Betriebssysteme ist also eine Voraussetzung für die Teilnahme an dem „eAntrag“-Verfahren mit Datenabruf und Datenübermittlung und liegt auch im Verantwortungsbereich der Gemeindebehörden und Versicherungsämter (siehe Verpflichtungserklärung Teil 6).

1.5 Genehmigung und Änderung

Die Leitlinie und Richtlinien zur IT-Sicherheit des Verfahrens "eAntrag" wurden durch die Deutsche Rentenversicherung in Abstimmung mit dem BSI verabschiedet bzw. geändert und in Kraft gesetzt.

Die Deutsche Rentenversicherung ist für die Definition, Dokumentation und Freigabe von Sicherheitsstandards für das Verfahren „eAntrag“ verantwortlich.

Alle Vereinbarungen mit den Teilnehmern am „eAntrag“-Verfahren bedürfen einer schriftlichen Form.

Die Leitlinie und Richtlinien werden in ihrer Eigenschaft als ergänzende organisatorische Maßnahme zum Sicherheitskonzept des Verfahrens regelmäßig spätestens nach drei Jahren auf ihre Aktualität hin überprüft und gegebenenfalls angepasst.

Im Falle von Änderungen der Leitlinie und Richtlinien werden die Gemeindebehörden bzw. Versicherungsämter informiert. Bei wesentlichen Änderungen behält sich die Deutsche Rentenversicherung vor, eine Verpflichtungserklärung erneut einzufordern.

1.6 Ansprechpartner für das Verfahren „eAntrag“ bei der Deutschen Rentenversicherung

Die bei den Trägern der Deutschen Rentenversicherung eingerichtete Hotline für „eAntrag“ ist Ansprechpartner für Gemeindebehörden bzw. Versicherungsämter.

1.7 Verantwortliche für das Verfahren „eAntrag“ bei den Gemeindebehörden und Versicherungsämtern

Der Leiter der Gemeindebehörde bzw. des Versicherungsamtes ist der Verfahrensverantwortliche für „eAntrag“. Er bestätigt die Umsetzung und sorgt für die Einhaltung der Sicherheitsvorschriften, die in der Richtlinie und in den erforderlichen Basisicherheitsmaßnahmen beschrieben sind.

2 Richtlinien

In den Richtlinien sind für Gemeindebehörden und Versicherungsämter Maßnahmen festgelegt, deren Umsetzung die Sicherheit des Verfahrens „eAntrag“ gewährleistet.

2.1 IT-Sicherheitskoordinator

Jede der am Verfahren „eAntrag“ teilnehmenden Gemeindebehörden bzw. Versicherungsämter benennt den zuständigen Trägern der Deutschen Rentenversicherung einen IT-Sicherheitskoordinator und seinen Vertreter für den eigenen Verwaltungsbereich.

Er trägt die Verantwortung für:

- die Umsetzung von Sicherheitsstandards für Installation, Konfiguration, Betrieb und Nutzung des „eAntrag“-Verfahrens,
- die autorisierte und rechtzeitige Einleitung von Notfallmaßnahmen (Notfall-Verantwortlicher) bei Eintreten der unten definierten Sicherheitsvorfälle,
- die Entgegennahme von Meldungen über Sicherheitsvorfälle,
- die Untersuchung und Bewertung von Sicherheitsvorfällen,
- die Nachbearbeitung des Sicherheitsvorfalls und
- die Überprüfung der Einhaltung der Sicherheitsvorkehrungen.

Grundlage: BSI Grundschutzkatalog Organisation und Notfallvorsorge(M 2.1, M 6.112)

Festlegung von Verantwortlichkeiten und Regelungen

Aufbau einer geeigneten Organisationsstruktur für das Notfallmanagement

2.2 Benutzer- und Zugangsverwaltung

Der Leiter der Organisation, der für die Nutzung des Verfahrens verantwortlich ist und der IT-Sicherheitskoordinator regeln die Vergabe von Zugriffsrechten grundsätzlich und dokumentieren diese. Dabei ist nur den Benutzern und dem IT-Sicherheitskoordinator, die mit „eAntrag“ arbeiten, Schreib-/Lesezugriff auf alle Installationsverzeichnisse der aktuellen Version zu gewähren. Gegebenenfalls können auch Administratoren im Rahmen der Aufgabenwahrnehmung einen Zugriff haben.

Es ist darauf zu achten, dass die Rollentrennung von IT-Sicherheitskoordinator und Benutzer, wie im Verfahren vorgesehen, eingehalten wird. Sofern aus personellen Gegebenheiten eine Rollentrennung nicht möglich ist, muss dies von der externen Stelle bei der Deutschen Rentenversicherung mit ausführlicher Begründung beantragt werden.

Grundlage: BSI Grundschutzkatalog Organisation (M 2.7, M 2.8)

Vergabe von Zugangsberechtigungen

Vergabe von Zugriffsrechten

2.2.1 Einrichten und Ändern von Zugriffen

- Zugriffsberechtigte dürfen nur durch den jeweiligen IT-Sicherheitskoordinator eingerichtet werden.
- Wenn ein Mitarbeiter aus der abrufberechtigten Stelle ausscheidet bzw. nicht mehr am Verfahren teilnimmt, muss der ihm zugewiesene Zugriff unverzüglich stillgelegt werden.
- Die Vergabe und der Entzug von Zugangsrechten ist aktuell zu Dokumentieren.
- Um Missbrauch zu verhindern, ist bei längerer Abwesenheit der berechtigten Person die vorübergehende Sperrung des Zugriffs vorzunehmen.
- Für das Entsperren der Zugriffsberechtigung ist der zuständige IT-Sicherheitskoordinator der abrufberechtigten Stelle und sein Vertreter zuständig.
- Die Vergabe von Zugangsberechtigungen der Anwender sind dem IT-Sicherheitskoordinator und seinem Vertreter vorbehalten.
- Jeder Arbeitsplatzrechner eines Mitarbeiters muss so konfiguriert werden, dass nach 10 Minuten ohne Benutzerrückmeldung der manuelle Zugriff auf den Rechner automatisch gesperrt wird, z. B. durch einen Bildschirmschoner mit Passwortschutz.

