Verfahren „eSolution“

Leit- und Richtlinien

Stand: 24. Oktober 2024

Deutsche Rentenversicherung
Bund

1. Inhaltsverzeichnis

Inhaltsverzeichnis

Präambel

Mit dem Verfahren eSolution wird berechtigten externen Kommunikationspartnern (G2G und G2B) eine Möglichkeit geschaffen online bei der Deutschen Rentenversicherung bestimmte Datenabrufe (Einzelauskünften im Rahmen ihrer Berechtigung) zu tätigen. Das Verfahren eSolution wird über das Internet (https://login.eservice-drv.de/eSolution/) aufgerufen. Für den Aufruf benötigt die externe Stelle ein Zertifikat.

Die Authentifizierung erfolgt über eLogin und die Benutzerverwaltung über NOVA.

Die dabei angestrebten Ziele lassen sich in folgende drei Kategorien klassifizieren:

- Strategieziele
    - Verbesserte Unternehmenskommunikation
    - Erhöhung der Prozess- und Servicequalität
    - Steigerung der Kundenzufriedenheit
    - Kostensenkung (Verwaltungs- und Verfahrenskosten)
- Prozessziele
    - Vermeidung von Medienbrüchen
    - Reduktion manueller Prozesse
    - Verringerung der Prozessdurchlaufzeiten
    - Harmonisierung von Prozessen
    - Schaffung eines zentralen Unternehmenszugangs für Kunden
- Ziele für die Informationstechnologie
    - Automatisierung von Prozessen
    - Verstärkte Nutzung von Standards
    - IT- und Datenkonsolidierung
    - Durchgängige Integration von Anwendungssystemen

Die Einhaltung der Leit- und Richtlinien ist eine Voraussetzung für die Teilnahme am Verfahren „eSolution“ mit Datenabruf von der Deutschen Rentenversicherung und liegt im Verantwortungsbereich der abrufberechtigten Stelle.

Teil 1: Leitlinien

Teil 2: Richtlinien

Anhang: Handlungsanweisung bei Sicherheitsvorfällen.

Im Text wird Personen betreffend nur die männliche Form verwendet. Dies geschieht ausschließlich aus Gründen der leichteren Lesbarkeit.

2. Leitlinie

2.1 Ziel der Leitlinie

Die Leitlinie dient der Realisierung und der Aufrechterhaltung eines hohen Schutzbedarfs im Hinblick auf Authentizität, Integrität und Vertraulichkeit der Daten.

2.2 Geltungsbereich

Der Geltungsbereich dieser Leitlinie erstreckt sich auf sämtliche Daten, Systeme und Netzwerkkomponenten, die im Zusammenhang mit dem Verfahren „eSolution“ stehen.

Diese Leitlinie ist für alle Mitarbeiter der abrufberechtigten Stellen, die die Dienste des Verfahrens „eSolution“ bedienen, benutzen oder damit zu tun haben, bindend.

2.3 Genehmigung und Änderung

Diese Leitlinie zur Sicherheit des Verfahrens „eSolution“ wird durch die Deutsche Rentenversicherung verabschiedet, beziehungsweise geändert und in Kraft gesetzt.

Die Deutsche Rentenversicherung ist für die Definition, Dokumentation, Freigabe und Kontrolle von Sicherheitsstandards für das Verfahren „eSolution“ verantwortlich. Die Leit- und Richtlinie wird spätestens nach drei Jahren überprüft. Bei wesentlichen Änderungen ist die Nutzungsvereinbarung erneut durch die abrufberechtigte Stelle zu unterschreiben.

Der Verfahrensverantwortlicher des Verfahrens „eSolution“ bei der Deutschen Rentenversicherung Bund in Würzburg ist der Ansprechpartner für die abrufberechtigten Stellen.

Alle Vereinbarungen mit den abrufberechtigten Stellen bedürfen der schriftlichen Form.

2.4 Verantwortliche für das Verfahren „eSolution“ bei den abrufberechtigten Stellen

Der Leiter der abrufberechtigten Stelle oder ein von ihm Bevollmächtigter ist der Verfahrensverantwortliche für die Nutzung der Dienste im Verfahren „eSolution“. Er sorgt für die Einhaltung der Sicherheitsvorschriften, die in dieser Leit– und Richtlinie beschrieben sind.

