Rahmenbedingung und Mindestanforde-rungen zur IT-Sicherheit

für die Nutzung des Verfahrens eAntrag der Deutschen Rentenversicherung in den Gemeindebehörden und Versicherungsämtern

004.04.00

Autor

Michael Vogel

Deutsche Rentenversicherung Rheinland-Pfalz

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

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

Inhaltsverzeichnis

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, Virenscanner etc.) getroffen werden, die erforderlich sind, um die Einhaltung der datenschutzrechtlichen Vorschriften zu gewährleisten (Artikel 5, 25, 32 DSGVO).

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) 200-2 und 200-3 mit einer entsprechenden Risikoanalyse erstellt und umgesetzt.

Für den sicheren Einsatz des Verfahrens bei Gemeindebehörden und Versicherungsämter sind bestimmte Mindestanforderungen bzw. Rahmenbedingungen erforderlich, die in dem vorliegenden Dokument erfasst wurden. Die verfahrensspezifischen Mindestanforderungen referenzieren auf IT-Grundschutz-Standards des Bundesamtes für Sicherheit in der Informationstechnik. Ferner sind sie Teil der Sicherheitskonzeption des Verfahrens „eAntrag“ und erfüllen somit auch Anforderungen des § 151 a Abs 3 SGB VI für eine sichere 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. Versicherungsämter 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 Bausteine, welche die Gefährdungen und entsprechende Gegenmaßnahmen beim Einsatz solcher Systeme beschreiben. Durch die Deutsche Rentenversicherung sind im Einvernehmen mit dem BSI im Sinne einer erweiterten Risikoanalyse zutreffende Maßnahmen für die Gemeindebehörden bzw. Versicherungsämter - auf der Grundlage der 2. Edition des IT-Grundschutz-Kompendiums - 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 Rahmenbedingung 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 200-1 bis 200-3 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 Handhabe der Daten Genüge getan wird.

1.2 Geltungsbereich

Die vorliegende Rahmenbedingung bzw. Mindestanforderungen 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.
- Gewährleistung der besonderen Sicherheitanforderungen an kritsche Infrastrukturen (§ 8a BSI-Gesetz)

- 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).
- berechtigte 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 Artikel 32 DSGVO (Sicherheit der Verarbeitung) zum Schutz der Sozialdaten zu beachten. Unzulässige Datenerhebung, -verarbeitung und -nutzung führen zu Schadenersatzansprüchen nach Artikel 82 DSGVO. 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. Dies stellt auch keinen Widerspruch zur Kritis-Verordnung da, weil ein Ersatzverfahren (offline-Nutzung) vorhanden ist und die sogenannte Schadschwelle nicht erreicht ist. (vgl. Branchenspezifischer Sicherheitsstandard der Deutschen Rentenversicherung – kurz: B3S, S. 10 ff.).

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 Rahmenbedingung 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 Rahmenbedingung bzw. Mindestanforderungen für die Nutzung des Verfahrens "eAntrag" wurden durch die Deutsche Rentenversicherung in Abstimmung mit dem BSI verabschiedet bzw. geändert und in Kraft gesetzt.[1]

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 Rahmenbedingung bzw. Mindestanforderungen 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 Rahmenbedingung bzw. Mindestanforderungen 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 Rahmenbedingung bzw. Mindestanforderungen und in den erforderlichen Basissicherheitsmaßnahmen beschrieben sind.

[1] § 151a SGB VI

2 Mindestanforderungen

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

Bei den folgenden Maßnahmen wird auf das IT-Grundschutz-Kompendium verwiesen und die jeweiligen Bausteine benannt. Der konkrete Regelungsbedarf ist durch den IT-Sicherheitskoordinator kontextbezogen zu prüfen.

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 ist daher der zentrale Ansprechpartner der Deutschen Rentenversicherung für das Verfahren eAntrag bei der kommunalen Behörde.

Er trägt die Verantwortung für:

- die Umsetzung von Sicherheitsstandards für Installation, Konfiguration, Betrieb und Nutzung des „eAntrag“-Verfahrens,
- die Entgegennahme von Meldungen über Sicherheitsvorfälle,
- die Untersuchung und Bewertung von Sicherheitsvorfällen,
- die Nachbearbeitung des Sicherheitsvorfalls und die Überprüfung der Einhaltung der Sicherheitsvorkehrungen.