Grundlage: BSI Grundschutzkatalog Organisation (M 2.7, M 2.8)

Vergabe von Zugangsberechtigungen

Vergabe von Zugriffsrechten

2.2.2 Umgang und Regelungen mit Signaturkarten

Beim Umgang mit Signaturkarten sind folgende Gebote zu beachten:

- Fremde Signaturkarten dürfen nicht ausprobiert oder genutzt werden.
- Die eigene Signaturkarte darf nicht
 - an andere Personen weitergegeben werden,
 - bei Verlassen des Arbeitsplatzes liegen bleiben,
 - so aufbewahrt werden, dass eine Benutzung durch Unbefugte ermöglicht wird.
- Der Verlust der Signaturkarte ist umgehend dem IT-Sicherheitskoordinator zu melden, damit die Zugriffsrechte gesperrt werden.
- Gefundene Signaturkarten sind umgehend bei dem IT-Sicherheitskoordinator bzw. seinem Vertreter abzugeben.

2.2.3 Umgang und Regelungen mit PINs der Signaturkarten

Beim Umgang mit PINs **der Signaturkarte** sind folgende Gebote zu beachten:

- Die PIN darf nicht leicht zu erraten sein.
- Die PIN muss geheim gehalten werden und darf nur dem Nutzer persönlich bekannt sein. Es ist verboten, die PIN zu hinterlegen.
- Ein PIN-Wechsel ist durchzuführen, wenn die PIN unautorisierten Personen bekannt geworden ist oder der Verdacht des Ausspähens besteht.
- Jeder Nutzer muss sich nach der Aufgabenerfüllung am Verfahren abmelden.
- Beim Verlassen des Arbeitsplatzes ist – um Missbrauch der Daten am Arbeitsplatz durch Dritte auszuschließen – der Zugang zum PC zu sperren.
- PINs sind unbeobachtet einzugeben und dürfen insbesondere nicht auf Funktionstasten hinterlegt werden.
- Fremde PINs dürfen nicht ausgeforscht, ausprobiert und benutzt werden.

Grundlage: BSI Grundschutzkatalog Organisation (M 2.7, M 2.8)

Vergabe von Zugangsberechtigungen

Vergabe von Zugriffsrechten

2.3 Personal

2.3.1 Einarbeitung/Einweisung neuer Mitarbeiter

Die Benutzer und IT-Sicherheitskoordinatoren, die mit „eAntrag“ arbeiten, erhalten eine Unterweisung in der Anwendung des Programms. Im Rahmen der Einweisung neuer Mitarbeiter müssen diese Leit- und Richtlinien und sonstige Handbücher bekannt gegeben werden.

Der IT-Sicherheitskoordinator muss außerdem Kenntnisse über die eingesetzten IT-Komponenten bzw. Protokolle besitzen und auch entsprechend geschult werden.

Grundlage: BSI Grundschutzkatalog Personal (M 3.1, M 3.4, M 3.5)

Geregelte Einarbeitung/Einweisung neuer Mitarbeiter

Schulung vor Programmnutzung

Schulung zu Sicherheitsmaßnahmen

2.3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen

Alle Mitarbeiter erhalten eine allgemeine Sicherheitsanweisung für die Nutzung der allgemeinen technischen Infrastruktur sowie der sicherheitsorganisatorischen Maßnahmen, die in einer Dienstanweisung zusammengefasst sind. Die Mitarbeiter sind auf die Einhaltung der einschlägigen Gesetze (z. B. § 5 BDSG "Datengeheimnis"), Vorschriften und Regelungen zu verpflichten. Die Verpflichtung muss von den Mitarbeitern gegengezeichnet werden.

Grundlage: BSI Grundschutzkatalog Personal (M 3.2)

Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen

2.3.3 Vertretungsregeln

Der gegenüber der Deutschen Rentenversicherung benannte IT-Sicherheitskoordinator und sein Stellvertreter der jeweils abrufberechtigten Gemeindebehörde bzw. des Versicherungsamtes vertreten sich entsprechend ihrer Rollenzuweisung gegenseitig.

Vertretungsregelungen haben den Sinn, für vorhersehbare Fälle (Urlaub, Dienstreise) und auch unvorhersehbare Fälle (Krankheit, Unfall, Kündigung) des Personenausfalls die Fortführung der Aufgabenwahrnehmung zu ermöglichen.

- Der Vertreter muss ausreichend geschult sein, damit er die Aufgaben inhaltlich übernehmen kann.
- Die Weitergabe von Signaturkarte und PIN ist nicht zulässig.

Grundlage: BSI Grundschutzkatalog Personal (M 3.3)

Vertretungsregelungen

2.3.4 Ausscheiden eines Mitarbeiters

- Beim Ausscheiden eines Mitarbeiters ist die Zugriffsberechtigung des Mitarbeiters unverzüglich zu sperren und zu löschen.
- Beim Ausscheiden eines Mitarbeiters ist zu gewährleisten, dass keine Daten vernichtet oder entwendet werden.

Grundlage: BSI Grundschutzkatalog Personal (M 3.6)

Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern

2.4 Behandlung von Sicherheitsvorfällen

2.4.1 Sicherheitsvorfälle

Als Sicherheitsvorfall wird ein Ereignis bezeichnet, das Auswirkungen nach sich ziehen kann, die einen hohen Schaden sowohl bezüglich Vertraulichkeit, Integrität als auch der Authentizität der Daten hervorrufen können. Die Verfügbarkeit hat dabei keine Bedeutung. Auf den Baustein B 1.8 der IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wird verwiesen.