2.5 Verantwortliche für das Verfahren „eSolution“ bei der Deutschen Rentenversicherung

Die Administratoren der abrufberechtigten Stellen werden durch die Hotline der Authentifizierung und der Benutzerverwaltung der Rentenversicherung Bund in Würzburg betreut.

Telefon-Nr.: 0931/ 6002-73500

Fax-Nr.: 0931/ 6002-73203

E-Mail-Adresse: drvlogin@deutsche-rentenversicherung.de

Servicezeiten:

Arbeitstag	Uhrzeit
Montag - Donnerstag	07:00 Uhr - 16:00 Uhr
Freitag	07:00 Uhr - 14:00 Uhr

Bei fachlichen Fragen zur Nutzung des Dienstes eSolution steht Ihnen die Hotline des Verfahrens „eSolution“ der Deutschen Rentenversicherung Bund in Würzburg betreut.

Hotline des Verfahrens „eSolution“

Telefon-Nr.: 0931/ 6002-73102

Fax-Nr.: 030/ 865-7923479

E-Mail-Adresse: eSolution-hotline@drv-bund.de

Servicezeiten:

Arbeitstag	Uhrzeit
Montag - Donnerstag	08:00 Uhr - 15:00 Uhr
Freitag	08:00 Uhr - 12:00 Uhr

3. Richtlinie

In der Richtlinie werden für die abrufberechtigten Stellen Maßnahmen festgelegt, die die Umsetzung der Sicherheit des Verfahrens „eSolution“ gewährleisten.

3.1 Administratoren

Die abrufberechtigten Stellen benennen der Deutschen Rentenversicherung schriftlich mindestens einen Administrator.

Die Administratoren, die mit dem Verfahren „eSolution“ arbeiten, erhalten eine Verfahrensbeschreibung zur Nutzung des Portals. Änderungen in der Person des Administrators und dessen Vertreter sind dem Administrator des Verfahrens „eSolution“ der Deutschen Rentenversicherung durch die abrufberechtigten Stellen schriftlich mitzuteilen.

Der Administrator bei den abrufberechtigten Stellen trägt die Verantwortung für:

- die Umsetzung von Sicherheitsstandards bei der Konfiguration, beim Betrieb und der Nutzung des Verfahrens „eSolution“,
- die autorisierte und rechtzeitige Einleitung von Notfallmaßnahmen (Notfallverantwortlicher) bei Eintreten der im Anhang definierten Sicherheitsvorfälle,
- die Entgegennahme von Meldungen über Sicherheitsvorfälle,
- die Untersuchung und Bewertung von Sicherheitsvorfällen,
- die Nachbearbeitung von Sicherheitsvorfällen und
- die Überprüfung der Einhaltung der Sicherheitsvorkehrungen.

3.2 Benutzer- und Zugangsverwaltung

Die Anmeldung am Verfahren „eSolution“ erfolgt über Benutzerkennung und Passwort (siehe Abschnitt 3.2.1) oder mit qualifizierter elektronischer Signatur (siehe Abschnitt 3.2.2). Dies ermöglicht dem Benutzer den Zugang zum Verfahren „eSolution“ entsprechend der seiner Kennung zugeordneten Rechte und den Zugriff auf die seiner Zugriffsberechtigung unterliegenden Daten. Art oder Umfang der möglichen Dienste oder Daten können von der Verwendung einer Signaturkarte abhängig sein. Der für die Nutzung des Verfahrens verantwortliche Leiter und die Administratoren der abrufberechtigten Stelle regeln die hausinternen Grundsätze bei der Vergabe von Zugriffsrechten. Im Verfahren „eSolution“ ist eine grundsätzliche Rollentrennung von Administrator und Benutzer vorgesehen. Jedem Benutzer ist anhand dieser Rolle ein Benutzerprofil zuzuweisen, das den Umfang definiert, in dem das Verfahren „eSolution“ genutzt werden kann.

Die Benutzer sind unter Hinweis auf die einschlägigen Regelungen der Leit- und Richtlinie über den ordnungsmäßigen Umgang mit der ihnen zur Verfügung gestellten Möglichkeit des Abrufs von Sozialdaten im Verfahren „eSolution“ schriftlich zu belehren und zu verpflichten.

