



Bearbeitungsreglement (Auszug)

RESY – Regress-System

Klassifizierung	INTERN
Status	genehmigt zur Nutzung
Projektnummer	22380
Projektleiter	Thomas Lanz
Version	Aus Template V2.1 – Version 1.0
Datum	1.12.2021
Auftraggeberin	Colette Nova
Autor/Autoren	Redguard AG

Änderungskontrolle

Version	Datum	Beschreibung, Bemerkung	Name
0.1	04.05.21	Initialerstellung	C. Liechti
0.2	15.06.21	Version zur Prüfung (Entwurf 1)	C. Liechti
0.3	25.08.21	Geprüft durch P. Beck, F. Stalder, T. Lanz, D. Stuber, A. von Wyl	T. Lanz
0.4	30.08.21	Einarbeitung Befunde	C. Liechti
1.0	01.12.21	Ergänzungen / Schlussarbeiten / Einarbeitung Korrekturen A. von Wyl	P. Beck

Verteiler

Funktion	Name	Departement / Amt
DSBO	Isabelle Rogg	EDI / BSV
ISBO	Stefan Blaser	EDI / BSV
PL	Thomas Lanz	EDI / BSV
GPV	Peter Beck	EDI / BSV

Inhaltsverzeichnis

1	Generelles	4
1.1	Beschreibung	4
1.2	Hilfsmittel.....	4
1.3	Zweck des Dokuments.....	4
1.4	Genehmigung.....	5
2	Bearbeitungsreglement.....	6
2.1	Allgemeines	6
2.1.1	Gesetzliche Grundlagen.....	6
2.1.2	Rechtsgrundlagen der Datensammlung	7
2.1.3	Zweck der Datensammlung.....	7
2.1.4	Inhalt der Datensammlung	7
2.2	Verantwortlichkeiten	8
2.2.1	Verantwortliches Bundesorgan.....	8
2.2.2	Leistungserbringer	9
2.2.3	Kantonale Organe und weitere Partner	10
2.3	Benutzer und Datenzugriff.....	10
2.3.1	Benutzerkreis	10
2.3.2	Zugriffsberechtigungen.....	11
2.3.3	Rollen.....	12
2.3.4	Berechtigungsmatrix	13
2.3.5	Prozess Zugriffsberechtigung.....	14
2.4	Bearbeitung der Personendaten	15
2.4.1	Geschäftsprozesse	15
2.4.2	Eintragung in der Fallverwaltung	15
2.4.3	Datenbekanntgabe.....	15
2.4.4	Kontrolle der erfassten Personendaten	15
2.4.5	Prozesse / Datenverarbeitungsverfahren	16
2.5	Aufbewahrungsdauer, Archivierung und Löschung	16
2.5.1	Aufbewahrungsdauer	16
2.5.2	Archivierung und Löschung.....	16
2.6	Technische und organisatorische Massnahmen	16
2.7	Rechte der betroffenen Personen	17
3	Anhang	19
3.1	Anmeldung Datensammlung.....	19
3.2	Dokumentenverzeichnis	20
3.3	Abkürzungen	21
3.4	Begriffe des Datenschutzes	22

1 Generelles

1.1 Beschreibung

Grundlage des Bearbeitungsreglements - im Rahmen von IKT-Vorhaben der Bundesverwaltung - ist das ISDS-Konzept. Der Inhaber einer automatisierten Datensammlung erstellt ein Bearbeitungsreglement, wenn diese Datensammlung (siehe Art. 21 VDSG):

- besonders schützenswerte Personendaten oder Persönlichkeitsprofile beinhaltet;
- durch mehrere Bundesorgane benutzt wird;
- Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen zugänglich gemacht wird; oder
- mit anderen Datensammlungen verknüpft ist.

Das Bearbeitungsreglement soll für die notwendige Transparenz im Rahmen der Systementwicklung, -adaption wie auch der elektronischen Bearbeitung von Personendaten sorgen. Die erste Version des Bearbeitungsreglements ist zum Ende der HERMES Phase Konzept verfügbar.

Das Bearbeitungsreglement ist regelmässig zu aktualisieren.

1.2 Hilfsmittel

Für die Erarbeitung des Bearbeitungsreglements dienen folgende Hilfsmittel:

Hilfsmittel:

- Dokument des EDÖB „Was muss in einem Bearbeitungsreglement aufgeführt werden?“
- Leitfaden für die Bearbeitung von Personendaten in der Bundesverwaltung, EDÖB, August 2009
- Leitfaden für die Erarbeitung der Rechtsgrundlagen für den Betrieb eines Systems zur automatisierten Bearbeitung von Personendaten, BJ, 16. Dezember 2010
- Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes
- BSI Grundsatzkompodium: Baustein CON.2 Datenschutz
- ISO-Standard ISO/IEC 27002: Informationssicherheit und Datenschutz

1.3 Zweck des Dokuments

Das Bearbeitungsreglement umschreibt insbesondere die interne Organisation des verantwortlichen Bundesorgans sowie das Datenbearbeitungs- und Kontrollverfahren und enthält die Auflistung aller Unterlagen über die Planung, die Realisierung, den Betrieb und die Weiterentwicklung der Datensammlung. Es bezweckt vor allem die Schaffung einer optimalen Transparenz der automatisierten Bearbeitung von Personendaten, um eine fachgemässe Auswertung und Beurteilung allfälliger Datenschutzrisiken zu ermöglichen.

