Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Sozialversicherungen BSV

Weisungen über die Anforderungen an die Informationssicherheit und den Datenschutz der Informationssysteme der Durchführungsstellen der 1. Säule/FamZ (W-ISDS)

Gültig ab 1. Januar 2024

Stand: 12.05.2025

318.108.08 d W-ISDS

01.25

Änderungsverzeichnis

VERSION	DATUM	VERFASSER	BEMERKUNGEN
1.0	01.01.2024	BSV	Publizierte Version
1.1	15.03.2024	Markus Moog (BSV)	Anpassungen Layout/Formatierung
1.2	April 2024	Michael Jeitziner (IG)	Erstellen Änderungsverzeichnis, Mapping Controls auf Standard ISO/IEC 27001:2022, Anpassung Rz 2.8.2
1.3	18.04.2024	Markus Moog (BSV) Michael Jeitziner (IG)	Inhaltsverzeichnis und Registriernummer eingefügt Ergänzung Weisungstext Rz 2.14
1.4	24.04.2024	Markus Moog (BSV)	Formatierungen, Fussnote 6 gelöscht, Anhang 3 Information Security Konzept entfernt, Hilfsmittel-Tabelle eingefügt und Downloads verlinkt
1.5	30.04.2024	Markus Moog (BSV)	Querverweise Rz und Anhänge, Tabelle Hilfsmittel und Vorlagen eingefügt und verlinkt
1.6	31.05.2024	Markus Moog (BSV)	Titel 2.13 geändert, Rollenbeschreibungen (Anhang 5)
1.7	30.07.2024	Markus Burri (BSV) Markus Moog (BSV)	Anhang 3 (neu): Schutzbedarfsanalyse und IT Grundschutz; Anhang 2: Neuer Meldeprozess eingefügt
1.8	04.11.2024	Markus Moog (BSV)	1.6: Gültigkeit und Handhabung von Prüfberichten nach ISO 27001 und ISAE eingefügt, Grafik Meldeprozess neu eingefügt, Links Hilfsmittel und Vorlagen angepasst
1.9	11.11.2024	Markus Moog Markus Burri	Anhang 2: Neu modellierter Meldeprozess nach BPMN eingefügt, Beispiele für Schutzgruppen und Zuweisungen (Anhang 3) eingefügt, Kommentar zum ausstehenden GL-Entscheid BSV zu Clouddiensten erfasst, Review des gesamten Dokuments
1.9.1	14.11.2024	Markus Moog Markus Burri	2.10.1: Umformulierung Beispiel 2.15.1: Ergänzung der Beschreibung, Erläuterung, dass Dritte sowohl IT Lieferanten als auch andere Dienstleister sein können
1.9.2	15.11.2024	Markus Moog Markus Burri	Update Beschreibung der Cloud-Dienste und Vorwort
2.0	17.12.2024	Markus Moog Markus Burri	Finale Version Abnahme durch KoKo eGov am 16.12.2024
2.1	24.03.2025	Markus Moog Markus Burri	Präzisierung bezüglich Verwendung von Microsoft 365

Vorwort

Die Weisungen richten sich an die Durchführungsstellen der 1. Säule/FamZ. Sie werden hinsichtlich der AHVG-Gesetzesrevision, die am 1. Januar 2024 in Kraft tritt, publiziert. Die Aufsicht über die AHV, die seit 1948 nahezu unverändert geblieben war, wird sich fortan stärker an den Risiken orientieren. Die Governance wird verstärkt und die Informationssysteme der 1. Säule werden zweckmässig gesteuert.