Grundlage: IT-Grundschutz-Kompendium Organisation und Personal (ORP.1); Detektion und Reaktion (DER.4)

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: IT-Grundschutz-Kompendium Organisation und Personal (ORP.4)

Vergabe von Zugangsberechtigungen

Vergabe von Zugriffsrechten

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: IT-Grundschutz-Kompendium Organisation und Personal (ORP.4)

Vergabe von Zugangsberechtigungen

Vergabe von Zugriffsrechten

Umgang und Regelungen mit Signaturkarten

Beim Umgang mit Signaturkarten[2] 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 der Zugang gesperrt wird.
- Gefundene Signaturkarten sind umgehend bei dem IT-Sicherheitskoordinator bzw. seinem Vertreter abzugeben.

[2] In der Regel werden evaluierte Signaturkarten eingesetzt.

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: IT-Grundschutz-Kompendium Organisation und Personal (ORP.4)

Vergabe von Zugangsberechtigungen

Vergabe von Zugriffsrechten

2.3 Personal

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 Rahmenbedingung und Mindesanforderungen zur IT-Sicherheit 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: IT-Grundschutz-Kompendium Organisation und Personal, Konzepte und Vorgehensweisen* (ORP.2, CON.5)**

Geregelte Einarbeitung/Einweisung neuer Mitarbeiter

Schulung von Mitarbeitern

Heranführen von Nutzerinnen und Nutzer an die Anwendung

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. § 35 SGB I"Sozialgeheimnis"), Vorschriften und Regelungen zu verpflichten. Die Verpflichtung muss von den Mitarbeitern gegengezeichnet werden.

Grundlage: *IT-Grundschutz-Kompendium Organisation und Personal* (ORP.5)

Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen

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: *IT-Grundschutz-Kompendium Organisation und Personal* (ORP.2)

Vertretungsregelungen

Ausscheiden eines Mitarbeiters

- Beim Ausscheiden eines Mitarbeiters ist der Zugang des Mitarbeiters unverzüglich zu sperren und stillzulegen.
- Beim Ausscheiden eines Mitarbeiters ist zu gewährleisten, dass keine Daten vernichtet oder entwendet werden.

Grundlage: IT-Grundschutz-Kompendium Organisation und Personal (ORP.2)

Geregelte Verfahrensweise beim Weggang von Mitarbeitern

2.4 Behandlung von Sicherheitsvorfällen

Sicherheitsvorfälle

Als IT-Sicherheitsvorfall wird ein Ereignis bezeichnet, das Auswirkungen für die sichere Nutzung der Anwendung nach sich ziehen kann und wird in Kapitel 3 über die Stufen 1-3 näher spezifiziert. Sicherheitsvorfälle werden dem IT-Sicherheitskoordinator gemeldet und bewertet. Auf den Baustein DER.2.1 des IT-Grundschutz-Kompendiums 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: ***IT-Grundschutz-Kompendium Detektion und Reaktion (DER.2.1)***

Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen

Aufbau von Organisationsstrukturen zur Behandlung von Sicherheitsvorfällen

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

Hierbei wird auf Kapitel 3 verwiesen.

- Die Qualitätssicherung sichtet und bewertet 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.
Es wird empfohlen, dass der IT-Sicherheitskoordinator ein Template zur Einstufung von möglichen Sicherheitsvorfällen erstellt.

Grundlage: ***IT-Grundschutz-Kompendium Detektion und Reaktion (DER.2.1)***

Eskalationsstrategie für Sicherheitsvorfälle

Festlegung von Meldewegen für Sicherheitsvorfälle

Konsequenzen bei Verstößen

Verstöße gegen Vorgaben aus diesem Dokument bzw. deren Nichtbeachtung 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.

Reaktion auf Störungen oder Alarmierungen

Jeder Sicherheitsvorfall ist entsprechend zu klassifizieren. 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 Vorgaben aus diesem Dokument 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 der Verstoß entstanden ist.
- Anschließend müssen die angemessenen schadensbehebenden oder - 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: IT-Grundschutz-Kompendium Detektion und Reaktion (DER.2.1)

Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen

Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen

Festlegung von Meldewegen für Sicherheitsvorfälle

Eskalationsstrategie für Sicherheitsvorfälle

Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen

Behebung von Sicherheitsvorfällen

Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen

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: IT-Grundschutz-Kompendium Detektion und Reaktion (DER.2.1)

Nachbereitung von Sicherheitsvorfällen

2.5 Wartungs- und Reparaturarbeiten

Grundlage: IT-Grundschutz-Kompendium Organisation und Personal (ORP.1)

Regelungen für Wartungs- und Reparaturarbeiten

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.

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.