1.4 Genehmigung

Die Unterschriften zur Genehmigung müssen vor der Betriebsaufnahme geleistet werden.

Mit seiner Unterschrift bestätigt der Datenschutzberater das Bearbeitungsreglement geprüft zu haben. Sie oder er haben insbesondere geprüft ob das Dokument vollständig ausgefüllt ist und alle geforderten Massnahmen dokumentiert sind. Sie oder er hat die Angaben kritisch hinterfragt, ob sie konsistent sind und im Kontext der Bearbeitung der Daten stimmen.

Der Auftraggeber und der Inhaber der Datensammlung genehmigen mit ihrer Unterschrift das Bearbeitungsreglement.

Datum / Name / Unterschrift

Datenschutzberaterin BSV

(DSBO):

Isabelle Rogg

Sig. Rogg

.....

Datum / Name / Unterschrift

Inhaber der Datensammlung:

Peter Beck, Leiter Bereich Regress

AHV/IV

Sig. Nova

.....

Datum / Name / Unterschrift

Auftraggeberin:

Colette Nova, Mitglied der Geschäftsleitung, Leiterin AHV, berufliche
Vorsorge und EL (ABEL)

Sig. Beck

.....

2 Bearbeitungsreglement

2.1 Allgemeines

2.1.1 Gesetzliche Grundlagen

Organe des Bundes dürfen Personendaten bearbeiten, wenn dafür eine gesetzliche Grundlage besteht (Art. 17 DSGVO).

Besonders schützenswerte Personendaten sowie Persönlichkeitsprofile dürfen sie nur bearbeiten, wenn ein Gesetz im formellen Sinn es ausdrücklich vorsieht oder wenn ausnahmsweise:

- es für eine in einem Gesetz im formellen Sinn klar umschriebene Aufgabe unentbehrlich ist;
- der Bundesrat es im Einzelfall bewilligt, weil die Rechte der betroffenen Person nicht gefährdet sind; oder
- die betroffene Person im Einzelfall eingewilligt oder ihre Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.

Wird die Bearbeitung von Personendaten durch Vereinbarung (z.B. Outsourcing-Vertrag) oder Gesetz Dritten übertragen, so müssen nach Art. 10a Abs. 1 DSGVO folgende Voraussetzungen erfüllt sein:

- die Daten werden nur so bearbeitet, wie der Auftraggeber (das Amt, die Organisationseinheit) selbst es tun dürfte;
- keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.

Der Auftraggeber (bzw. das verantwortliche Bundesorgan) muss sich insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet (Art. 10a Abs. 2 DSGVO).

Art. 19, Abs. 3 und 3^{bis} DSGVO sehen vor:

Bundesorgane dürfen Personendaten durch ein Abrufverfahren zugänglich machen, wenn dies ausdrücklich vorgesehen ist. Besonders schützenswerte Personendaten sowie Persönlichkeitsprofile dürfen nur durch ein Abrufverfahren zugänglich gemacht werden, wenn ein Gesetz im formellen Sinn es ausdrücklich vorsieht.

Bundesorgane dürfen Personendaten mittels automatisierter Informations- und Kommunikationsdienste jedermann zugänglich machen, wenn eine Rechtsgrundlage die Veröffentlichung dieser Daten vorsieht oder wenn sie gestützt auf Absatz 1 bis Informationen der Öffentlichkeit zugänglich machen. Besteht das öffentliche Interesse an der Zugänglichmachung nicht mehr, so sind die betreffenden Daten wieder aus dem automatisierten Informations- und Kommunikationsdienst zu entfernen.

2.1.2 Rechtsgrundlagen der Datensammlung

Das Bundesamt für Sozialversicherungen (BSV), handelnd durch den Bereich Regress AHV/IV,

gestützt auf

- Art. 72 – 75 des Bundesgesetzes vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG);
- Art. 13 – 17 der Verordnung vom 11. September 2002 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSV);
- Art. 49a Bst. d und Art. 50a Abs. 1 Bst. a des Bundesgesetzes vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung (AHVG);
- Art. 66 und Art. 66a des Bundesgesetzes vom 19. Juni 1959 über die Invalidenversicherung (IVG);
- Art. 11a Abs. 2 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG);
- und auf Art. 21 der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG).

2.1.3 Zweck der Datensammlung

Das Fallverwaltungssystem wird vom BSV und den RD zur Ablage, Verwaltung und Dokumentation der Regressfälle genutzt. Es dient ebenfalls der Berechnung, Dokumentation und Bekanntgabe von Regressforderungen.

2.1.4 Inhalt der Datensammlung

Kategorien von Personendaten

Mit dem Fallverwaltungssystem bearbeitet werden überwiegend personenbezogene Daten wie Name, Adresse, neue Versichertennummer, Suva-Nummer, Geburtsdatum, Familie, Ausbildung, Beruf, Arbeitgeber, Arbeitsort, Einkommen, Vermögen, Unfall (Regress- oder Haftpflichtereignis), Gesundheit, Nationalität, Sprachen und Versicherungen (sog. Falldaten). Zudem werden nicht personenbezogene Daten wie Adressen der Ausgleichskassen, Suva-Agenturen, IV-Stellen und Versicherungsgesellschaften bearbeitet. Diese Aufzählungen entsprechen in der Gesamtheit nahezu sämtlicher Daten der Fallverwaltung, ohne indessen einen Anspruch auf Vollständigkeit zu erheben.

