Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Sozialversicherungen BSV

Weisungen über die Sicherheit der gemeinsamen Anwendungen (SGA) in den Bereichen AHV/IV/EO/EL/FamZLw/FamZ

Gültig ab 1. Januar 2015

Stand: 1. Januar 2016

318.106.09 d

12.15

Vorwort

Gemäss Artikel 50b Absatz 2 AHVG regelt der Bundesrat den Zugriff auf das zentrale Register der Versicherten und der laufenden Leistungen, insbesondere in Bezug auf die Datensicherheit. Am 4. Juni 2010 beschloss der Bundesrat eine Reihe von Massnahmen für einen sicheren Zugang zum Datennetz des Bundes.

Gemäss Artikel 63 Absatz 3 AHVG sorgt das Bundesamt für Sozialversicherungen (BSV) insbesondere für einen zweckmässigen Einsatz technischer Einrichtungen zur Vernetzung der Durchführungsstellen der ersten Säule und der Familienausgleichskassen mit der Zentralen Ausgleichsstelle (ZAS).

Gemäss Artikel 176 Absatz 4 AHVV regelt das Bundesamt für Sozialversicherungen (BSV) die Zusammenarbeit zwischen den Durchführungsstellen der ersten Säule, der Familienausgleichskassen und der Zentralen Ausgleichsstelle (ZAS).

Darauf gestützt legt die vorliegende Version der vom BSV in Auftrag gegebenen Weisungen die allgemeinen Grundsätze für die Sicherheit der gemeinsamen, allen Durchführungsstellen zur Verfügung stehenden Anwendungen fest.

Die Initialversion der Weisungen fokussiert auf die Sicherheit der Zugriffe auf die gemeinsamen Anwendungen.

Vorwort zum Nachtrag 1, gültig ab 1. Januar 2016

Die Aufgaben der Zentralen Authentisierungsmittelstelle wurden der Zentralen Ausgleichsstelle abgetreten. Die Formulare, die mit den Weisungen SGA zusammenhängen, wurden angepasst und vereinfacht.

Inhaltsverzeichnis

Abkürzungen

AHV	Alters- und Hinterlassenenversicherung
AHVG	Bundesgesetz über die AHV
AHVV	Verordnung über die AHV
BSV	Bundesamt für Sozialversicherungen
DS	Durchführungsstelle
FamZLw	Familienzulagen in der Landwirtschaft
FamZ	Familienzulagen
ISB	Informatiksteuerungsorgan des Bundes
KBI	Koordinations- und Bewilligungsinstanz
RIO	Registration Identification Officer
ZAMS	Zentrale Authentisierungsmittelstelle
ZAS	Zentrale Ausgleichsstelle

Liste der mitgeltenden Dokumente zu diesen Weisungen

[1] Liste der gemeinsamen Anwendungen
[2] Formular „Meldung Vertrauensperson“
[3] Formular „Meldung Registration Identification Officer (RIO) “
[4] Formular „Authentisierungsmittel“
[5] Formular „Antrag KBI“

Die gültigen Listen und Formulare sind auf folgender Webseite zu finden www.bsv.admin.ch (Rubrik Praxis > Vollzug > eGov).

Kapitel I

1. Geltungsbereich und Definitionen

1.1 Geltungsbereich

1101 Gestützt auf Artikel 50b Absatz 2, Artikel 59 Absatz 1 sowie Artikel 63 Absatz 3 des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHVG, SR 831.10), auf Artikel 176 Absatz 4 der Verordnung über die Alters- und Hinterlassenenversicherung (AHVV, SR 831.101) und auf Artikel 66 des Bundesgesetzes über die Invalidenvesicherung (IVG, SR 831.20) sowie auf den Bundesratsbeschluss vom 4. Juni 2010 (Zwei-Faktor-Authentisierung) legen die vorliegenden Weisungen die Rahmenbedingungen fest für die Sicherheit der gemeinsamen Anwendungen in den Bereichen AHV/IV/EO/ EL/ FamZLw/ FamZ.

1102 Gemeinsame Anwendungen stehen allen Durchführungsstellen zur Verfügung. Die Liste der gemeinsamen Anwendungen [1] wird vom BSV publiziert.

1103 Diese Weisungen richten sich nicht an Mitarbeitern/innen des Bundes, die bereits mit einem Zwei-Faktor Authentifizierungsmittel ausgerüstet sind.

1.2 Definitionen

1201 *Zwei-Faktor-Authentisierung für Personen*: besteht einerseits aus einem Zugang über ein technisches Hilfsmittel (Faktor Haben), das den Zugriff auf das Netzwerk des Bundes sicherstellt, und andererseits aus einem Benutzernamen und einem Kennwort (Faktor Wissen), mit dem der Zugriff auf die Anwendungen erfolgt.