Sicherheitsvorfälle werden zum Beispiel erkennbar durch:

- Vorgangsdaten, die ohne erkennbaren Grund verloren gehen oder auf die ein Zugriff nicht möglich ist (z.B. durch Datenmanipulation)
- ohne erkennbaren Grund gesperrte Kennungen
- Fehlermeldungen des Systems, die auf einen Missbrauch hindeuten
- Auftreten von Schadsoftware (z. B. Viren)
- vorsätzlicher Missbrauch der Anwendung (z.B. Speicherung von Screenshots)
- Abruf von Daten, die nicht für den Geschäftsablauf notwendig sind (Abruf zusätzlicher Versicherungskonten)

Grundlage: BSI Grundschutzkatalog Notfallvorsorge (M 6.58)

Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen

2.4.2 Eskalationsstufen/Behandlung von Sicherheitsvorfällen

Die Eskalationsstufen beschreiben ein hierarchisches Modell zur Behandlung von Sicherheitsvorfällen, bei dem jede höhere Stufe die Maßnahmen der darunter liegenden beinhaltet.

Für „eAntrag“ werden folgende Eskalationsstufen unterschieden:

Stufe 1	Qualitätssicherung als Vorstufe zur Eskalation
Stufe 2	Standard-Eskalation
Stufe 3	Krisen-Eskalation

- Die Qualitätssicherung sichert die Systemdaten und beschreibt die zur Klassifizierung und Bearbeitung nötigen Informationen für eintretende Sicherheitsvorfälle.

- Die Standard-Eskalation beschreibt die Vorgehensweise bei absehbaren bzw. eingetretenen Abweichungen der Standardnutzung.
- Die Krisen-Eskalation ist eine weitere Aktionsstufe innerhalb der Eskalationsprozedur, die bei Störungen mit hohem Schaden und hoher Tragweite zur Anwendung kommt, sofern die Möglichkeiten der Standard-Eskalation für diese spezielle Situation nicht ausreichend sind.

Eine amtsinterne Eskalationsstrategie für Sicherheitsvorfälle ist einzurichten.

Grundlage: BSI Grundschutzkatalog Notfallvorsorge (M 6.61)

Eskalationsstrategie für Sicherheitsvorfälle

2.4.3 Konsequenzen bei Verstößen

Verstöße gegen diese Leitlinie und Richtlinien müssen aufgrund gesetzlicher Regelungen der zuständigen Aufsichtsbehörde weitergeleitet werden. Die Deutsche Rentenversicherung behält sich in Zusammenarbeit mit dem Landesdatenschutzbeauftragten vor, den Zugang zum Verfahren zu sperren.

2.4.4 Reaktion auf Störungen oder Alarmierungen

Bei Missbrauch bzw. Schadensverdacht sind die im Alarmierungsplan (Kapitel 4) festgelegten Schritte einzuhalten.

- Grundsätzlich ist die Hotline der Deutschen Rentenversicherung zu informieren.
- Bei vorsätzlichem oder fahrlässigem Verstoß gegen diese Leitlinie und die Richtlinien durch die Nutzer sind die gleichen Maßnahmen zu treffen, wie bei Missachtung von Organisationsanweisungen. Nach Prüfung durch die IT-Sicherheit und den Datenschutzbeauftragten der Deutschen Rentenversicherung sind in Abhängigkeit von der Schwere des Verstoßes die Aufsichtsbehörden der abrufberechtigten Stellen zu informieren.
- Es muss untersucht werden, wie und wo die Verletzung dieser Leit- und Richtlinien entstanden ist.
- Anschließend müssen die angemessenen schadensbehebenden der -mindernden Maßnahmen durchgeführt werden. Soweit erforderlich, müssen zusätzliche schadensvorbeugende Maßnahmen ergriffen werden. Die durchzuführenden Aktionen hängen von der Schwere des Verstoßes ab.
- Es muss geregelt sein, wer für Kontakte mit der Deutschen Rentenversicherung und anderen Behörden (z.B. Aufsichtsbehörde) verantwortlich ist, um Informationen über bekannte Sicherheitslücken einzuholen oder um Informationen über

aufgetretene Sicherheitslücken weiterzugeben. Es muss dafür Sorge getragen werden, dass evtl. mitbetroffene Stellen schnellstens informiert werden.

- Die Verantwortlichkeiten und Maßnahmen bei Sicherheitsvorfällen sind im Alarmierungsplan beschrieben.

Nach einem eingetretenen Sicherheitsvorfall ab Eskalationsstufe 2 soll der IT-Sicherheitskoordinator die Durchführung der Maßnahmen einer abschließenden Bewertung unterziehen und die Ergebnisse dieser Bewertung allen beteiligten Stellen mitteilen.

Grundlage: BSI Grundschutzkatalog Notfallvorsorge (M 6.58 – M 6.65)

Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen

Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen

Festlegung von Meldewegen für Sicherheitsvorfälle

Eskalationsstrategie für Sicherheitsvorfälle

Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen

Untersuchung und Bewertung eines Sicherheitsvorfalls

Behebung von Sicherheitsvorfällen

Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen

2.4.5 Evaluierung der Eskalationsstrategie

Nach einem eingetretenen Sicherheitsvorfall ist die Durchführung der Maßnahmen von der betroffenen Gemeindebehörde bzw. des Versicherungsamtes zu auditieren und einer abschließenden Bewertung zu unterziehen. Die Ergebnisse dieser Bewertung sind der Deutschen Rentenversicherung mitzuteilen, um eine transparente Optimierung der Sicherheitsmechanismen in Absprache mit dem betroffenen Gemeinde- bzw. Versicherungsamt zu ermöglichen.

Grundlage: BSI Grundschutzkatalog Notfallvorsorge (M 6.66)

Nachbereitung von Sicherheitsvorfällen

2.5 Wartungs- und Reparaturarbeiten

Grundlage: BSI Grundschutzkatalog Organisation (M 2.4)

Regelungen für Wartungs- und Reparaturarbeiten

2.5.1 Interne Wartungs- und Reparaturarbeiten

Um nichtautorisierte Handlungen zu vermeiden, müssen Wartungs- und Reparaturarbeiten, insbesondere wenn sie durch externe Firmen durchgeführt werden, durch eine fachkundige Kraft beaufsichtigt werden.