Herkunft der Personendaten

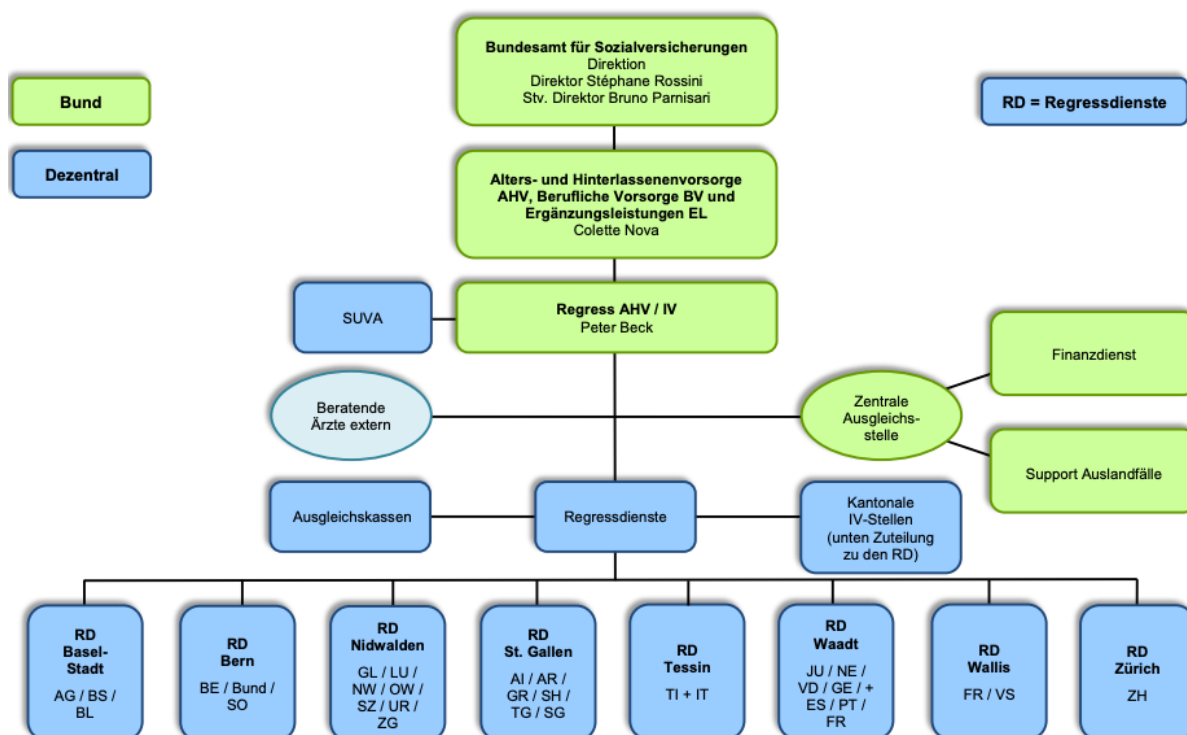
Die Personendaten, die in RESY bearbeitet werden, stammen grundsätzlich von den in einen Regressfall involvierten Partnern (Ausgleichskassen, IV-Stellen, ZAS/UPI, Suva, Haftpflichtversicherer (H3)). Die Daten werden bei der Regressanfrage durch die IV-Stelle oder AK durch einen Sachbearbeiter/Benutzer manuell erfasst oder werden als strukturierte Daten einer sedex Meldung angeliefert und importiert.

2.2 Verantwortlichkeiten

2.2.1 Verantwortliches Bundesorgan

Die Regressansprüche der AHV und IV werden unter Leitung des BSV durch die Regressdienste (RD) der Ausgleichskassen, IV-Stellen oder Sozialversicherungsanstalten geltend gemacht. Das BSV hat folgenden acht kantonalen Regressdiensten diese Aufgabe übertragen:

- Regressdienst Basel
- Regressdienst Bern
- Regressdienst St. Gallen
- Regressdienst Tessin, welcher auch den Auslandregress Italien macht
- Regressdienst Wallis
- Regressdienst Waadt, welcher auch den Auslandregress Frankreich, Spanien und Portugal macht
- Regressdienst Zentralschweiz
- Regressdienst Zürich



27.07.2020 / Mpa

Abbildung 1: Organigramm Regress

Wer	Name
Verantwortliches Bundesorgan	Bundesamt für Sozialversicherungen Bereich Regress Effingerstrasse 20 3003 Bern
Inhaber der Daten	Datenherr: der für die eigenen Fälle verantwortliche Bereich Regress AHV/IV des BSV und der für die eigenen Fälle verantwortliche RD einer AK bzw. IV-Stelle
FAV (Fachwendungsverantwortliche)	Daniela Mettler BSV
ISBD	Philippe Chammartin GS-EDI
ISBO	Stefan Blaser BSV
DSBO	Isabelle Rogg BSV

1. Das BSV ist verantwortliches Bundesorgan und Datenherr der eigenen Dossiers der Fallverwaltung.
2. Der Fachanwendungsverantwortliche (FAV) ist zugleich Benutzeradministrator und sorgt bei den Benutzern für die Einhaltung des Bearbeitungsreglements. Er ist verantwortlich für den täglichen Betrieb und leitet das Change Board, das zuständig ist für die Weiterentwicklung der Fallverwaltung und für die Ausarbeitung der entsprechenden Verträge mit den Leistungserbringern. Dies erfolgt in enger Zusammenarbeit mit dem Technischen Applikationsverantwortlichen (TAV).
3. Der FAV organisiert zudem die Schulungen. Er erstellt die Schulungsunterlagen, die Handbücher und organisiert Grund- und Wiederholungskurse für die zugriffsberechtigten Mitarbeiter des Bundes und der Kantone.
4. Als Benutzer des Fallverwaltungssystem sind die Mitarbeiter des Bereichs Regress AHV/IV dafür verantwortlich, dass die Daten der von ihnen bearbeitenden Fälle richtig und vollständig sind.
5. Der Bereich Recht RE ist zuständig für die materielle Bearbeitung sämtlicher Auskunftsbegehren, die bezogen auf die vom Bund und den Kantonen genutzte Fallverwaltung eingereicht werden.