Im Herbst 2017 wurde vom Bundesrat der Entwurf zu einer Totalrevision des Datenschutzgesetzes verabschiedet. Das neue Datenschutzgesetz wurde an die veränderten technologischen sowie gesellschaftlichen Verhältnissen angepasst und stärkt die Rechte der Personendaten der betroffenen Personen. Die vorliegenden Weisungen berücksichtigen entsprechend auch das revidierte Datenschutzgesetz und die Ausführungsbestimmungen in der neuen Verordnung über den Datenschutz die am 1. September 2023 in Kraft getreten sind. Mit den vorherigen Empfehlungen vom 1. Januar 2022 wurde bereits sichergestellt, dass sich die Durchführungsstellen (DS) optimal auf die BSV-Weisungen zu den Informationssicherheits- und Datenschutz-Anforderungen (ISDS) vorbereiten konnten. Zu diesem Zweck wurden insbesondere auch die IT-Vertreter der DS (Projekt eAHV/IV Information Security) eng in die Ausarbeitung einbezogen.

Folgende Themen wurden für die Weiterbearbeitung der Empfehlungen berücksichtigt:

- **ISDS Basis- und erweiterte Dokumentation** (Ziff. 2.8.2 und 2.8.3 bzw. Anhänge 3 und 4)**:** Die Anforderung wurden auf Kompatibilität mit der neuen DSV überprüft.
- **Auftrag Dritter/Subunternehmer** (Ziff. 2.15.1, 2. Bullet)**:** In Bezug auf die Einschaltung von Subunternehmen (Art. 9 Abs. 3 DSG) ist die Genehmigung des Auftraggebers notwendig.
- **Auftragsbearbeiter im Ausland** (Ziff. 2.15.1, 3. Bullet und Anhang 3 Bst. E)**:** Gemäss dieser Empfehlung ist die Datenhaltung grundsätzlich in der Schweiz vorgesehen, und auch die Dienstleistungen für den Betrieb müssen grundsätzlich im Inland erfolgen und Ausnahmen müssen begründet sein. Werden Personendaten von einem Auftragsbearbeiter im Ausland bearbeitet, kommt es zu einer Datenbekanntgabe ins Ausland, und es kommen komplexe Bestimmungen des DSG zum Tragen. Die Einsetzung eines Dritten als Auftragsbearbeiter im Ausland ist sehr komplex und bedarf äusserst vieler rechtlicher Abklärungen bei Ländern, zu denen der Bundesrat nicht festgestellt hat, dass ein angemessener Schutz gewährleistet ist gemäss Art. 16 Abs. 1 DSG. In Ziff. 2.15 ist ein Hinweis auf die Einschränkungen nach DSG, der letztlich für alle DS Geltung haben muss (keine Ausnahmen für kantonale Stellen vorgesehen). Personendaten dürfen ins Ausland bekannt gegeben werden, wenn ein Verhaltenskodex oder eine Zertifizierung einen geeigneten Datenschutz gewährleistet (Art. 12 Abs. 1 DSV).
- **Clouddienste Dritter mit Datenhaltung in der Schweiz:** Seit der Veröffentlichung der eGov Mitteilung 043[1] Anfang 2022 haben diverse Entwicklungen stattgefunden. So hat der Bundesrat mit dem Swiss-U:S. Data Privacy Framework[2] auf den 15. September 2024 eine Änderung der Datenschutzverordnung in Kraft gesetzt[3]. Weiter wurden die Risiken des Foreign Lawful Access (Zugriff auf Daten durch ausländische Behörden, namentlich CLOUD Act) neu bewertet. Vor diesem Hintergrund hat das BSV eine Einschätzung gemacht, ob die Verwendung von M365 die Anforderungen der W-ISDS bezüglich Bearbeitung und Speicherung von besonders schützenswerten Daten erfüllt.

Grundsätzlich sind die Durchführungsstellen selbst für den Schutz ihrer Daten verantwortlich, sie müssen jedoch die nach der vorliegenden Weisung notwendigen Risikoeinschätzungen vornehmen (siehe Rz 2.15.2).