1202 *Rechner-Authentisierung:* erfolgt durch Maschinenzertifikate sowie Netzwerkkomponenten welche die Sicherheit des Datenzugriffs erhöht. Die Rechner-Authentisierung erfordert ein sedex-Zertifikat.

1203 *Authentisierungsmittel:* Benutzende erhalten für die Zwei-Faktor-Authentisierung ein Authentisierungsmittel in Form eines physischen Datenträgers. Das ISB definiert das zugelassene Authentisierungsmittel entsprechend der Vertraulichkeitseinstufung der Anwendungsdaten.

1204 *Identifikationsmittel*: Ausweisdokument, welches die zuständige Behörde ausstellt und welches die Identifikation einer Person ermöglicht. Das ISB definiert die zugelassenen Identifikationsmittel.

1205 *Durchführungsstelle(DS)*: Durchführungsstelle von AHV/IV/EO/EL/ FamZLw/FamZ.

1206 *Vertrauensperson:* Rolle, die eine Mitarbeiterin oder ein Mitarbeiter der Durchführungsstelle wahrnimmt. Sie ist Ansprechstelle der Benutzenden einer Durchführungsstelle und leitet deren Anträge (Zugriffe, Mutationen etc.) dem Bewilligungsbüro der gemeinsamen Anwendung weiter.

1207 *Registration Information Officer (RIO):* Rolle, die eine Mitarbeiterin oder ein Mitarbeiter der Durchführungsstelle wahrnimmt. Er ist für die Verwaltung der Authentisierungsmittel zuständig, d.h. für die Bestellung der Authentisierungsmittel bei der Zentralen Authentisierungsmittelstelle und für die Erteilung bzw. Entfernung der Zuweisung eines Authentisierungsmittels zu einem Benutzer.

1208 *Bewilligungsbüro der gemeinsamen Anwendungen*: Verwaltet die Zugriffe auf die gemeinsamen Anwendungen in dessen Zuständigkeitsbereich.

1209 *Zentrale Authentisierungsmittelstelle (ZAMS)*: nimmt die Verwaltung der Authentisierungsanträge und die Zuteilung der RIO vor. Sie organisiert den zentralen Support.

1210 *Koordinations- und Bewilligungsinstanz (KBI)*: löst bzw. regelt die Ausnahmen, Unklarheiten und die nicht definierten Fälle aus diesen Weisungen.

Kapitel II

2. Persönlicher Zugriff

2.1 Grundsatz

2.1.1 Benutzer

2101 Die persönlichen Zugriffe auf die gemeinsamen Anwendungen, welche sich im Bundesnetz befinden, erfolgen über eine Zwei-Faktor-Authentisierung. Die Anwendungen, welche eine Zwei-Faktor-Authentisierung benötigen befinden sich auf der Liste der gemeinsamen Anwendungen [1].

2102 Die Benutzenden fordern über ihre Vertrauensperson den Zugriff auf einzelne gemeinsame Anwendungen an. Sie erhalten über ihre Vertrauensperson einen Benutzernamen und ein Kennwort für den persönlichen Zugriff auf die gemeinsamen Anwendungen.

2103 Nachdem die Benutzenden durch den RIO identifiziert wurden, erhalten sie ihr Authentisierungsmittel.

2.1.2 Vertrauensperson

2111 Jede Durchführungsstelle (DS) bezeichnet im Rahmen der in Artikel 59 Absatz 1 AHVG garantierten Selbstverwaltung mindestens zwei und maximal zehn Vertrauenspersonen pro Bewilligungsbüro. Die Erreichbarkeit der Vertrauensperson muss während der üblichen Bürozeitengewährleistet sein.

2112 Jede Vertrauensperson muss bei einer Durchführungsstelle unter Vertrag stehen. Die Vertrauensperson wird von der DS-Leitung ernannt. Beide Parteien müssen ein für diesen Zweck vorgesehenes Formular unterzeichnen und dem Bewilligungsbüro übermitteln.

2113 Jede Mutation betreffend eine Vertrauensperson ist dem Bewilligungsbüro zu melden.

2.1.3 Registration Identification Officer (RIO)

2121 Jede Durchführungsstelle bezeichnet im Rahmen der in Artikel 59 Absatz 1 AHVG garantierten Selbstverwaltung mindestens zwei und maximal zehn Registration Identification Officers (RIO). Die Erreichbarkeit der RIO während den üblichen Bürozeiten muss gewährleistet sein.

2122 Sind mehrere Durchführungsstellen (DS) der gleichen Leitung unterstellt, kann diese RIO bestimmen, die für alle angegliederten Stellen zuständig sind. Die Gruppierung von Stellen ist der KBI mittels Formular „Antrag KBI“ [5] zu melden.