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 Verantwortliche für die Sicherheit des Betriebs des Verfahrens eAntrag. 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.
- Prüfung durch den zuständigen Datenschutzbeauftragten der Gemeindebehörde bzw. des Versicherungsamtes.
- IT-Sicherheitskoordinator informiert umgehend die Hotline des zuständigen Rentenversicherungsträgers.
- Innerhalb von 2 Werktagen erhält die betroffene Gemeindebehörde bzw. das Versicherungsamt durch die Deutsche Rentenversicherung eine Empfehlung 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
- Auftreten von Malware

Maßnahmen:

Zusätzlich zu den in Stufe 1 aufgeführten Maßnahmen:

- IT-Sicherheitskoordinator veranlasst Sperrung aller Zugriffsberechtigungen zum Programm „eAntrag“ sowie zu den entsprechenden Verzeichnissen
- IT-Sicherheitskoordinator informiert umgehend den Behördenleiter
- 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 Empfehlung 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:

Zusätzlich zu den in Stufe 1 und 2 aufgeführten Maßnahmen:

- Information der Aufsichtsbehörden der Gemeindebehörde bzw. des Versicherungsamtes.

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“ 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“ 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 zu betrachten. 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-Kompendium“ (Link siehe Glossar).

Baustein ORP.3: Sensibilisierung und Schulung

Umsetzung

ORP.3.A2	Ansprechpartner zu Sicherheitsfragen

Baustein OPS.1.1.3: Patch- und Änderungsmanagement

Planung und Konzeption

OPS.1.1.3.A2	Festlegung der Verantwortlichkeiten

Betrieb

OPS.1.1.3.A10	Sicherstellung der Integrität und Authentizität von Softwarepaketen
OPS.1.1.3.A3	Konfiguration von Autoupdate-Mechanismen
APP.2.1.A5	Sichere Konfiguration und Konfigurationsänderungen von Verzeichnisdiensten

Baustein CON.3: Datensicherungskonzept

Planung und Konzeption

CON.3.A6	Entwicklung eines Datensicherungskonzepts

Umsetzung

CON.3.A4	Erstellung eines Minimaldatensicherungskonzeptes

Betrieb

CON.3.A12	Geeignete Aufbewahrung der Backup-Datenträger

Business Continuity Management

CON.3.A5	Regelmäßige Datensicherung

Baustein OPS.1.1.4: Schutz vor Schadprogrammen

Planung und Konzeption

OPS.1.1.4.A1	Erstellung eines Konzeptes für den Schutz vor Schadprogrammen
OPS.1.1.4.A7	Sensibilisierung und Verpflichtung der Benutzer

Beschaffung

OPS.1.1.4.A3 OPS.1.1.4.A4 OPS.1.1.4.A8 OPS.1.1.4.A11 OPS.1.1.4.A12	Auswahl eines Viren-Schutzprogramms

Umsetzung

OPS.1.1.4.A2	Nutzung systemspezifischer Schutzmechanismen

Baustein OPS.1.1.4: Schutz vor Schadprogrammen

Betrieb

OPS.1.1.4.A6	Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen
OPS.1.1.4.A7	Sensibilisierung und Verpflichtung der Benutzer
OPS.1.2.3.A4	Schutz vor Schadsoftware
OPS.1.1.4.A4 OPS.1.1.4.A5 SYS.1.1.A9 SYS.2.1.A6 SYS.2.2.2.A3 SYS.3.1.A4	Einsatz von Viren-Schutzprogrammen

Business Continuity Management

OPS.1.1.4.A9	Meldung von Infektionen mit Schadprogrammen
SYS.2.1.A38	Einbindung in die Notfallplanung
CON.3.A5 SYS.1.1.A8 SYS.2.1.A4	Regelmäßige Datensicherung

Baustein INF.7: Büroarbeitsplatz

Planung und Konzeption

INF.7.A5	Ergonomischer Arbeitsplatz

Umsetzung

INF.7.A4 INF.1.A7 INF.2.A6	Zutrittsregelung und -kontrolle

Betrieb

INF.7.A2 INF.1.A6 INF:10.A3	Geschlossene Fenster und Türen
INF.7.A2 INF.1.A11	Abgeschlossene Türen
INF.7.A7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
INF.7.A8 INF.9.A10	Einsatz von Diebstahlsicherungen

Baustein SYS.2.1: Allgemeiner Client

Betrieb

SYS.2.1.A14	Updates und Patches für Firmware, Betriebssystem und Anwendungen
SYS.2.3.A4 SYS.1.5.A1 SYS.1.1.A7 NET.1.2.A5 NET.3.1.A2 NET.3.2.A11 APP.3.1.A6 APP.3.2.A6 APP.3.6.A5	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
SYS.2.1.A22	Abmelden nach Aufgabenerfüllung
SYS.2.1.A5	Bildschirmsperre
SYS.2.1.A6 SYS.2.2.2.A3 SYS.1.1.A9 SYS.3.1.A4 OPS.1.1.4.A4 OPS.1.1.4.A5	Einsatz von Viren-Schutzprogrammen
SYS.2.1.A24 SYS.1.3.A3	Umgang mit Wechseldatenträgern im laufenden System
SYS.2.1.A31 SYS.1.1.A19	Einrichtung lokaler Paketfilter
SYS.2.1.A20	Schutz der Administrationsschnittstellen
SYS.2.1.A40	Betriebsdokumentation
SYS.2.1.A30	Einrichten einer Referenzinstallation für Clients
APP.1.2.A1-A12	Sichere Nutzung von Browsern
SYS.2.1.A18	Nutzung von TLS
SYS.3.1.A3	Einsatz von Personal Firewalls