Als Maßnahmen vor und nach Wartungs- und Reparaturarbeiten sind einzuplanen:

- Ankündigung der Maßnahme gegenüber den betroffenen Mitarbeitern.
- Wartungstechniker müssen sich auf Verlangen ausweisen.
- Der Zugriff auf Daten durch den Wartungstechniker ist soweit wie möglich zu vermeiden.
- Die dem Wartungstechniker eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach Abschluss der Arbeiten zu widerrufen bzw. zu löschen.
- Nach der Durchführung von Wartungs- oder Reparaturarbeiten sind - je nach "Eindringtiefe" des Wartungspersonals - Passwortänderungen z.B. beim Betriebssystem erforderlich.
- Die durchgeführten Wartungsarbeiten sind zu dokumentieren (Umfang, Ergebnisse, Zeitpunkt, Name des Wartungstechnikers).
- Bei Fernwartung ist sicherzustellen, dass kein Zugriff auf verfahrensbezogene Daten möglich ist.

2.5.2 Externe Wartungs- und Reparaturarbeiten

Bei Wartungen oder Reparaturen, die außer Haus durchgeführt werden müssen, ist das Programm „eAntrag“ und die zugehörigen Datenbestände auf dem betroffenen System vorher sicher zu löschen.

2.5.3 Ordnungsgemäße Entsorgung von Betriebsmitteln

Werden Betriebsmittel gewechselt, ist für die sichere Löschung der Daten zu sorgen.

Ist dieses nicht möglich, so ist der Datenträger mechanisch zu zerstören. Erst danach darf der Datenträger entsorgt werden.

Beim Entsorgen von gedruckten Materialien, wie z.B. Formulare oder Unterschriftenblatt, ist darauf zu achten, dass keine Rückschlüsse auf vorher gespeicherte Daten möglich sind.

3 Alarmierungsplan bei Sicherheitsvorfällen

Nach Eingang einer Meldung über eine sicherheitsrelevante Unregelmäßigkeit muss zunächst entschieden werden, ob es sich um ein lokales Sicherheitsproblem oder um einen Sicherheitsvorfall mit ggf. zu erwartenden größeren Schäden handelt.

Verantwortlichkeiten

Der IT-Sicherheitskoordinator ist aus Sicht der Deutschen Rentenversicherung der Notfall-Verantwortliche. Er ist für die Bewertung von Sicherheitsvorfällen (Eskalationsstufen) und rechtzeitige Einleitung von Notfallmaßnahmen zuständig. Er sollte eine erste Einschätzung der möglichen Schadenshöhe, der Folgeschäden, der potentiell intern und extern Betroffenen und möglicher Konsequenzen abgeben. Weitere Ansprechpartner sind der Behördenleiter und der Datenschutzbeauftragte.

Eskalationsstufen

Die Eskalationsstufen beschreiben ein hierarchisches Modell zur Behandlung von Sicherheitsvorfällen, bei dem jede höhere Stufe die Maßnahmen der darunter liegenden beinhaltet.

Stufe 1

Was kennzeichnet Sicherheitsstufe 1:

z.B.:

- gehäufte Probleme bei der Benutzeranmeldung
- gehäufte Probleme beim Versenden und Empfangen der Datensätze
- gehäufte Probleme bei der Installation
- gehäufte Probleme beim Anlegen/Sperren von Nutzern
- gehäufte Probleme bei der Vergabe von Zertifikaten
- Verlust von Daten
- Auftreten von Malware

Maßnahmen:

- Mitarbeiter meldet den Vorfall dem IT-Sicherheitskoordinator
- IT-Sicherheitskoordinator sorgt für die Qualitätssicherung
- IT-Sicherheitskoordinator informiert die Hotline der Versicherungsträger

- Innerhalb von 2 Werktagen erhält die betroffene Gemeindebehörde bzw. das Versicherungsamt durch die Deutsche Rentenversicherung eine Erklärung zum weiteren Vorgehen

Stufe 2

Zusätzlich zu den in Stufe 1 beschriebenen Sachverhalten kennzeichnet Sicherheitsstufe 2:

z.B.:

- Verdacht auf Missbrauch von Daten
- Verdacht auf unautorisierte Änderung von Daten
- Verdacht auf unerlaubte Änderung am Programm (Code und Konfiguration)
- Datensätze, die nicht mehr zugreifbar sind (z.B. durch Datenmanipulation)
- Fehlermeldungen des Systems, die auf einen Missbrauch hindeuten
- massenhaftes Auftreten von Malware

Maßnahmen:

- Mitarbeiter meldet den Vorfall dem IT-Sicherheitskoordinator
- IT-Sicherheitskoordinator veranlasst Sperrung aller Zugriffsberechtigungen zum Programm „eAntrag“ sowie zu den entsprechenden Verzeichnissen und informiert den Behördenleiter
- IT-Sicherheitskoordinator informiert die Hotline der Rentenversicherungsträger
- Die Unterstützung der Deutschen Rentenversicherung bei der Aufklärung des Sicherheitsvorfalls wird durch die lokal Verantwortlichen sichergestellt. (Dokumentation, Sicherung von Beweismitteln, Erreichbarkeit der Verantwortlichen)
- Der zuständige Träger der Deutschen Rentenversicherung definiert die Voraussetzungen für einen Wiederanlauf
- Innerhalb von einem Werktag erhält die betroffene Gemeindebehörde bzw. das Versicherungsamt durch die Deutsche Rentenversicherung eine Erklärung zum weiteren Vorgehen.