[1] eGov Mitteilung Nr. 043 vom 01.01.2022

[2] Medienmitteilung zum Swiss-U.S. Data Privacy Framework

[3] Ergänzung im Anhang 1 der DSV

Inhaltsverzeichnis

1 Ziel, Zweck, Gegenstand, Grundsätze, Geltungsbereich sowie Bezüge im Rechtssystem 5
1.1 Ziel, Zweck und Gegenstand 5
1.2 Geltungsbereich 5
1.3 Definition eines Informationssystems (IS) 6
1.4 Grundsatz Informationssicherheits-Management- System (ISMS) 6
1.5 Informationssicherheit 7
1.6 Gültigkeit und Handhabung von Prüfberichten gemäss ISO 27001, ISAE 3000 Typ 1 und Typ 2 8

2 Anforderungen 9
2.1 Informationssicherheits-Management-System (ISMS) 9
2.2 Grundaufbau des ISMS der Durchführungsstelle 9
2.3 Informationssicherheitsleitlinien 9
2.4 Anforderungen an die Informationssicherheitsorganisation 10
2.5 Anforderungen an Projekte im Bereich Informationssysteme 11
2.6 Informationssicherheit bei Mobilgeräten und Mobile Working 11
2.7 Informationssicherheit und Personal 12
2.8 IS-Schutzobjekte: Inventar, ISDS-Dokumentationen und weitere Anforderungen 12
2.9 Zugriffssteuerung zu den Informationssystemen 14
2.10 Kryptographie 14
2.11 Physischer Schutz 15
2.12 Massnahmen für die Betriebssicherheit 16
2.13 Netzwerk- und Kommunikationssicherheit 17
2.14 Änderungen an Informationssystemen 18
2.15 Verträge mit Dritten 19
2.16 Management von Informationssicherheitsvorfällen 20
2.17 Aufrechterhaltung der Informationssicherheit (Business Continuity Management BCM) 21
2.18 Richtlinienkonformität 21

Anhang 1: Rechtsbezüge zum Thema Informationssicherheit 22

Anhang 2: Meldeprozess Sicherheitsvorfall 24

Anhang 3 ISDS-Basisdokumentation 25

Anhang 4: Erweiterte ISDS-Dokumentation 37

Anhang 5: Rollenanforderungen an die Durchführungsstellen 41

Anhang 6: Hilfsmittel und Vorlagen 42

Abkürzungsverzeichnis 43

ISDS Anforderungen

Rz-Nr.	Weisungen BSV zur Informationssicherheit	Verweise auf ISO/IEC 27001:2022 A = Normativer Anhang	Kommentar
	1 Ziel, Zweck, Gegenstand, Grundsätze, Geltungsbereich sowie Bezüge im Rechtssystem		
1.1	**1.1 Ziel, Zweck und Gegenstand** Mit der Änderung des Bundesgesetzes über die Alters- und Hinterlassenenversicherung und der Modernisierung der Aufsicht in der 1. Säule sowie der Optimierung der 2. Säule der Alters-, Hinterlassenen- und Invalidenvorsorge weist das BSV die Durchführungsstellen an, bei ihren Informationssystemen laufend auf die nachfolgend umrissenen, neuen Rahmenbedingungen zu achten. Ein zentrales Anliegen der Gesetzesrevision ist es, dass die Informationssysteme der 1. Säule über die notwendige Stabilität und Anpassungsfähigkeit verfügen sowie die Informationssicherheit und den Datenschutz gewährleisten. Ganz grundsätzlich liegt es in der Eigenverantwortung der Durchführungsstellen, das Erreichen dieser Ziele sicherzustellen (vgl. Art. 49a Abs. 2 AHVG). Die exakte Umsetzung bezüglich Scope und Grösse der ISMS-Organisation ist unter anderem auch von der Risikobewertung und der Governance der Durchführungsstellen abhängig. In Bezug auf Informationssicherheit und Datenschutz müssen die Durchführungsstellen zusätzlich die von der BSV festgelegten Anforderungen erfüllen (Art. 49a Abs. 3 AHVG). Diese Anforderungen sind von den Durchführungsstellen zu beachten, soweit sie unter deren Geltungsbereich fallen (vgl. Rz 1.2). Mit diesen Weisungen werden die Anforderungen an die Informationssysteme für die Informationssicherheit und den Datenschutz skizziert (Art. 49a Abs. 3 in Verbindung mit Art. 72a Abs. 2 Bst. b AHVG), welche von den Durchführungsstellen erfüllt sein sollten (alle Rz von Kapitel 2).		
1.2	**1.2 Geltungsbereich** Die vorliegenden Weisungen zu den Anforderungen nach Rz 2 richten sich an alle Durchführungsstellen der AHV, IV, EO, und EL (vgl. Art. 66 Abs. 1 Bst. a IVG, Art. 21 Abs. 2 EOG, Art. 26 Abs. 1 Bst. a ELG). Sie richten sich auch an alle Zweigstellen nach Artikel 65 AHVG. Die Weisungen gelten zudem für die Durchführung der Familienzulagen (Art. 25 Bst. a in Verbindung mit Art. 27 Abs. 3 FamZG sowie Art. 25 FLG)		