3.2.1 Umgang mit Benutzerkennung/ Passwort

3.2.1.1 Einrichten und Ändern von Benutzerkennungen

- Benutzerkennungen werden maschinell gebildet.
- Benutzer dürfen nur durch den jeweiligen Administrator angelegt werden.
- Wenn ein Mitarbeiter aus der abrufberechtigten Stelle ausscheidet oder nicht mehr am Verfahren „eSolution“ teilnimmt, muss die ihm zugewiesene Benutzerkennung unverzüglich stillgelegt werden.

Aus Revisionsgründen und im Rahmen der Datensicherheit werden die Zugriffe bei der Deutschen Rentenversicherung protokolliert und für 6 Monate gespeichert.

- Um einen Missbrauch zu verhindern, ist die vorübergehende Sperrung der Benutzerkennung bei längerer Abwesenheit der berechtigten Person vorzunehmen.
- Die Vergabe/Änderung/Sperrung einer Benutzerkennung wird maschinell dokumentiert.

3.2.1.2 Umgang und Regelungen mit Passwörtern

Beim Umgang mit Passwörtern ist Folgendes zu beachten:

- Das Passwort darf nicht leicht zu erraten sein.
- Das Passwort muss geheim gehalten werden und darf nur dem Benutzer persönlich bekannt sein. Es ist verboten die Passwörter zu hinterlegen.
- Ein Passwortwechsel ist durchzuführen, wenn das Passwort oder die Kennung unautorisierten Personen bekannt geworden ist.
- Jeder Benutzer muss sich nach der Aufgabenerfüllung am Verfahren „eSolution“ abmelden.
- Jedes Passwort muss bei der ersten Anmeldung geändert werden (Startpasswort).
- Passwörter werden nach drei falschen Eingaben gesperrt. Die Anmeldung wird abgebrochen.
- Um einen Missbrauch durch Unbefugte auszuschließen, ist der Zugang zum PC beim Verlassen des Arbeitsplatzes zu sperren (zum Beispiel durch das Ziehen der Mitarbeiterchipkarte oder Aktivieren des Bildschirmschoners mit Passwortschutz).
- Passwörter sind unbeobachtet einzugeben und dürfen insbesondere nicht auf Funktionstasten hinterlegt werden.
- Fremde Passwörter dürfen nicht ausgeforscht, ausprobiert und benutzt werden.
- Passwörter müssen so komplex wie technisch möglich zusammengesetzt sein (Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen). Dies ist der wesentlichste Schutz vor systematischem Ausspähen.

Folgende Regelungen müssen bei der Passwortvergabe eingehalten werden:

- Die Passwörter müssen zwischen zwölf und zwanzig Zeichen lang sein.
- Grundsätzlich sollten sie nur einmal vergeben werden. Die letzten drei verwendeten Passwörter werden gespeichert (Passworthistorie). Das neue Passwort muss sich von diesen abgelaufenen Passwörtern unterscheiden.
- Passwörter, die leicht zu erraten sind (Trivial-Passwörter), dürfen nicht verwendet werden.
- Passwörter müssen aus mindestens drei Zeichengruppen (Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen) bestehen.

Zu vermeiden sind insbesondere:

- Begriffe wie zum Beispiel „Test”, „Gast” oder „System”,
- Begriffe aus dem Aufgabengebiet,
- Automarken, PKW-Kennzeichen, einfache Ziffern- und Buchstabenkombinationen,
- Zahlen und Daten aus dem Lebensbereich des Benutzers,
- Zeichenkombinationen, die nur unwesentlich von den vorherigen Passwörtern

abweichen,

- Zeichenwiederholungen oder Zeichen, die durch nebeneinander liegende Tasten eingegeben werden.

Auf Antrag eines Berechtigten hebt der zuständige Administrator der abrufberechtigten Stelle die Sperre der Benutzerkennung auf, nachdem er sich von der Identität des Berechtigten überzeugt hat.

3.2.2 Umgang mit Signaturkarten

Beim Umgang mit Signaturkarten ist Folgendes zu beachten:

- Akzeptiert werden nur zertifizierte Signaturkarten.
- Die Beschaffung der Signaturkarten sowie der Kartenleser erfolgt in Zuständigkeit der abrufberechtigten Stellen.
- Die Freischaltung der Karte sowie die Vergabe der PIN erfolgen nur durch den einzelnen Benutzer.
- Die Signaturkarte ist von jedem einzelnen Benutzer sicher zu verwahren.
- Eine Weitergabe an Dritte ist nicht zulässig.