2123 Jeder/jede RIO muss bei einer Durchführungsstelle(DS) unter Vertrag stehen. Der/die RIO wird von der Leitung der DS identifiziert und ernannt. Beide Parteien müssen ein dafür vorgesehenes Formular „Meldung Registration Identification Officer (RIO)“ [3] unterzeichnen und der ZAMS übermitteln.

2124 Die Durchführungsstelle kann die Verantwortung ihrer RIO auf Drittstellen (z.B. Leistungserbringer) ausdehnen. Die Ausdehnung der Verantwortung muss mittels Formular „Antrag KBI“ [5] bei der KBI beantragt werden.

2125 Jeder Antrag betreffend Zuteilung, Mutation oder Aufhebung der RIO-Rolle ist der ZAMS mittels Formular „Meldung Registration Identification Officer RIO“ [3] zu melden.

2.1.4 Rollenbesetzung

2131 Die Rollen Vertrauensperson und RIO können der gleichen Mitarbeiterin oder dem gleichen Mitarbeiter zugewiesen werden.

2132 Eine Vertrauensperson kann für verschiedene Bewilligungsbüros zuständig sein.

2.2 Identifikationsregeln

2201 Die RIO identifizieren Benutzer, die ihrer Durchführungsstelle oder einer Drittstelle (Rz 2124) angegliedert sind, anhand eines amtlichen, zum Zeitpunkt der Identifikation nicht abgelaufenen Lichtbild-Ausweises, d. h. anhand eines Reisepasses oder einer Identitätskarte. Eine Fotokopie oder eine elektronische Speicherung des Identifizierungs-Dokuments wird aufbewahrt. Diese beinhaltet Vorname, Name, Foto und das Geburtsdatum sowie Ausweis-Nummer und Gültigkeitsdatum des Ausweises. Die Kopie oder die elektronische Speicherung wird bis zur Vernichtung des Personaldossiers aufbewahrt.

2202 Falls ein Benutzer/eine Benutzerin über kein gültiges amtliches Dokument verfügt, handelt es sich um einen Sonderfall, der über ein Ausnahmeverfahren durch die KBI zu genehmigen ist.

2203 Bei jeder Abgabe eines Authentisierungsmittels ist der/die RIO verpflichtet, die Identifikation des Benutzers/der Benutzerin vorzunehmen.

2.3 Aufgaben und Verpflichtungen

2.3.1 Aufgaben und Verpflichtungen der Benutzer

2301 Die Benutzenden aktivieren das persönliche Authentisierungsmittel mit einem Link, den sie zuvor per E-Mail erhalten haben.

2302 Benutzername, Passwort und Authentisierungsmittel sind persönlich und vertraulich.

2303 Das Authentisierungsmittel darf nicht ins Ausland mitgenommen werden.

2.3.2 Aufgaben und Verpflichtungen der Vertrauensperson

2311 Die Vertrauensperson ist als einzige Rolle berechtigt, beim Bewilligungsbüro einen Antrag einzureichen. Sie spezifiziert, welchen Benutzenden welche Zugriffsberechtigungen auf welche gemeinsame Anwendung erteilt werden sollen und informiert den/die RIO über die Zuweisung der Zugriffsrechte.

2312 Der Zugriff wird mit den vom Bewilligungsbüro zur Verfügung gestellten Formularen, beantragt.

2313 Bei einer Neuzuweisung, einem Abgang oder Rollenwechsel eines Benutzers oder einer Benutzerin, muss die Vertrauensperson die vorzunehmende Mutation dem Bewilligungsbüro melden und den RIO innert 15 Tagen über die Mutation informieren.

2.3.3 Aufgaben und Verpflichtungen des/der RIO

2321 Der/die RIO ist verantwortlich für die Identifizierung der Benutzenden, welchen er/sie ein Authentisierungsmittel übergibt und zuweist. Diesbezüglich gelten die Identifikationsregeln (Rz 2201-2203).

2322 Der/die RIO erfasst und speichert die Identifikationsnummer und die Art des Ausweises auf der Verwaltungsplattform für die Authentisierungsmittel.

2323 Der/die RIO (auf Personenebene) eine Liste der zugewiesenen, der inaktiven (d. h. noch nicht zugewiesenen), der deaktivierten, der defekten und der verlorenen Authentisierungsmittel.

2324 Der/die RIO weist den Benutzenden deren Authentisierungsmittel zu.

2325 Der/die RIO nimmt Authentisierungsmittel, die nicht länger einem Benutzer/einer Benutzerin zugewiesen sind, zurück, deaktiviert sie und informiert die Vertrauensperson über die

Rücknahme. Deaktivierte Authentisierungsmittel können erneut zugewiesen werden.

2326 Der/die RIO meldet Verluste oder defekte Authentisierungsmittel der ZAMS mittels Formular „Authentisierungsmittel“ [4].