Baustein SYS.2.1: Allgemeiner Client	
OPS.1.1.5	Protokollierung

Baustein NET.3.2: Firewall

Betrieb

NET.3.2.A11	Einspielen von Updates und Patches
NET.3.2.A6	Schutz der Administrationsschnittstellen
NET.3.2.A20	Absicherung von grundlegenden Internetprotokollen

Baustein NET.1.2: Netzmanagement

Planung und Konzeption

NET.1.2.A1	Planung des Netzmanagements
NET.1.2.A2	Anforderungsspezifikation für das Netzmanagement
NET.1.2.A13	Erstellung eines Netzmanagement-Konzeptes
NET.1.2.A10	Beschränkung der SNMP-Kommunikation
NET.1.2.A12	Ist-Aufnahme und Dokumentation des Netzmanagements

Beschaffung

NET.1.2.A2	Anforderungsspezifikation für das Netzmanagement

Betrieb

NET.1.2.A15	Konzept für den sicheren Betrieb der Netzmanagement-Infrastruktur
NET.1.2.A24	Zentrale Konfigurationsverwaltung für Netzkomponenten
NET.1.2.A6	Regelmäßige Datensicherung

Business Continuity Management

NET.1.2.A27	Einbindung des Netzmanagements in die Notfallplanung
NET.1.2.A38	Festlegung von Notbetriebsformen für die Netzmanagement-Infrastruktur

4.2 Erweiterte Maßnahmen zu Hard- und Software

Abhängig von der eingesetzten Hard- und Software sind nachfolgende Maßnahmen für jede Gemeindebehörde und jedes Versicherungsamt optional. Zusätzlich zu den unter Punkt 4.1 genannten Mindestanforderungen 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. Für eine vollständige Umsetzung ist der IT-Sicherheitskoordinator verantwortlich. Der Sicherheitskoordinator ermittelt selbst entsprechende Maßnahmen, setzt diese gegebenenfalls um und protokolliert dies. Dieser Schritt stellt einen integralen Bestandteil des Sicherheitskonzeptes dar.

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-Kompendium“ (Link siehe Glossar).

Bausteine:

- SYS: IT-Systeme
- NET: Netze und Kommunikation
- INF: Infrastruktur

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 ISMS: Sicherheitsmanagement

Planung und Konzeption

ISMS.1.A3	Erstellung einer Leitlinie zur Informationssicherheit
ISMS.1.A2	Festlegung der Sicherheitsziele und -strategie
ISMS.1.A1	Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene

Umsetzung

ISMS.1.A6	Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit
ISMS.1.A10 ISMS.1.A7	Erstellung eines Sicherheitskonzepts
ISMS.1.A8	Integration der Mitarbeiter in den Sicherheitsprozess
ISMS.1.A9	Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse
ORP.5.A10	Klassifizierung von Informationen (nach Schutzbedarf)
ISMS.1.A16	Erstellung von zielgruppengerechten Sicherheitsrichtlinien
ISMS.1.A15	Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit
ISMS.1.A5	Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten

Betrieb

ISMS.1.A11 ORP.5.A7	Aufrechterhaltung der Informationssicherheit
ISMS.1.A12	Management-Berichte zur Informationssicherheit
ISMS.1.A13	Dokumentation des Sicherheitsprozesses

5 Verpflichtungserklärung

Deutsche Rentenversicherung Auswahl des Trägers

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 Rahmenbedingung bzw. Mindestanforderungen 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 Rahmenbedingung bzw. Mindestanforderungen 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 der Rahmenbedingung bzw. die Mindestanforderungen als „Erforderliche Sicherheitsmaßnahmen für Hardware- und Betriebssysteme“ (Teil 4) festgelegt sind,
- die Verpflichtung der Mitarbeiter auf die Einhaltung der in den Mindestanforderungen (Teil 2) beschriebenen Maßnahmen,
- die Beachtung des Alarmierungsplans (Teil 3) im Falle eines Sicherheitsvorfalls, insbesondere die Einbindung des zuständigen Datenschutzbeauftragten der Gemeindebehörder bzw. des Versicherungsamtes.
- 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/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html