Beim Umgang mit der PIN ist Folgendes zu beachten:

- Die PIN muss mindestens sechsstellig sein.
- Leicht zu erratene PIN wie zum Beispiel das Geburtsdatum, sollten nicht verwendet werden.
- Nach dreimaliger Eingabe der falschen PIN, wird die Signaturkarte unbrauchbar.

3.2.3 Vergabe von Zugriffsrechten

Die Festlegung und Veränderung von Zugriffsrechten ist vom jeweils zuständigen Administrator vorzunehmen.

3.3 Personal

3.3.1 Einarbeitung/Einweisung neuer Mitarbeiter

Neu eingestellte Mitarbeiter müssen vor der Nutzung des Verfahrens „eSolution“ eine Einweisung erhalten.

Im Rahmen der Einweisung neuer Mitarbeiter müssen diese Leit- und Richtlinien bekannt gegeben werden.

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

Bei der Einstellung von Mitarbeitern müssen diese verpflichtet werden, einschlägige Gesetze (zum Beispiel § 5 BDSG "Datengeheimnis"; § 35 SGB I „Sozialgeheimnis“), Vorschriften und interne Regelungen einzuhalten. Damit sollen neue Mitarbeiter mit den bestehenden Vorschriften und Regelungen zur Sicherheit bekannt gemacht und gleichzeitig zu deren Einhaltung angehalten werden.

Der Abruf von Sozialdaten unter Nutzung des Verfahrens „eSolution“ hat sich an den

Grundsätzen der Erforderlichkeit (§ 67a Abs. 1 SGB X) sowie der Datenvermeidung und -sparsamkeit (§ 78b SGB X) zu orientieren.

3.3.3 Vertretungsregelung

Die der Deutschen Rentenversicherung benannten Administratoren und Benutzer der abrufberechtigten Stelle vertreten sich entsprechend ihrer Rollenzuweisung gegenseitig.

Vertretungsregelungen haben den Sinn, für Fälle des Personenausfalls die Fortführung der Aufgabenwahrnehmung zu ermöglichen.

Es muss geregelt sein, wer wen in welchen Angelegenheiten mit welchen Kompetenzen vertritt.

Der Vertreter muss ausreichend geschult sein, damit er die Aufgaben übernehmen kann.

Die Weitergabe von Benutzerkennungen, Signaturkarten und Passwörtern beziehungsweise PIN ist nicht zulässig.

3.3.4 Ausscheiden eines Mitarbeiters

Beim Ausscheiden eines Mitarbeiters ist die Benutzerkennung des Mitarbeiters unverzüglich stillzulegen.

3.4 Behandlung von Sicherheitsvorfällen

3.4.1 Sicherheitsanweisung

Die abrufberechtigten Stellen, die personenbezogene Daten verarbeiten, müssen geeignete und dem aktuellen Stand der Technik entsprechende technische und organisatorische Maßnahmen (zum Beispiel Firewall, Virenscanner etc.) treffen, die erforderlich sind, um die Einhaltung der datenschutzrechtlichen Vorschriften zu gewährleisten (§ 78a SGB X).

Dies sind Maßnahmen zur Datensicherung 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.

3.4.2 Sicherheitsvorfälle

Als Sicherheitsvorfall wird ein Ereignis bezeichnet, das Auswirkungen nach sich ziehen kann, die einen großen Schaden sowohl bezüglich Vertraulichkeit, Integrität und der Authentizität der Daten hervorrufen können. Die Verfügbarkeit hat dabei keine Bedeutung. Auf DER.2.1 des IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wird verwiesen.

Sicherheitsvorfälle werden zum Beispiel erkennbar durch:

- gesperrte Benutzerkennungen ohne erkennbaren Grund

- Fehlermeldungen des Systems, die auf einen Missbrauch hindeuten
- Auftreten von Computer-Viren
- vorsätzlicher Missbrauch der Anwendung
- Abruf von Daten, die nicht für den Geschäftsablauf notwendig sind (Abruf zusätzlicher Versicherungskonten)

3.4.3 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 (siehe Anhang Handlungsanweisung bei Sicherheitsvorfällen).

3.4.4 Konsequenzen bei Verstößen

Verstöße gegen diese Leit- und Richtlinien werden der zuständigen Aufsichtsbehörde gemeldet.