Stufe 3

Zusätzlich zu den in Stufe 1 und 2 beschriebenen Sachverhalten kennzeichnet Sicherheitsstufe 3:

z.B.:

- vorsätzlicher Missbrauch der Anwendung (z.B. Screenshots)
- Abruf von Daten, die nicht für den Geschäftsablauf notwendig sind (Abruf zusätzlicher Versicherungskonten)
- unerlaubte Weitergabe von Daten
- unautorisierte Änderung von Daten
- unerlaubte Änderung am Programm (Code und Konfiguration)

Maßnahmen:

- IT-Sicherheitskoordinator informiert umgehend die Hotline der Rentenversicherungsträger und den Behördenleiter
- Innerhalb von einem Werktag erhält die betroffene Gemeindebehörde bzw. das Versicherungsamt durch die Deutsche Rentenversicherung eine Erklärung zum weiteren Vorgehen
- Prüfung durch den zuständigen Datenschutzbeauftragten des Versicherungsamtes
- Information der Aufsichtsbehörden der Versicherungsämter

4 Erforderliche Sicherheitsmaßnahmen für Hardware und Betriebssysteme

Im Folgenden sind die Maßnahmen zusammengestellt, für die bislang keine unmittelbaren Handlungsanweisungen im vorliegenden Dokument abgeleitet wurden, deren Beachtung und Umsetzung seitens der Gemeindebehörde und des Versicherungsamtes aber wiederum der Erhaltung eines hohen Sicherheitsstandards beim Betrieb der Anwendung „eAntrag“ dient.

Dabei wurden im Abschnitt 4.1 „Generelle Maßnahmen für obligatorische IT-Komponenten und Ressourcen“ beschrieben, die auf jeden Fall realisiert sein müssen, damit eAntrag/Expertenversion eingesetzt werden kann.

Im Abschnitt 4.2 „Erweiterte Maßnahmen zu Hard- und Software“ wurden zusätzlich zu den generellen Maßnahmen Bausteine aufgeführt, die auf der Grundlage der Infrastruktur in der jeweiligen Gemeindebehörde bzw. des Versicherungsamtes hinsichtlich der aufgeführten Maßnahmen zu überprüfen und gegebenenfalls anzuwenden, sind.

Weiterhin wurden im Abschnitt 4.3 „Empfohlene Maßnahmen zum IT-Sicherheitsmanagement“ beschrieben, die grundsätzlich für den Einsatz des Verfahrens eAntrag/Expertenversion empfohlen werden.

4.1 Generelle Maßnahmen für obligatorische IT-Komponenten und Ressourcen

Unabhängig von der eingesetzten Hard- und Software sind mindestens diese Maßnahmen für jede Gemeindebehörde und jedes Versicherungsamt zutreffend. Dabei sind nur die wichtigsten einschlägigen Maßnahmen benannt. Einen vollständigen und aktuellen Überblick über die Maßnahmen sowie umfangreiche Erläuterungen zu deren Anwendung erhält man im Internetangebot des Bundesamtes für Sicherheit in der Informationstechnik unter der Rubrik „IT-Grundschutz/IT-Grundschutz-Kataloge“ (Link siehe Glossar).

Baustein B 1.13 Sensibilisierung und Schulung zur Informationssicherheit

Umsetzung

M 3.46	Ansprechpartner zu Sicherheitsfragen
--------	--------------------------------------

Betrieb

M 2.198	Sensibilisierung der Mitarbeiter für Informationssicherheit
---------	---

Baustein B 1.14 Patch- und Änderungsmanagement

Planung und Konzeption

M 2.423	Festlegung der Verantwortlichkeiten für das Patch- und Änderungsmanagement
---------	--

Betrieb

M 4.78	Sorgfältige Durchführung von Konfigurationsänderungen
M 4.177	Sicherstellung der Integrität und Authentizität von Softwarepaketen
M 4.324	Konfiguration von Autoupdate-Mechanismen beim Patch- und Änderungsmanagement

Baustein B 1.4 Datensicherungskonzept

Planung und Konzeption

M 6.33	Entwicklung eines Datensicherungskonzepts
--------	---

Umsetzung

M 6.37	Dokumentation der Datensicherung
--------	----------------------------------

Betrieb

M 6.20	Geeignete Aufbewahrung der Backup-Datenträger
--------	---

Notfallvorsorge

M 6.32	Regelmäßige Datensicherung
--------	----------------------------

Baustein B 1.6 Schutz vor Schadprogrammen

Planung und Konzeption

M 2.154	Erstellung eines Sicherheitskonzeptes gegen Schadprogramme
---------	--

M. 2.160	Regelungen zum Schutz vor Schadprogrammen
----------	---

Beschaffung

M 2.157	Auswahl eines geeigneten Viren-Schutzprogramms
---------	--

Umsetzung

M 4.84	Nutzung der BIOS-Sicherheitsmechanismen
--------	---

Betrieb

M 2.159	Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen
---------	--

Baustein B 1.6 Schutz vor Schadprogrammen	
--	--

M 2.224	Vorbeugung gegen Schadprogramme
---------	---------------------------------

M 4.3	Einsatz von Viren-Schutzprogrammen
-------	------------------------------------

Notfallvorsorge

M 6.23	Verhaltensregeln bei Auftreten von Schadprogrammen
--------	--

M 6.24	Erstellen eines Notfall-Bootmediums
--------	-------------------------------------

Notfallvorsorge

M 6.32	Regelmäßige Datensicherung
--------	----------------------------

Baustein B 2.3 Büroraum / Lokaler Arbeitsplatz

Planung und Konzeption

M 3.9	Ergonomischer Arbeitsplatz
-------	----------------------------

Umsetzung

M 2.17	Zutrittsregelung und -kontrolle
--------	---------------------------------

Betrieb

M 1.15	Geschlossene Fenster und Türen
--------	--------------------------------

M 1.23	Abgeschlossene Türen
--------	----------------------

M 1.45	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
--------	--

M 1.46	Einsatz von Diebstahl-Sicherungen
--------	-----------------------------------

Baustein B 3.201 Allgemeiner Client

Betrieb

M 2.273	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
M 3.18	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
M 4.2	Bildschirm Sperre
M 4.3	Einsatz von Viren-Schutzprogrammen
M 4.4	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
M 4.200	Umgang mit USB-Speichermedien
M 4.238	Einsatz eines lokalen Paketfilters
M 4.241	Sicherer Betrieb von Clients
M 4.242	Einrichten einer Referenzinstallation für Clients
M 5.45	Sichere Nutzung von Browsern

Baustein B 3.208 Internet-PC

Planung und Konzeption

M 2.234	Konzeption eines Internet-PCs
M 2.235	Richtlinien für die Nutzung von Internet-PCs
M 4.41	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
M 5.66	Clientseitige Verwendung von TLS/SSL
M 5.92	Sichere Internet-Anbindung von Internet-PCs