2.2.2 Leistungserbringer

Wer	Name
Systembetreiber	Systembetrieb BIT, gemäss Marktleistung Cloud-Service-Modell PaaS (Platform as a Service):
Anwendungsbetreiber	Anwendungsbetrieb Corix: <ul style="list-style-type: none"> ▪ Applikation

2.2.3 Kantonale Organe und weitere Partner

Wer	Name
Partner	Partner, welche Informationen an RESY senden oder empfangen, selbst aber keine Anwender sind: <ul style="list-style-type: none"> ▪ Ausgleichskassen ▪ IV-Stellen ▪ ZAS – IVST27 (IV-Stelle für Versicherte im Ausland) ▪ Suva ▪ Haftpflichtversicherer (H3)

1. Die AK bzw. IV-Stelle ist Datenherr der eigenen Dossiers der Fallverwaltung.
2. Jeder RD der AK bzw. der IV-Stelle ist gehalten, einen PowerUser zu ernennen, der vor Ort für das gute Funktionieren der Fallverwaltung zuständig ist. Der PowerUser ist verantwortlich für den Betrieb und die Datensicherheit des Fallverwaltungssystems sowie für die Einhaltung des Bearbeitungsreglements vor Ort. Er ist Kontaktperson zum Applikationsverantwortlichen und meldet diesem technische Probleme, die die Fallverwaltung betreffen.
3. Der PowerUser meldet dem Administrator BSV die Zu- oder Abgänge der Mitarbeiter der RD, damit dieser die Zugriffsberechtigung erteilen, resp. deaktivieren kann.
4. Die Mitarbeiter der RD bearbeiten ihre Fälle und sind verantwortlich dafür, dass die Daten richtig und vollständig sind.

2.3 Benutzer und Datenzugriff

2.3.1 Benutzerkreis

Die Nutzer und Partner rund um die Applikation RESY sind in folgender Abbildung illustriert:

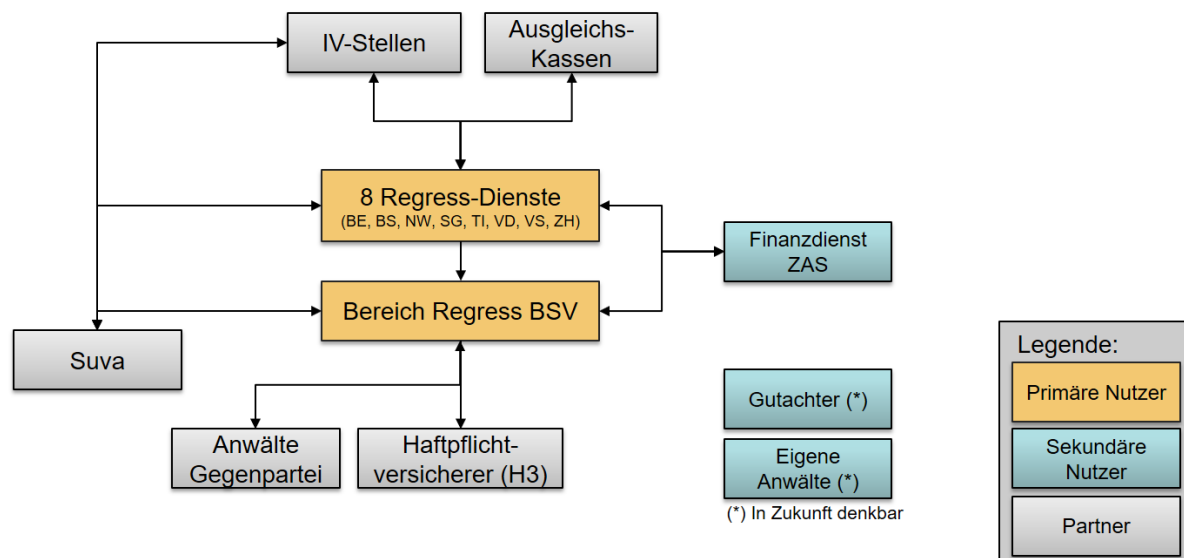


Abbildung 2: Nutzer RESY und Partner in der Regressabwicklung.

Wer	Name
Benutzerkreis	Primäre Nutzer: <ul style="list-style-type: none"> ▪ 8 kantonale/regionale Regressdienste ▪ Bereich Regress BSV Sekundäre Nutzer: <ul style="list-style-type: none"> ▪ Finanzdienst ZAS

Ausschliesslich die primären Nutzer arbeiten direkt mit der Applikation RESY. Alle anderen Nutzer liefern Daten oder erhalten Daten aus der Applikation RESY, ohne direkt darauf Zugriff zu haben. Einzige Ausnahme ist die ZAS welche für einzelne Reports direkt auf RESY Zugriff hat.