3.4.5 Reaktion auf Störungen oder Alarmierungen

Bei einem Missbrauch beziehungsweise Schadensverdacht sind die in der Handlungsanweisung bei Sicherheitsvorfällen festgelegten Schritte einzuhalten.

Grundsätzlich ist die Hotline der Deutschen Rentenversicherung Bund zu informieren.

Bei vorsätzlichem oder fahrlässigem Verstoß gegen die in diesen Leit- und Richtlinien niedergelegten Grundsätze sind die gleichen Maßnahmen zu treffen, wie bei Missachtung von Organisationsanweisungen. Nach Prüfung durch die IT-Sicherheit und den Datenschutzbeauftragten der Deutschen Rentenversicherung Bund sind in Abhängigkeit von der Schwere des Verstoßes die Aufsichtsbehörden der abrufberechtigten Stellen zu informieren.

Es muss untersucht werden, wie und wo die Verletzung der in diesen Leit- und Richtlinien niedergelegten Grundsätze 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 auf Seiten der abrufberechtigten Stelle für Kontakte mit der Deutschen Rentenversicherung und anderen Behörden (zum Beispiel der zuständigen 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 in der Handlungsanweisung beschrieben.

3.4.6 Evaluierung der Eskalationsstrategie

Nach einem eingetretenen Sicherheitsvorfall ist die Durchführung der Maßnahmen von der abrufberechtigten Stelle zu auditieren und einer abschließenden Bewertung zu unterziehen. Die Ergebnisse dieser Bewertung sind der Hotline der Deutschen Rentenversicherung Bund mitzuteilen, um eine transparente Optimierung der Sicherheitsmechanismen in Absprache mit der abrufberechtigten Stelle zu ermöglichen.

3.5 Wartungs- und Reparaturarbeiten

3.5.1 Interne Wartungs- und Reparaturarbeiten

Um nicht autorisierte Handlungen zu vermeiden, müssen Wartungs- und Reparaturarbeiten, insbesondere wenn sie durch externe Firmen durchgeführt werden, durch fachkundiges Personal 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 den Arbeiten zu widerrufen beziehungsweise zu löschen.
- Nach der Durchführung von Wartungs- oder Reparaturarbeiten sind - je nach "Eindringtiefe" des Wartungspersonals - Passwortänderungen 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.

3.5.2 Externe Wartungs- und Reparaturarbeiten

Bei Wartungen oder Reparaturen, die außer Haus durchgeführt werden müssen, sind Daten, die im Zusammenhang mit der Benutzung des Verfahrens „eSolution“ auf dem Rechner abgelegt wurden, zu löschen. Hierunter sind evtl. anfallende Log-Dateien, temporäre Dateien sowie abgespeicherte Vermerke, die nicht zwangsläufig durch die Anwendung entstehen, aber im Zusammenhang mit der Benutzung der Anwendung stehen, einzuordnen.

3.5.3 Ordnungsgemäße Entsorgung von Betriebsmitteln

Werden Betriebsmittel gewechselt, ist für die unwiederbringliche Löschung der gespeicherten Zertifikate und Daten zu sorgen. Ist dies nicht möglich, so ist der Datenträger mechanisch zu zerstören und anschließend zu entsorgen.

Anhang: Handlungsanweisung bei Sicherheitsvorfällen

Nach Eingang einer Meldung bei dem Administrator der abrufberechtigten Stelle über eine sicherheitsrelevante Unregelmäßigkeit muss dieser entscheiden, ob es sich um ein lokales Sicherheitsproblem oder um einen Sicherheitsvorfall mit ggf. zu erwartenden größeren Schäden handelt.

Verantwortlichkeiten

Der Notfallverantwortliche ist grundsätzlich der Leiter der abrufberechtigten Stelle. Dieser kann die Aufgabe an eine fachlich versierte Person delegieren. Der Notfallverantwortliche 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 die Administratoren und der Datenschutzbeauftragte der abrufberechtigten Stelle.

Eskalationsstufen

Die Eskalationsstufen beschreiben ein hierarchisches Modell zur Behandlung von Sicherheitsvorfällen, bei dem jede höhere Stufe die Maßnahmen der darunter liegenden beinhaltet. Für das Verfahren „eSolution“ 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. Der Administrator der abrufberechtigten Stelle bestimmt die Standards und Vorgehensweise.