2327 Der/die RIO sorgt für eine umweltgerechte Entsorgung defekter Authentisierungsmittel innerhalb von 90 Tagen (Batteriesammelstelle).

2328 Weitere Fälle und Ausnahmen werden durch die KBI geregelt.

2329 Der/die RIO bestellt die Authentisierungsmittel mittels Formular „Authentisierungsmittel“ [4] bei der ZAMS.

2330 Der/die RIO bestätigt der ZAMS mittels Formular „Authentisierungsmittel“ [4] den Erhalt der Authentisierungsmittel.

3. Rechner-Authentisierung

3.1 Grundsatz

3101 Der Zugriff eines Rechners auf gemeinsame Anwendungen erfordert keine Zwei-Faktor-Authentisierung.

3102 Zugriffe auf Applikationen erfolgen über das AHV/IV-Netz und folgen den Weisungen über den Anschluss ans Netzwerk (WAN).

3103 Für die Rechner-Authentisierung wird das sedex-Zertifikat verwendet.

Kapitel III

4. Zentrale Stellen

4.1 Bewilligungsbüro der gemeinsamen Anwendung

4.1.1 Grundsatz

4101 Jedes Bewilligungsbüro ist die Kontaktstelle zwischen einer bestimmten gemeinsamen Anwendung und den Vertrauenspersonen.

4102 Es ist die Ansprechstelle der Vertrauenspersonen.

4103 Ein Bewilligungsbüro wird für jede gemeinsame Anwendung gemäss „Liste der gemeinsamen Anwendungen“ [1] durch die zuständige Stelle ernannt und dem KBI gemeldet.

4104 Jedes Bewilligungsbüro stellt die erforderlichen Formulare zur Verfügung. Jede Änderung in der Struktur der Formulare muss dem KBI unterbreitet werden.

4.1.2 Aufgaben und Verpflichtungen

4111 Das Bewilligungsbüro verwaltet Zugriffs- und Benutzerberechtigungen für eine bestimmte gemeinsame Anwendung. Der Antrag wird durch die Vertrauensperson gestellt.

4112 Das Bewilligungsbüro führt ein Inventar der Vertrauenspersonen pro Durchführungsstelle.

4113 Das Bewilligungsbüro stellt eine Supportorganisation sicher, welche vom KBI genehmigt wird.

4.2 Zentrale Authentisierungsmittelstelle (ZAMS)

4.2.1 Grundsatz

4201 Die Zentrale Authentisierungsmittelstelle ist die Koordinationsstelle zwischen den RIO und dem Lieferanten der Authentisierungsmittel.

4.2.2 Aufgaben und Verpflichtungen

4211 Die ZAMS validiert die RIO, indem sie diese in der Verwaltungsplattform für die Authentisierungsmittel innert einem Arbeitstag nach Eintreffen des Formulars aktiviert und deaktiviert.

4212 Die ZAMS stellt sicher, dass die bestellten Authentisierungsmittel den Durchführungsstellen (DS) zugestellt werden.

4213 Die ZAMS führt das Inventar der verteilten Authentisierungsmittel, auf Ebene DS oder Gruppierung von Stellen.

4214 Die ZAMS stellt eine Supportorganisation sicher, welche vom KBI genehmigt wird.

4.3 Koordinations- und Bewilligungsinstanz (KBI)

4.3.1 Grundsatz

4301 Die Funktion Koordinations- und Bewilligungsinstanz (KBI) wird durch das BSV wahrgenommen (egov@bsv.admin.ch).

4302 Die KBI kann Ihre Aufgaben delegieren.

4.3.2 Aufgaben und Verpflichtungen

4311 Die KBI genehmigt die Anträge der Bewilligungsbüros, der Zentralen Authentisierungsmittelstelle (ZAMS) und der Durchführungsstellen gemäss vorliegenden Weisungen.

4312 Die KBI regelt Sonderfälle auf Anfrage.

4313 Die KBI überprüft bei den Durchführungsstellen (DS) mindestens:

- die Anzahl RIO
- die Liste der berechtigten Benutzenden
- die Ausweiskopien der berechtigten Benutzenden
- die Liste der aktiven und inaktiven Authentisierungsmittel.

4314 Die KBI überprüft beim Bewilligungsbüro mindestens:

- die Liste der Vertrauenspersonen
- die Verwaltung der Mutationen der Vertrauenspersonen.

4315 Die KBI überprüft bei der Zentralen Authentisierungsmittelstelle (ZAMS) mindestens:

- die Liste der RIO
- die Verwaltung der Mutationen der RIOs
- das Inventar der Bestellungen der Authentisierungsmittel.

4316 Die KBI kann weitere Aspekte der Überprüfung definieren.

5. Inkrafttreten

5001 Diese Weisungen treten am 1. Januar 2015 in Kraft.