Umsetzung

M 4.151	Sichere Installation von Internet-PCs
M 5.91	Einsatz von Personal Firewalls für Clients
M 5.98	Schutz vor Missbrauch kostenpflichtiger Einwahlnummern

Betrieb

M 2.313	Sichere Anmeldung bei Internet-Diensten
M 4.3	Einsatz von Viren-Schutzprogrammen
M 4.152	Sicherer Betrieb von Internet-PCs
M 5.59	Schutz vor DNS-Spoofing bei Authentisierungsmechanismen
M 5.69	Schutz vor aktiven Inhalten
M 5.93	Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs
M 5.94	Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs
M 5.95	Sicherer E-Commerce bei der Nutzung von Internet-PCs
M 5.96	Sichere Nutzung von Webmail

Notfallvorsorge

M 6.79	Datensicherung beim Einsatz von Internet-PCs
--------	--

Baustein B 3.301 Sicherheitgateway (Firewall)

Betrieb

M 2.78	Sicherer Betrieb eines Sicherheitgateways
M 5.39	Sicherer Einsatz der Protokolle und Dienste

Baustein B 3.406 Drucker, Kopierer und Multifunktionsgeräte

Planung und Konzeption

M 2.397	Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten
M 2.398	Benutzerrichtlinien für den Umgang von Druckern, Kopierern und Multifunktionsgeräten

Beschaffung

M 2.399	Kriterien für die Beschaffung und geeignete Auswahl von Druckern, Kopierern und Multifunktionsgeräten
---------	---

Umsetzung

M 1.32	Geeignete Aufstellung von Druckern und Kopierern
M 4.299	Authentisierung bei Druckern, Kopierern und Multifunktionsgeräten
M 4.300	Informationsschutz bei Druckern, Kopierern und Multifunktionsgeräten
M 4.301	Beschränkung der Zugriffe auf Drucker, Kopierer und Multifunktionsgeräte

Betrieb

M 2.52	Versorgung und Kontrolle der Verbrauchsgüter
M 4.302	Protokollierung bei Druckern, Kopierern und Multifunktionsgeräten
M 4.303	Einsatz von netzfähigen Dokumentenscannern
M 4.304	Verwaltung von Druckern
M 5.146	Netztrennung beim Einsatz von Multifunktionsgeräten

Aussonderung

M 2.13	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
M 2.400	Sichere Außerbetriebnahme von Druckern, Kopierern und Multifunktionsgeräten

Notfallvorsorge

M 6.105	Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten
---------	---

Baustein B 4.2 Netz- und Systemmanagement

Planung und Konzeption

M 2.143	Entwicklung eines Netzmanagementkonzeptes
M 2.144	Verwendung von SNMP als Netzmanagement-Protokoll
M 2.168	IT-System-Analyse vor Einführung eines Systemmanagementsystems
M 2.169	Entwickeln einer Systemmanagementstrategie

Beschaffung

M 2.145	Anforderungen an ein Netzmanagement-Tool
M 2.170	Anforderungen an ein Systemmanagementsystem
M 2.171	Geeignete Auswahl eines Systemmanagement-Produktes

Umsetzung

M 4.91	Sichere Installation eines Systemmanagementsystems
--------	--

Betrieb

M 2.146	Sicherer Betrieb eines Netzmanagementsystems
M 4.92	Sicherer Betrieb eines Systemmanagementsystems

Notfallvorsorge

M 6.57	Erstellen eines Notfallplans für den Ausfall des Managementsystems
--------	--

4.2 Erweiterte Maßnahmen zu Hard- und Software

Abhängig von der eingesetzten Hard- und Software sind diese Maßnahmen für jede Gemeindebehörde und jedes Versicherungsamt optional. Zusätzlich zu den generellen Maßnahmen sind die nachfolgend aufgeführten Bausteine auf der Grundlage der Infrastruktur in der jeweiligen Gemeindebehörde bzw. des Versicherungsamtes hinsichtlich der aufgeführten Maßnahmen zu überprüfen und gegebenenfalls anzuwenden. Die entsprechenden Maßnahmen sind hier selbst zu ermitteln und gegebenenfalls umzusetzen. Die vollständigen und aktuellen Maßnahmen für den jeweiligen Baustein sowie umfangreiche Erläuterungen zu deren Anwendung erhält man im Internetangebot des Bundesamtes für Sicherheit in der Informationstechnik unter der Rubrik „IT-Grundschutz/IT-Grundschutz-Kataloge“ (Link siehe Glossar).

Bausteine:

- B 3.101 Allgemeiner Server
- B 3.202 Allgemeines nicht vernetztes IT-System
- B 3.302 Router und Switches
- B 3.303 Speicherlösungen / Cloud Storage
- B 4.6 WLAN
- B 4.8 Bluetooth
- B 5.14 Mobile Datenträger
- B 5.3 Groupware

4.3 Empfohlene Maßnahmen zum IT-Sicherheitsmanagement

Aufgaben zum IT-Sicherheitsmanagement, die speziell „eAntrag“ betreffen, werden zentral von der Deutschen Rentenversicherung wahrgenommen. Dennoch werden die Maßnahmen zu diesem Baustein ebenfalls aufgelistet, da sie der Sicherheit der IT-Infrastruktur dienen, im Gegensatz zu den oben genannten Maßnahmen allerdings auf Seiten der Gemeindebehörden bzw. Versicherungsämtern keinen unmittelbaren Einfluss auf die Sicherheit des Verfahrens „eAntrag“ haben.