Die Standard-Eskalation beschreibt die Vorgehensweise bei absehbaren beziehungsweise eingetretenen Abweichungen der Standardnutzung.

Die Krisen-Eskalation ist eine weitere Aktionsstufe innerhalb der Eskalationsprozedur, die bei Störungen mit hohem Schaden und großer Tragweite zur Anwendung kommt, sofern die Möglichkeiten der Standard-Eskalation für diese spezielle Situation nicht ausreichend sind.

Stufe 1

Die Sicherheitsstufe 1 wird zum Beispiel gekennzeichnet durch:

- gehäufte Probleme bei der Benutzeranmeldung
- gehäufte Probleme beim Senden und Empfangen der Daten
- gehäufte Probleme beim Anlegen/Sperren von Benutzern
- gehäufte Probleme bei der Nutzung von Zertifikaten

Maßnahmen:

- Der Mitarbeiter meldet den Vorfall seinem Administrator.
- Der Administrator meldet den Vorfall dem Notfallverantwortlichen der abrufberechtigten Stelle.
- Der Notfallverantwortliche der abrufberechtigten Stelle sorgt für die Qualitätssicherung.
- Der Notfallverantwortliche der abrufberechtigten Stelle informiert die Hotline der Deutschen Rentenversicherung Bund.
- Innerhalb von zwei Werktagen erhält der Notfallverantwortliche der abrufberechtigten Stelle eine Erklärung zum weiteren Vorgehen von der Hotline der Deutschen Rentenversicherung Bund.

Stufe 2

Die Sicherheitsstufe 2 wird zum Beispiel gekennzeichnet durch:

- Verdacht auf Missbrauch von Daten
- Verlust von Daten
- Verdacht auf unerlaubte Änderung am Programm (Code und Konfiguration)
- Fehlermeldungen des Systems, die auf einen Missbrauch hindeuten
- Auftreten von Computer-Viren

Maßnahmen:

- Der Mitarbeiter meldet den Vorfall seinem Administrator.
- Der Administrator veranlasst die Sperrung der Benutzer für das Verfahren „eSolution“ der abrufberechtigten Stelle und informiert den Notfallverantwortlichen der abrufberechtigten Stelle.
- Der Notfallverantwortliche der abrufberechtigten Stelle informiert die Hotline der Deutschen Rentenversicherung Bund.
- Bei der Aufklärung des Sicherheitsvorfalls wird der Notfallverantwortliche der abrufberechtigten Stelle durch die Deutsche Rentenversicherung unterstützt (Dokumentation, Sicherung von Beweismitteln, Erreichbarkeit der Verantwortlichen).
- Die Deutsche Rentenversicherung definiert die Voraussetzungen für eine erneute Benutzung des Verfahrens „eSolution“.
- Innerhalb von einem Werktag erhält der Notfallverantwortliche der abrufberechtigten Stelle eine Erklärung zum weiteren Vorgehen von der Hotline der Deutschen Rentenversicherung Bund.

Stufe 3

Die Sicherheitsstufe 3 wird zum Beispiel gekennzeichnet durch:

- Abruf von Daten, die nicht für den Geschäftsablauf notwendig sind (Abruf zusätzlicher Versicherungskonten)
- Missbrauch von Daten
- unerlaubte Weitergabe von Daten
- unerlaubte Änderung am Programm (Code und Konfiguration)

Maßnahmen:

- Der Notfallverantwortliche der abrufberechtigten Stelle informiert umgehend die Hotline der Deutschen Rentenversicherung Bund.
- Innerhalb von einem Werktag erhält der Notfallverantwortliche der abrufberechtigten Stelle eine Erklärung zum weiteren Vorgehen von der Hotline der Deutschen Rentenversicherung Bund.
- Es erfolgt eine Prüfung durch den zuständigen Datenschutzbeauftragten der abrufberechtigten Stelle.
- Die abrufberechtigte Stelle informiert ihre Aufsichtsbehörde.

Abkürzungsverzeichnis:

G2G	Government to Government (Behörde zu Behörde)
G2B	Government to Business (Behörde zu Unternehmen)
NOVA	Nutzer – Organisation – Verfahren – Administration
PIN	Persönliche Identifikationsnummer
SGB	Sozialgesetzbuch