1. Die Voraussetzungen für die Erteilung einer Zugriffsberechtigung ist ein Arbeitsverhältnis mit dem BSV oder mit einer AK bzw. IV-Stelle und eine Tätigkeit im Bereich Regress oder im RD.
2. Für die Erteilung der Zugriffsberechtigung werden die vorgeschriebenen Sicherheitsmittel verwendet.

2.3.2 Zugriffsberechtigungen

Als Authentifizierungsmittel wird eine Zwei-Faktor-Authentisierung eingesetzt, die der Sicherheitsstufe «hoch» entspricht, welche für den Zugriff auf Daten mit besonders schützenswerten Personendaten erforderlich ist.

Es gelten nachfolgende Grundsätze:

- Die Benutzer der verschiedenen Kategorien verfügen gemäss Rollenkonzept nur über diejenigen Berechtigungen, die sie tatsächlich benötigen.
- Die mit der Fallverwaltung arbeitenden Organisationseinheiten wie der Bereich Regress AHV/IV des BSV oder der RD einer AK bzw. IV-Stelle können einzig ihre eigenen Daten, die zu einem Fall, resp. zu einem Dossier zusammengefügt sind, lesen, eingeben und bearbeiten.
- Jedes Dossier kann nur einzeln mittels Änderung des Benutzers von einer Organisationseinheit zur anderen transferiert werden. Der Entscheid über den Transfer eines Dossiers fällt der Benutzer der abtretenden Organisationseinheit aufgrund eines schriftlich oder mündlich geäusserten Antrags des Benutzers der übernehmenden Organisationseinheit.

2.3.3 Rollen

Rolle	Beschreibung
Administrator BSV	Im BSV werden mindestens ein Administrator und ein Stellvertreter ernannt. Diese übernehmen spezifische administrative Aufgaben bei der Benutzerverwaltung (u.a. Erteilung von Zugriffsberechtigungen an Benutzer aus BSV und RD) und Stammdatenverwaltung. Sie sind auch die direkte Kontaktperson für fachliche Anliegen der PowerUser der RDs.
Administrator corix	Verantwortlich für Wartung, Support und Weiterentwicklung der Applikation. Er setzt alle Konfigurationsänderungen um, die seitens der Betriebsorganisation mit corix vereinbart werden. Zudem betreibt er gewisse Komponenten der Applikation wie Installierung von Updates der benötigten Software. Zudem Betrieb des 2nd Level und 3rd Level Support.
PowerUser	Jeder RD soll einen PowerUser bestimmen, welcher spezifische, administrative Aufgaben (z.B. Vorlagenbewirtschaftung, Stammdaten Management, etc.) für seinen Mandanten übernimmt. Zudem unterstützt der PowerUser die Anwender seines RD bei der Verwendung der Applikation.
Sachbearbeiter	Der Benutzer des BSV oder eines RD verwendet die Applikation, um Regressfälle zu bearbeiten.
Sachbearbeiter ZAS	Der Benutzer der ZAS verwendet <i>RESY</i> , um bestimmte Daten zu den Regressfällen in das eigene System zu übernehmen. Im Endausbau ist eine Schnittstelle zwischen <i>RESY</i> und der ZAS Finanzapplikation geplant. Diese Rolle hat nur Lese-Zugriff auf alle Fälle (evtl. eingeschränkte Sicht, wie finanzielle Angaben, ohne medizinischen Informationen, etc.).
Leiter Regress	Es muss analysiert werden, ob es für den Leiter Regress spezielle Funktionalitäten gibt, welche die Rollen <i>Benutzer</i> und <i>Leiter RD</i> nicht zur Verfügung hat.

2.3.4 Berechtigungsmatrix

Berechtigungen / Rolle	Bund – BSV			Kanton – RD			Dritte - LE
	Administrator BSV	Leiter Regress	Sachbearbeiter	PowerUser	Sachbearbeiter	ZAS	
Mandant (Regressdienst)	A	A	E	E	E	A	A
Regressfälle	S	S	S	S	S	L	L
Aufgaben	S	S	S	S	S	X	L
Posteingang	S	S	S	S	S	X	L
Partner	S	L	L	L	L	X	L
RD-Verwaltung (inkl. Vorlagen, Kategorien)	S	L	L	S	L	X	
Admin-Verwaltung	S	X	X	X	X	X	S
Textbausteine administrieren	S	X	X	X	X	X	S
Benutzerverwaltung	S	L	X	X	X	X	L

Zugriffsstufen

S: Schreibend, L: Lesend, X: kein Zugriff

Mandant: A: Alle Mandanten, E: Eigener RD

2.3.5 Prozess Zugriffsberechtigung

Die Prozesse «Benutzer anlegen» und «Benutzer deaktivieren» sind detailliert in den Kapiteln 4.3.4 und 4.3.5 im Betriebskonzept dokumentiert.

Beantragung Zugriffsberechtigung

- Die Zugriffsberechtigung zum Fallverwaltungssystem wird jedem Benutzer persönlich erteilt (Zugriffsprofil oder Rolle) und darf nicht an Drittpersonen weitergegeben werden.
- Die Anträge für Zugriffsberechtigungen sind durch den Leiter des Bereichs Regress AHV/IV oder des RD schriftlich an den FAV zu richten.
- Der Benutzer führt einen initialen Login-Versuch durch und vervollständigt seine Angaben und begründet seinen Zugriffswunsch.
- Der FAV prüft die Anträge auf Vollständigkeit und erteilt die Zugriffsberechtigung oder er weist den Antrag ab. In Grenzfällen entscheidet der Leiter des Bereichs Regress AHV/IV.
- Anträge für die individuellen Zugriffsberechtigungen für die an der Entwicklung und am Unterhalt des Fallverwaltungssystems arbeitenden Mitarbeiter der Leistungserbringer werden ebenfalls vom FAV bearbeitet.
- Der FAV erfasst und verwaltet die Zugriffe der verschiedenen Benutzer der Fallverwaltung.