Baustein B 1.0 Sicherheitsmanagement

Planung und Konzeption

M 2.192	Erstellung einer Leitlinie zur Informationssicherheit
M 2.335	Festlegung der Sicherheitsziele und -strategie
M 2.336	Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene

Umsetzung

M 2.193	Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit
M 2.195	Erstellung eines Sicherheitskonzepts
M 2.197	Integration der Mitarbeiter in den Sicherheitsprozess
M 2.337	Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse
M 2.338	Erstellung von zielgruppengerechten Sicherheitsrichtlinien
M 2.339	Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit
M 2.475	Vertragsgestaltung bei Bestellung eines externen IT-Sicherheitsbeauftragten

Betrieb

M 2.199	Aufrechterhaltung der Informationssicherheit
M 2.200	Management-Berichte zur Informationssicherheit
M 2.201	Dokumentation des Sicherheitsprozesses

5 Verpflichtungserklärung

Deutsche Rentenversicherung _____

Straße, Hausnummer

PLZ, Ort

Verpflichtungserklärung für die Teilnahme am Verfahren „eAntrag“

- § 1 Für die Teilnahme am Verfahren „eAntrag“ mit Datenabruf und Datenübermittlung von der bzw. an die Rentenversicherung ist die Unterzeichnung dieser Erklärung und die Übersendung an die Deutsche Rentenversicherung erforderlich.
- § 2 Die teilnehmende Gemeindebehörde bzw. das teilnehmende Versicherungsamt erklärt, die Leitlinien und Richtlinien gemäß Sicherheitskonzept auf der Grundlage des § 151a SGB VI zur Kenntnis genommen zu haben und in der jeweils gültigen Fassung zu beachten und einzuhalten.
- § 3 Insbesondere wird
- die Einhaltung der in der Leitlinie und Richtlinien beschriebenen Maßnahmen durch die Gemeindebehörde bzw. das Versicherungsamt,
 - die Umsetzung der Maßnahmen nach den IT-Grundschutz-Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die in den Leit- und Richtlinien als „Erforderliche Sicherheitsmaßnahmen für Hardware- und Betriebssysteme“ (Teil 4) festgelegt sind,
 - die Verpflichtung der Mitarbeiter auf die Einhaltung der in den Richtlinien (Teil 2) beschriebenen Maßnahmen,
 - die Beachtung des Alarmierungsplans (Teil 3) im Falle eines Sicherheitsvorfalls,
 - die Beachtung der Installationsanleitung und der entsprechenden Programmhandbücher für das Verfahren „eAntrag“,
- erklärt.

§ 4 Sicherheitsauditing

Die an dem Verfahren teilnehmenden Stellen können einem Sicherheitsauditing durch die zuständigen Aufsichtsbehörden der Gemeindebehörde bzw. des Versicherungsamtes unterzogen werden. In diesem Auditing wird die Einrichtung und Beachtung der für die Teilnahme am Verfahren notwendigen Sicherheitsmaßnahmen überprüft.

§ 5 Änderungen von Namen der am Verfahren beteiligten Personen oder der Adresse der Gemeinde bzw. Abmeldung vom Verfahren müssen der Deutschen Rentenversicherung bzw. dem zuständigen Versicherungsträger unverzüglich mitgeteilt werden.

Mit der Unterzeichnung wird die Kenntnisnahme und das Einverständnis mit dem Vorstehenden erklärt.

Ort, Datum

Name in Klarschrift Unterschrift Behördenleiter/ Stempel

Absender:

Gemeinde

Gemeindeschlüssel

Strasse

Ort

Glossar

BSI Bundesamt für Sicherheit in der Informationstechnik

DRV Deutsche Rentenversicherung

Link zu IT-Grundschutz-Bausteinen und -Maßnahmen im Internetangebot des BSI:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

Deutsche Rentenversicherung Baden-Württemberg
Gartenstr. 105 76135 Karlsruhe

*An die Gemeinden und Städte
zur zukünftigen eAntrag-Nutzung Var. 4*

mit Datenabruf

Karlsruhe, den 27.02.2019

**eAntrag/Expertenversion – Onlineanbindung der kommunalen
Behörden für die Antragsaufnahme im automatisierten
Verfahren in Baden-Württemberg**

Sehr geehrte Damen und Herren,

wir bedanken uns für Ihr Interesse an der Online-Version mit Datenabruf. Bei dieser Variante können die in § 151a SGB VI genannten Daten von der Deutschen Rentenversicherung abgerufen werden. Voraussetzung ist jedoch, dass sich alle Nutzer des Verfahrens aus Sicherheitsgründen mit einer digitalen Signaturkarte authentifizieren müssen. Nach erfolgter Antragsaufnahme werden die Antragsdaten in elektronischer Form an den zuständigen Rentenversicherungsträger weitergeleitet. Das ausgedruckte Unterschriftenblatt ist auf dem Postweg an den zuständigen Rentenversicherungsträger zu senden.

Voraussetzung ist allerdings, dass die im Sicherheitskonzept enthaltenen Leit- und Richtlinien für die Nutzung des Verfahrens eAntrag bei den Gemeindebehörden und Versicherungsämtern in Ihrem Hause umgesetzt sind bzw. werden. Wir haben Ihnen als Anlage ein Exemplar dieser Leitlinie und Richtlinien für das Verfahren Antrag/Expertenversion zu Ihrer Kenntnis sowie eine Teilnahmeerklärung beigelegt. Sollten Sie Interesse an der Online-Variante mit Datenabruf haben, so lassen Sie bitte beide Erklärungen vom Dienststellenleiter unterschreiben. Beides kann uns per Post oder Fax zugestellt werden.

Sofern Sie sich für die Nutzung des Verfahrens in der Online-Anbindung entscheiden sollten, bitten wir Sie, die als Anlage beigelegte Verpflichtungserklärung zu unterzeichnen und mit dem Dienstsiegel in Papierform an uns zurückzusenden. Gleichzeitig bitten wir Sie auch den Verfahrensverantwortlichen und den IT-Sicherheitskoordinator zu benennen.

Sobald die Verpflichtungserklärung schriftlich bei uns vorliegt, werden wir uns hinsichtlich des Termins für die Online-Anbindung mit Ihnen in Verbindung setzen.