Rz-Nr.	Weisungen BSV zur Informationssicherheit	Verweise auf ISO/IEC 27001:2022 A = Normativer Anhang	Kommentar
1.3	**1.3 Definition eines Informationssystems (IS)** Ein Informationssystem ist ein Hilfsmittel für die Datenbearbeitung, Datenbekanntgabe sowie für das Profiling (nach DSG) zur Aufgabenerfüllung[4] und enthält technische und organisatorische Elemente. Dazu gehören insbesondere: - Technische Elemente: Hardware, Software und Netzkomponenten, - Anwendung und Datenbestände, - Organisatorische Elemente: Prozesse, Aufgaben, Kompetenzen und Verantwortungen für den Aufbau und den Betrieb. Ein Informationssystem ist immer ein Wert, der adäquat zu schützen ist. Es handelt sich damit um ein Schutzobjekt (vgl. Rz 2.8).	A.5.9	
1.4	**1.4 Grundsatz Informationssicherheits-Management-System (ISMS)** Als Grundlage für die Erfüllung der Anforderungen sollte den Durchführungsstellen ein von ihnen zu betreibendes Informationssicherheits-Management-System (ISMS) dienen. Ein ISMS ist ein Führungsinstrument und dient der systematischen Planung, Umsetzung, Überprüfung und Verbesserung der Informationssicherheit. Es umfasst die dafür nötigen Vorschriften und Verfahren und macht sichtbar, wem in der Organisation, welche Aufgaben, Kompetenzen und Verantwortlichkeiten zugeordnet werden. Mit dem Begriff «ISMS» wird implizit auf die Norm ISO/IEC 27001 verwiesen, die sowohl in der Privatwirtschaft als auch vermehrt in öffentlichen Verwaltungen als Standard gilt. Das ISMS orientiert sich an den nationalen[5] und internationalen[6] Standards und muss wenigstens den nachfolgenden Vorgaben entsprechen. Es ist Gegenstand der Prüfung der Revisionsstelle im Sinne von Art. 68a, Abs. 2 Bst. c AHVG. Die Revisionsstelle prüft, ob das ISMS der Durchführungsstellen den in diesen Weisungen umrissenen Anforderungen entspricht. Davon ausgenommen sind die Familienausgleichskassen nach Artikel 14 Buchstabe a FamZG, sofern die kantonalen Familienzulagengesetze nichts anderes vorsehen.		Art. 68a AHVG gilt nicht für das FamZG (anders FLG). Die Regelung der Kassenrevision und der Arbeitgeberkontrolle liegt nach Art. 17 Abs. 2 Bst. i FamZG explizit in kantonaler Kompetenz. Für die Durchführungsstellen der AHV, welche auch die Durchführung bei den Familienzulagen als übertragene Aufgabe wahrnehmen, wird sich die Revision auf das ISMS erstrecken, unter Einschluss der Familienzulagen, wobei gegebenenfalls eine separate Berichterstattung u.a. im Sinne von

[4] im Sinne von Art. 5Bst. d-g DSG

[5] insbesondere die Vorgaben IKT-Grundschutz in der Bundesverwaltung, bzw. Informationssicherheitsgesetzes ISG

[6] ISO/EC 27001:2022 betreffend Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen sowie ISO/IEC 27002:2022 betreffend Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmassnahmen der die in ISO/IEC 27001:2022, Anhang A beschriebenen normativen Informationssicherheitsmassnahmen erläutert und Vorschläge für deren Umsetzung macht.