Deaktivierung der Zugriffsberechtigung:

- Der Leiter des Bereichs Regress AHV/IV oder des RD beantragt beim FAV die Entziehung der Zugriffsberechtigung.
- Der FAV deaktiviert die Zugriffsberechtigung auf den durch den Leiter RD definierten Deaktivierungszeitpunkt.
- Missbräuche der Zugriffsberechtigung im Bereich des RD melden der FAV und der entsprechende PowerUser einander gegenseitig. Der FAV kann die betroffene Zugriffsberechtigung deaktivieren. Missbräuche der Zugriffsberechtigung im BSV meldet der FAV dem Leiter Bereich Regress AHV/IV, der über die Deaktivierung der betroffenen Zugriffsberechtigung entscheidet.

2.4 Bearbeitung der Personendaten

2.4.1 Geschäftsprozesse

Der Prozess für die Regressfallbearbeitung ist im Geschäftsorganisationkonzept detailliert beschrieben.

2.4.2 Eintragung in der Fallverwaltung

In Anwendung der Art. 72 – 75 ATSG und Art. 13 – 17 ATSV; Art. 49a Bst. d und Art. 50a Abs. 1 Bst. a AHVG sowie Art. 66 und Art. 66a IVG werden personenbezogene Leistungsdaten der AHV, der IV und weiterer Versicherungen in die Fallverwaltung eingetragen, sofern ein Regressereignis erkannt worden ist und bearbeitet wird. Zur Eintragung der regressrelevanten Daten wird in der Fallverwaltung ein Fall, resp. ein Dossier eröffnet und einem verantwortlichen Benutzer zugewiesen.

2.4.3 Datenbekanntgabe

Bekanntgabe der Daten

Die Bekanntgabe der Daten an die an einem Fall beteiligten Behörden des Bundes und der Kantone, Rechtspflegebehörden, beratenden Ärzte, externe Anwälte und Versicherungen (Privat- oder Sozialversicherungen) richtet sich nach Art. 49a Bst. d und Art. 50a Abs. 1 Bst. a AHVG, Art. 66 und 66a IVG sowie Art. 47 Abs. 1 Bst. d ATSG. Die Daten werden nur insoweit und in dem Umfange bekanntgegeben, wie sie zur Begründung und Durchsetzung einer Regressforderung notwendig sind.

ID	Datenlieferant	Datenempfänger	Zweck der Datenübertragung	Datenart	Periodizität	Medium
	IVS, AK, Suva	BSV und RD (RESY)	Fallbearbeitung	Falldaten	täglich	Sedex Briefpost
	BSV und RD (RESY)	Partner	Fallbearbeitung	Falldaten	täglich	Secure Messaging (HIN) Briefpost
	Register und DWH der ZAS	BSV und RD (Vertigo und Leonardo)	Fallbearbeitung	Falldaten	täglich	Sedex
	Vertigo und Leonardo	Partner	Fallbearbeitung	Falldaten	täglich	Secure Messaging (HIN) Briefpost
	Schadennummerservice Suva	RESY	Schadennummerübertragung	Falldaten	täglich	Server to Server (verschlüsselt)
	Personenregister UPI	RESY	Personendatenübertragung	Falldaten	täglich	Server to Server (verschlüsselt)

2.4.4 Kontrolle der erfassten Personendaten

Das BSV und die RD erfassen die regressrelevanten Daten in den von ihnen geführten Fällen. Der fallführende Benutzer ist dafür verantwortlich, dass die Daten des Falles richtig und vollständig eingetragen sind.

2.4.5 Prozesse / Datenverarbeitungsverfahren

Berichtigung von Daten

Mutationswünsche der Benutzer erfolgen an den FAV und Leiter RD. Änderungen an den Stammdaten erfolgen ebenfalls durch den FAV. Berichtigungen von Personendaten werden durch die Sachbearbeiter bei Bedarf fallbezogen durchgeführt.

Anonymisierung von Daten

Eine Anonymisierung der Daten in der produktiven Umgebung findet nicht statt.

Speicherung von Daten

Die Speicherung der Daten erfolgt in einer Datenbank in der Schweiz beim Bundesamt für Informatik und Telekommunikation BIT.

Aufbewahrung von Daten

Die Aufbewahrungsdauer nach Abschluss eines Regressfalles beträgt 30 Jahre (siehe Kapitel 2.5.1 Aufbewahrungsdauer).

Archivierung und Vernichtung von Daten

(siehe Kapitel 2.5.2 Archivierung und Löschung)

2.5 Aufbewahrungsdauer, Archivierung und Löschung

2.5.1 Aufbewahrungsdauer

Die Aufbewahrungsdauer der Daten richtet sich primär nach der Dauer der Fallbearbeitung. Solange ein Fall nicht abgeschlossen, resp. nicht deaktiviert ist, werden die Daten bearbeitet. Nach Ablauf des Kalenderjahrs, in welchem der Fall abgeschlossen worden ist, werden die Daten für die Bearbeitung gesperrt und bleiben wegen möglichen Rückfällen und Spätfolgen während 30 Jahren in der Fallverwaltung gespeichert.