Abteilung
Organisation Entwicklung Controlling
Gartenstr. 105 76135 Karlsruhe
Postanschrift 76122 Karlsruhe
www.deutsche-rentenversicherung-bw.de

Ansprechpartner/in
Stephan Kuntz – Gert Hiller
Telefon: 0721/825 – 23322 oder 23321
Telefax: 0721/825 - 9923322
E-Mail: eAntrag-hotline@drv-bw.de
De-Mail: oeco@drv-bw.de-mail.de

Servicezeit:
Mo-Do 08:00 - 16:00 Uhr
Fr 08:00 - 14:00 Uhr

Sofern Sie noch weitere Fragen zu der bevorstehenden Online-Anbindung bzw. zur Umsetzung der Leit- und Richtlinien haben sollten, bitten wir Sie, sich mit uns in Verbindung zu setzen.

Mit freundlichen Grüßen
Im Auftrag

Ihr eAntrag-Team der
Deutschen Rentenversicherung
Baden-Württemberg

Anlage

- Verpflichtungserklärung der Gemeinde / Versicherungsamt
- Registrierungsdaten-Teilnahmeerklärung am Verfahren *rveServices-eAntrag/Expertenversion*
- Leit- und Richtlinien für die Nutzung des Verfahrens

Gemeinde / Stadt:

Straße:

PLZ Gemeinde/Stadt:

Deutsche Rentenversicherung
Baden-Württemberg
Abt. 23 - Organisation Entwicklung Controlling
Team eKommunikation
zu Händen der Herren Kuntz / Hiller

76122 Karlsruhe

Verpflichtungserklärung für die Teilnahme am Verfahren „eAntrag“

- § 1 Für die Teilnahme am Verfahren „eAntrag“ mit Datenabruf und Datenübermittlung von der bzw. an die Rentenversicherung ist die Unterzeichnung dieser Erklärung und die Übersendung an die Deutsche Rentenversicherung erforderlich.
- § 2 Die teilnehmende Gemeindebehörde bzw. das teilnehmende Versicherungsamt erklärt, die Leitlinien und Richtlinien gemäß Sicherheitskonzept auf der Grundlage des § 151a SGB VI zur Kenntnis genommen zu haben und in der jeweils gültigen Fassung zu beachten und einzuhalten.
- § 3 Insbesondere wird
- die Einhaltung der in der Leitlinie und Richtlinien beschriebenen Maßnahmen durch die Gemeindebehörde bzw. das Versicherungsamt,
 - die Umsetzung der Maßnahmen nach den IT-Grundschutz-Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die in den Leit- und Richtlinien als „Erforderliche Sicherheitsmaßnahmen für Hardware- und Betriebssysteme“ (Teil 4) festgelegt sind,
 - die Verpflichtung der Mitarbeiter auf die Einhaltung der in den Richtlinien (Teil 2) beschriebenen Maßnahmen,
 - die Beachtung des Alarmierungsplans (Teil 3) im Falle eines Sicherheitsvorfalls,
 - die Beachtung der Installationsanleitung und der entsprechenden Programmhandbücher für das Verfahren „eAntrag“,
- erklärt.

§ 4 Sicherheitsauditing

Die an dem Verfahren teilnehmenden Stellen können einem Sicherheitsauditing durch die zuständigen Aufsichtsbehörden der Gemeindebehörde bzw. des Versicherungsamtes unterzogen werden. In diesem Auditing wird die Einrichtung und Beachtung der für die Teilnahme am Verfahren notwendigen Sicherheitsmaßnahmen überprüft.

§ 5 Änderungen von Namen der am Verfahren beteiligten Personen oder der Adresse der Gemeinde bzw. Abmeldung vom Verfahren müssen der Deutschen Rentenversicherung bzw. dem zuständigen Versicherungsträger unverzüglich mitgeteilt werden.

Mit der Unterzeichnung wird die Kenntnisnahme und das Einverständnis mit dem Vorstehenden erklärt.

Ort, Datum

Name in Klarschrift

Unterschrift Behördenleiter/ Stempel

Registrierungsdaten eAntrag mit Datenabruf

(bitte senden Sie dieses Formular ausgefüllt an Ihren zuständigen Rentenversicherungsträger)

Zuständiger Rentenversicherungsträger:		Deutsche Rentenversicherung Baden-Württemberg	
Adresse der Gemeindebehörde/des Versicherungsamtes			
Gemeinde / Stadt			
Straße/Postfach			
PLZ/Ort		E-Mail	
IT-Sicherheitskoordinator		Vertreter des IT-Sicherheitskoordinators	
Vorname		Vorname	
Nachname		Nachname	
Tel.		Tel.	
Fax		Fax	
E-Mail		E-Mail	
Verantwortlicher für das Verfahren			
Vorname			
Nachname			
Tel.			
Fax			
E-Mail			

- Die Administration der Benutzerverwaltung für die Variante „mit Datenabruf“ soll von den nachfolgend benannten Personen vorgenommen werden.
- Die bisher gemeldeten Administratoren der Benutzerverwaltung, die für die Nutzung der Variante „ohne Datenabruf“ gemeldet wurden, werden auch die Variante „mit Datenabruf“ verwalten.

Ort/Datum

Unterschrift

Registrierungsformular für Gemeindeadministratoren

Angaben zur kommunalen Behörde	Pflichtfeld	
<i>Gemeindeschlüssel</i>	Ja	
<i>Vollständiger Gemeindename</i>	Ja	
<i>Namenszusatz</i>	Nein	
<i>Straße</i>	Nein	
<i>Hausnummer</i>	Nein	
<i>Postleitzahl</i>	Ja	
<i>Ort</i>	Ja	

Angaben zum Administrator	Pflichtfeld	
<i>Anrede Administrator</i>	Ja	
<i>Titel Administrator</i>	Nein	
<i>Namenszusatz Administrator</i>	Nein	
<i>Name Administrator</i>	Ja	
<i>Vorname Administrator</i>	Ja	
<i>Geburtsdatum Administrator</i>	Ja	
<i>Telefonnummer Administrator</i>	Ja	
<i>Faxnummer Administrator</i>	Ja	
<i>E-Mail Administrator</i>	Ja	

Für jeden Administrator bitte ein gesondertes Formular ausfüllen.

Ort / Datum

Unterschrift