Rz-Nr.	Weisungen BSV zur Informationssicherheit	Verweise auf ISO/IEC 27001:2022 A = Normativer Anhang	Kommentar
			Rz 3604 WÜWA möglich ist.
1.5	**1.5 Informationssicherheit** Informationssicherheit ist ein umfassender Begriff. Entsprechend umfassend sind Massnahmen, welche darauf abzielen, diese zu gewährleisten (von der Projektentwicklung bis zum Geräteschutz). Datensicherheit und grosse Teile des Datenschutzes gehören zur Informationssicherheit. 1. Datensicherheit umfasst in praktischer Hinsicht alle Massnahmen zur Sicherstellung der Vertraulichkeit, Integrität, Nachvollziehbarkeit und Verfügbarkeit der Informationen. 2. Datenschutz umfasst in praktischer Hinsicht alle Massnahmen zur Verhinderung einer unerwünschten Bearbeitung von Personendaten und deren Folgen. Der Schutz zielt auf die Person und nicht die Daten an sich ab. Grundsätzlich sind bei der Informationssicherheit die Vorschriften aus ganz verschiedenen Rechtsquellen anwendbar und von den Durchführungsstellen zu beachten (vgl. Anhang 1: Übersicht nationale Rechtsquellen, ISO-Normen). Die vorliegenden Weisungen konzentrieren sich auf die Anforderungen an ein ISMS und behandeln keine Datenschutzfragen, wie sie sich aus dem direkten Verhältnis zwischen versicherter Person und Durchführungsstelle ergeben können. Für solche Fälle ist nach wie vor das Kreisschreiben über die Schweigepflicht und die Datenbekanntgabe in der AHV/IV/EO/EL/FamZLw/FamZ (KSSD) anwendbar. Die Anliegen des Datenschutzes werden jedoch in diesen für die Durchführungsstellen geltenden Weisungen berücksichtigt, indem die Anforderungen des Datenschutzes bei der Erarbeitung der ISDS-Basisdokumentation zur Informationssicherheit geprüft werden müssen (vgl. Teil Buchstabe a gemäss Rz 2.8.2). Für Fragen der Aufbewahrung von Daten ist überdies die Weisung über die Aktenführung in der AHV/IV/EO/EL/FamZLw/FamZ (WAF) zu beachten.		Es handelt sich um technische und organisatorische Massnahme. Diese sind nicht zu verwechseln mit den technischen und organisatorischen Massnahmen nach Artikel 153d AHVG[7], welche nur von Behörden, Organisationen und Personen eingehalten werden müssen, die ausserhalb der Sozialversicherungen zur Nutzung der AHV-Versichertennummer berechtigt sind.

[7] Gemäss Botschaft zur Änderung des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (Systematische Verwendung der AHV-Nummer durch Behörden (BBl **2019** 7359)