2.5.2 Archivierung und Löschung

Betreffend Abgabe der Daten an das Bundesarchiv, resp. an die kantonalen Archive, und Vernichtung der Daten massgebend ist die Weisung über die Aktenführung in der AHV/IV/EO/EL/Fazli/FamZ (WAF), gültig ab 1. Januar 2011.

Die Löschung ist zum aktuellen Zeitpunkt noch nicht geregelt.

2.6 Technische und organisatorische Massnahmen

Zugangs- und Datenträgerkontrolle

Unbefugten Personen ist der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren. Unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen.

- Zugang zu den Rechenzentren erhalten nur diejenigen Personen, die diesen Zugang benötigen. Details sind in den Zugangskonzepten der beteiligten Leistungserbringer geregelt.
- Die Datenendgeräte sind in geschützten Zonen platziert. Der Zugang zu den geschützten Zonen ist kontrolliert.
- Die Datenträger der Arbeitsplatzcomputer sind verschlüsselt.
- Ausgedruckte Daten sind so aufzubewahren, dass Drittpersonen (z.B. Reinigungspersonal) sie nicht einsehen und / oder nicht kopieren können. Die Datenausdrucke

werden sofort vernichtet, sobald sie den Zweck ihrer Erstellung erfüllt haben.

Benutzer- und Zugriffskontrolle

Die Benutzung von automatisierten Datenverarbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen ist zu verhindern. Der Zugriff der berechtigten Personen ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen.

- Benutzer, die auf das Regress-System zugreifen, müssen sich mittels starker 2-Faktor-Authentifizierung authentifizieren.
- Der Zugriff auf das Regress-System ist für die Benutzer und Administratoren gemäss den Rollen und Zugriffsberechtigungen (siehe Kapitel 2.3.4 Berechtigungsmatrix) eingeschränkt.

Transportkontrolle

Bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

- Die Datenübertragung innerhalb des Regress-Systems sowie Übermittlungen an Partner erfolgen verschlüsselt.

Datensicherung

- Die Daten der Fallverwaltung werden vom BIT entsprechend den geltenden Weisungen der Bundesverwaltung gesichert. Regelmässig werden Datensicherungen angefertigt und sicher aufbewahrt.
- Die Wiederherstellung der Datenkonsistenz und –Integrität der Fallverwaltung nach einem Datenverlust oder dem Ausfall von Systemkomponenten ist garantiert.

Sensibilisierung und Meldepflicht

Die Benutzer sind über die Sicherheitseinstufung des Fallverwaltungssystems und Vorschriften im Umgang mit dem System und dessen Daten informiert. Mögliche Sanktionen bei vorsätzlichen oder fahrlässigen Verletzungen der Informatiksicherheit sind den Benutzern bekannt. Sämtliche Benutzer sind verpflichtet, folgende Feststellungen dem PowerUser, resp. FAV zu melden:

- a. Fehler in den erfassten Daten, sofern nicht selbst behebbar;
- b. Fehler in den Stammdaten oder deren Strukturen;
- c. beobachtete oder vermutete Schwachstellen bzw. Sicherheitsmängel des Systems;
- d. nicht umgesetzte oder nicht eingehaltene Sicherheitsmassnahmen;
- e. unvorhergesehene Ereignisse, die eine Auswirkung auf die Informatiksicherheit haben könnten.

Aufsicht und Verantwortlichkeit

- Das BSV trägt die Verantwortung für das Fallverwaltungssystem.
- Der FAV kontrolliert die Einhaltung der Informatiksicherheitsregeln des Bundes und die Befolgung der Bestimmungen des vorliegenden Bearbeitungsreglements.

2.7 Rechte der betroffenen Personen

Auskunftserteilung an betroffene Personen

- Jede Person kann beim BSV, Leiter Bereich Regress AHV/IV, Auskunft darüber verlangen, ob und welche Daten im Fallverwaltungssystem über sie bearbeitet werden und verlangen, dass unrichtige Daten berichtigt werden. Das Auskunftsrecht richtet sich nach Art. 8 und 9 DSG; Art. 1 und 2 sowie Art. 13 und 14 VDSG.

- Zur materiellen Bearbeitung der Auskunftsbeglehen ist der Bereich Recht RE zuständig. Dessen Zuständigkeit erstreckt sich auch auf diejenigen Beglehen, die bei den kantonalen Organen eingehen.
- Das Verfahren der Auskunftserteilung läuft analog dem Prozess BG-Gesuch ab. Sämtliche Auskunftsbeglehen werden im GEVER-System des BSV erfasst.

3 Anhang

3.1 Anmeldung Datensammlung

Register Nr.	Bezeichnung und Zweck der Datensammlung
200900069	eRegress: Registrierung und Verwaltung der Regressfälle

Register Nr.:
200900069

Inbetriebnahme der Datensammlung:
2007

Bezeichnung der Datensammlung:
eRegress

Zweck der Datensammlung:
Registrierung und Verwaltung der Regressfälle

Adresse des Inhabers:
Bundesamt für Sozialversicherungen
Effingerstrasse 20
3003 Bern

Rechtsgrundlage:

SR	Name	Art.	Abs. Bst.
830.1	Bundesgesetz vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG)	32, 47,	72ff.