Rz-Nr.	Weisungen BSV zur Informationssicherheit	Verweise auf ISO/IEC 27001:2022 A = Normativer Anhang	Kommentar
1.6	**1.6 Gültigkeit und Handhabung von Prüfberichten gemäss ISO 27001, ISAE 3000 Typ 1 und Typ 2** Gemäss dieser Weisung gelten Prüfberichte, die nach den Standards ISO 27001 sowie ISAE 3000 Typ 1 und/oder Typ 2 erstellt wurden und die Konformität mit der Weisung W-ISDS nachweisen, als ausreichend, wenn mindestens eine der folgenden Anforderungen erfüllt ist: 1. **ISO 27001 Zertifizierung:** Die Durchführungsstellen weisen ihren Zertifizierungsbericht der Revisionsstelle vor. Es braucht keine nochmalige vollumfängliche Prüfung, falls: • Der Anwendungsbereich des zertifizierten ISMS alle relevanten Organisationseinheiten und Geschäftsprozesse der Durchführungsstellen umfasst • In der Anwendbarkeitserklärung des ISMS keine der in der W-ISDS geforderten Sicherheitsmassnahmen ausgeschlossen sind • Im (Re-)Zertifizierungs-Audit alle in der W-ISDS geforderten Sicherheitsmassnahmen überprüft wurden 2. **ISAE 3000 Typ 1:** Prüfbericht, der auf Basis des ISAE 3000 Typ 1 erstellt wurde und auf alle festgelegten Anforderungen der Weisung W-ISDS referenziert. 3. **ISAE 3000 Typ 2:** Prüfbericht (Wirksamkeit), der gemäss ISAE 3000 Typ 2 mit hinreichender Sicherheit und zeitraumgeprüft erstellt und nach W-ISDS definierten Kontrollen geprüft wurde.		

	2 Anforderungen	ISO-Norm	Kommentar
2.1	**2.1 Informationssicherheits-Management-System (ISMS)[8]** Jede Durchführungsstelle verfügt über ein ISMS (vgl. 1.4).	4.4	
2.2	**2.2 Grundaufbau des ISMS der Durchführungsstelle**		
a	Die Durchführungsstellen legen in ihrem ISMS fest welche Themen relevant sind für die Erfüllung ihre Aufgaben nach Art. 63 AHVG (SR 831.10), Art. 57 IVG (SR 831.20) und ihre Tätigkeit im Rahmen des EOG (SR 834.1), ELG (SR 831.30), FLG (SR 836.1) und FamZG (SR 836.2).	4.1	
b	Sie identifizieren die involvierten Stellen und analysieren ihre Anforderungen in Bezug auf Informationssicherheit.	4.2	
c	Sie haben eine aktuelle Übersicht über alle Informationssysteme und IT-relevanten Aktivitäten (vgl. auch Inventar nach Ziff. 2.8.1), welche in das ISMS integriert sind.	A.5.9	
d	Gleichzeitig legen sie die diejenigen Bereiche fest, für welche die Anforderungen nicht Anwendung finden (z. B. Durchführungsstellen, welche Aufgaben ausserhalb der 1. Säule/FamZ wahrnehmen, müssen festlegen welche Anwendungsbereiche ausgenommen sind). Wird keine Abgrenzung vorgenommen, ist das ISMS auf die gesamte Organisation anwendbar. Beispielsweise muss eine Sozialversicherungsanstalt (SVA-Struktur) festlegen, ob sie ein ISMS für die Gesamtorganisation erstellt, oder für jede Durchführungsstelle/Organisationseinheit einzeln. Ebenso muss die zentrale Ausgleichstelle (ZAS) festlegen, ob sie ein ISMS für die gesamte ZAS erstellt oder ob die Durchführungsstellen der ZAS (gemäss ZAS Verordnung) ihr eigenes ISMS aufbauen.	4.3	
e	Die Durchführungsstellen sorgen für eine laufende Aktualisierung und Verbesserung des ISMS (einschliesslich BCM vgl. Rz. 2.17) und seiner Komponenten. Sie nehmen wenigstens jährlich eine Überprüfung der Aktualität vor.	4.4 A 5.30	
2.3	**2.3 Informationssicherheitsleitlinien** Die Geschäftsleitung der Durchführungsstelle erlässt basierend auf ihrem Grundaufbau des ISMS (Ziff. 2.2) Informationssicherheitsleitlinien und sorgt für deren Bekanntmachung innerhalb der Durchführungsstelle und gegenüber den involvierten externen Stellen, sowie die regelmässige Aktualisierung. Die Informationssicherheitsleitlinien achten auf das Aufgabentrennungsprinzip und beinhalten: 1. Die Umschreibung der Informationssicherheitsorganisation und ihre Schnittstellen zu den folgenden, vorgeschriebenen Elementen (Art. 66 AHVG): a. zum internen Kontrollsystem (IKS)	A.5.1 A.5.3	

[8] Für den Aufbau des ISMS wird folgender Leitfaden empfohlen:
- ISACA Leitfaden «Implementieren eines ISMS nach ISO/IEC 27001:2022»

	b. zum Qualitätsmanagementsystem (insbesondere kontinuierlicher Verbesserungsprozess KVP) c. zum Risikomanagementsystem (RM) 2. Die Regelung der adäquaten Information an die Geschäftsleitung und weitere involvierten Stellen (vgl. Rz 2.2 Bst. b und d) sowie gegebenenfalls: a. des EDÖB nach Artikel 24 DSG (bei einer entsprechenden Verletzung der Datensicherheit) oder des Datenschutzbeauftragten nach kantonalem Recht; b. des BSV durch die Informationssicherheitsorganisation und die Beschreibung eines Informationssicherheitsvorfallbearbeitungsprozesses (als Beispiel vgl. Anhang 2). 3. Die Regelung der adäquaten Information des BSV (und/oder der jeweils zuständigen Aufsichtsbehörde) über Informationssicherheitsvorfälle ist vorzusehen, wenn: • eine Information des EDÖB oder des kantonalen Datenschutzbeauftragten nötig ist; • eine Gefahr besteht, dass der Informationssicherheitsvorfall die Informationssysteme anderer Durchführungsstellen beeinträchtigt; • der Informationssicherheitsvorfall über wenige Einzelfälle hinaus die Interessen der Versicherten betrifft oder die Aufgabenerfüllung der Durchführungsstelle in Frage stellt; • der Informationssicherheitsvorfall grösseren finanziellen Schaden verursachen kann; • das Image der Versicherung über einen Bagatellfall hinaus beeinträchtigt werden kann (z.B. grösserer Datenverlust oder Datenmanipulation); • die Möglichkeit besteht, dass die Funktion der Informationssicherheitsorganisation der Durchführungsstelle in absehbarer Zeit nicht gegeben ist oder in der Vergangenheit beeinträchtigt wurde.	A.5.5 A.5.24	Siehe Meldeprozess
2.4	**2.4 Anforderungen an die Informationssicherheitsorganisation** Die Sicherheitsorganisation sieht wenigstens vor, dass die Durchführungsstelle einen Informationssicherheitsbeauftragten (ISB) bezeichnet und weitere Personen, die eine Schlüsselrolle in der Umsetzung der Informationssicherheit haben. Der ISB hat namentlich die folgenden Aufgaben: • Er koordiniert die Aspekte der Informationssicherheit innerhalb der Durchführungsstelle sowie mit allfälligen beauftragten Leistungserbringern (z.B. IT-Beauftragten, Lieferanten, etc.). • Er ist Ansprechpartner der Informationssicherheitsbeauftragten der IT-Leistungserbringer. • Er ist Ansprechpartner gegenüber dem BSV für Informationssicherheitsvorfälle für welche die von den Durchführungsstellen erlassenen Informationssicherheitsleitlinien die Information des BSV vorsehen (Rz 2.3 Ziff 3).	A.5.2	