Kategorien der bearbeiteten Personendaten:

- * Adresse
- * AHV - Nummer
- * Arbeitsort
- * Ausbildung
- * Identität
- * Beruf
- * Einkommen
- * Beurteilungen
- * Familie
- * Gesundheit
- * Nationalität / Heimatort
- * Finanzielle Situation
- * Sprachen
- * Vermögen / Kapital
- * Versicherungen
- * Name, Vorname
- * Geschlecht
- * Geburtsdatum

Kategorien der Datenempfänger:

- Kantonale Ausgleichskassen
- * Versicherungen
- Gerichte
- SUVA
- Vertrauensärzte
- Anwälte
- IV-Stellen
- Zentrale Ausgleichsstelle
- Schädiger/Haftpflichtversicherer

Kategorien der Beteiligten:

- Kantonale Ausgleichskassen
- Versicherungen
- Gerichte
- SUVA
- Vertrauensärzte
- Anwälte
- IV-Stellen
- Zentrale Ausgleichsstelle
- Schädiger/Haftpflichtversicherer

* Hauptkategorie

3.2 Dokumentenverzeichnis

Beinhaltet die Auflistung aller für die betreffende Datensammlung relevanten Gesetze, Verordnungen, Weisungen, Regelungen, technischen Spezifikationen, usw. Die Auflistung ist durch die departements- und/oder amtseigenen Dokumente zu ergänzen.

Dokumententyp	Titel
Gesetze	SR 830.1 Bundesgesetz vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) - Art. 32, 47, 72ff.
	SR 831.10 Bundesgesetz über die Alters- und Hinterlassenenversicherung (AHVG) – Art. 49a lit. D, Art. 50 it. a
	SR 831.20 Bundesgesetz über die Invalidenversicherung (IVG) - Art. 66a und b
	Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG; SR 235.1)
	Bundesgesetz vom 17. Dezember 2004 über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ; SR 152.3)
	Bundesgesetz vom 26. Juni 1998 über die Archivierung (Archivierungsgesetz, BGA; SR 152.1)
Verordnungen	SR 120.73 Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV)
	Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG; SR 235.11)
	SR 172.010.58 Verordnung über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung (VDTI)
	Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV; SR 510.411)
	Verordnung vom 3. Juli 2001 über den Schutz von Personaldaten in der Bundesverwaltung (SR 172.220.111.4)
	SR 172.010.442 Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen
Weisungen	Weisungen vom 18. Januar 2008 über die detaillierten Bearbeitungsvorschriften zum Informationsschutz (Bearbeitungsweisungen)
	Weisungen vom 18. Januar 2008 über die Klassifizierung (Klassifizierungskatalog)
Konzepte	Rollenkonzept RESY
	ISDS-Konzept RESY
	Betriebskonzept RESY
	Geschäftsorganisationskonzept RESY

3.3 Abkürzungen

Abkürzung	Bedeutung
Abs.	Absatz
AHV	Alters- und Hinterlassenenversicherung
AK	Kantonale Ausgleichskasse
Art.	Artikel
ATSG	Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts
Bst.	Buchstabe
BSV	Bundesamt für Sozialversicherungen
DSBO	Datenschutzberater in der Organisationseinheit
DSG	Bundesgesetz über den Datenschutz (SR 235.1)
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EL	Ergänzungsleistungen zur AHV und IV
EO	Erwerbsersatzordnung für Dienstleistende und bei Mutterschaft
FAV	Fachanwendungsverantwortlicher
GPV	Geschäftsprozessverantwortlicher
IKT	Informations- und Kommunikationstechnik
ISBO	Informatiksicherheitsbeauftragter der Organisationseinheit
ISBD	Informatiksicherheitsbeauftragter des Departements
ISDS-Konzept	Informationssicherheits- und Datenschutzkonzept
ISDSV	Informationssicherheits- und Datenschutzverantwortlicher
IV	Invalidenversicherung
PL	Projektleiter/-in
RD	Regressdienst einer kantonalen Ausgleichskasse bzw. IV-Stelle
RE	Bereich Recht, Geschäftsfeld Planung, Prozesse und Ressourcen (PPR), BSV
RESY	Regress-System
SV	Systemverantwortlicher/-e
VDSG	Verordnung zum Bundesgesetz über den Datenschutz (SR 235.11)
VE	Verwaltungseinheit
ZAS	Zentrale Ausgleichsstelle, Genf

3.4 Begriffe des Datenschutzes

Begriff	Bedeutung
Bearbeiten	Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten (siehe Art. 3 Bst. e DSGVO).
Bekanntgeben	Das Zugänglichmachen von Personendaten wie das Einsichtgewähren, Weitergeben oder Veröffentlichen (Art. 3 Bst. f DSGVO).
Besonders schützenswerte Personendaten	Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten; über die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit; über Massnahmen der sozialen Hilfe; und über administrative oder strafrechtliche Verfolgungen und Sanktionen (Art. 3 Bst. c DSGVO).
Datensammlung	Im Sinne des Datenschutzgesetzes bedeutet Datensammlung „jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar ist“ (Art. 3 Bst. g DSGVO).
Inhaber der Datensammlung	Inhaberin oder der Inhaber der Datensammlung sind private Personen oder Bundesorgane, die über den Zweck und den Inhalt der Datensammlung entscheiden (Art. 3 Bst. i DSGVO).
Personendaten	Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen; darunter fallen natürliche wie auch juristische Personen (Art. 3 Bst. a und b DSGVO).
Persönlichkeitsprofil	Ein Persönlichkeitsprofil ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt (Art. 3 Bst. d DSGVO).