	• Er prüft die Dokumentationen zur Informationssicherheit (insbesondere die ISDS- Dokumentationen vgl. Rz 2.8.2 und 2.8.3) und zur weiteren Umsetzung der Anforderungen • Er informiert den Leiter der Durchführungsstelle regelmässig über den aktuellen Stand der Aspekte der Informationssicherheit in ihrer Organisation. • Er gibt Empfehlungen zuhanden der Geschäftsleitung der Durchführungsstelle ab.		Besondere Regelung bei FAK (evt. Kanton)
2.5	**2.5 Anforderungen an Projekte im Bereich Informationssysteme** Ein Projekt im Bereich Informationssysteme ist ein zeitlich befristetes Vorhaben mit definierten Zielen und einer spezifischen Projektorganisation, dessen Hauptziel darin besteht, eine Anwendung einzuführen, anzupassen oder IS-Infrastrukturen aufzubauen oder zu verbessern. Die Durchführungsstellen sind dafür verantwortlich, die Notwendigkeit eines Projekts im Bereich Informationssysteme festzulegen und dessen Abwicklung zu regeln. Sie beachten dabei in jedem Fall Folgendes: 1. das Vorgehen hat einer definierten Projektmanagementmethode zu folgen, welche für die Nachvollziehbarkeit bei der Steuerung, Führung und Ausführung von Projekten verschiedener Charakteristiken und Komplexitäten sorgt. Die eingesetzte Projektmanagementmethode entspricht dem Standard der schweizerischen Norm des Vereins eCH oder ist gleichwertig (www.ech.ch). 2. es wird eine Informationssicherheits- und Datenschutzdokumentation (ISDS-Basis-Dokumentation nach Rz 2.8.2) erstellt, und wenn nötig, eine erweiterte ISDS-Dokumentation nach Rz 2.8.3.	A.5.8	
2.6	**2.6 Informationssicherheit bei Mobilgeräten und Mobile Working** Die Durchführungsstellen regeln: • Die Rahmenbedingungen, unter welchen Mobile Working und der Einsatz von Mobilgeräten für das eingesetzte Personal gestattet ist. • Die sichere geschäftliche Nutzung von privaten und geschäftlichen Mobilgeräten unter Berücksichtigung der Möglichkeit von Verlust, Diebstahl oder Beschädigung. Ausgenommen davon sind anonyme und personalisierte Zugriffsmöglichkeiten zu Anwendungen, welche als öffentliche Web-Auftritte der Durchführungsstelle ausgestaltet sind. Beim Einsatz privater Geräte ist auf einen gleichwertigen Schutz zu achten. • Das sichere Mobile Working mit unterstützenden Sicherheitsmassnahmen zum Schutz von Informationen, auf die von Mobilgeräten ausserhalb der Geschäftsräumlichkeiten aus zugegriffen wird oder die dort verarbeitet oder gespeichert werden. Bei der Bearbeitung geschäftlicher Informationen auf privaten Geräten müssen diese die gleichen Bedingungen hinsichtlich Informationssicherheit und Datenschutz erfüllen, wie die von der Durchführungsstelle bereitgestellten Geräte.	A.8.1, A.6.7	

2.7	**2.7 Informationssicherheit und Personal**		
2.7.1	**Personalsicherheit** Die Durchführungsstellen regeln den Einsatz des eigenen Personals und des Personals von beauftragten Dritten für die Zeit vor, während und nach dem Einsatz zwecks Gewährleistung der Informationssicherheit. Speziell vorzusehen ist ein Prozess für die angemessene Sicherheitsüberprüfung des ISB und weiterer Schlüsselrollen in der Informationssicherheitsorganisation (vgl. Rz. 2.4), welcher Risiken in Bezug auf die persönliche Integrität erkennen lässt und adäquate Massnahmen erlaubt. Es wird empfohlen, alle fünf Jahre eine Überprüfung des Betreibungs- und Strafregisterauszugs durchzuführen.	A.6.1, A.6.2, A.6.3, A.6.4, A.6.5	
2.7.2	**Information und Schulung** Die Durchführungsstellen sorgen dafür, dass das eingesetzte Personal mindestens jährlich über die Pflichten bezüglich der Informationssicherheit im Bilde ist und diesbezüglich sensibilisiert ist.	A.5.4, 6.3, 6.4	
2.7.3	**Änderung der Verhältnisse** Die Benutzerrechte des eingesetzten Personals auf Zutritt (vgl. Rz 2.11.1), Zugriff und Berechtigungen zu den Informationssystemen (vgl. Rz 2.9) sind aktuell zu halten. Sie müssen umgehend an veränderte Verhältnisse angepasst werden, wenn die Anstellung, der Auftrag oder eine entsprechende Nutzungsvereinbarung geändert oder beendet wird. Ein Prozess für die Behandlung unbenutzter Konten muss eingerichtet werden.	A.6.5	
2.8	**2.8 IS-Schutzobjekte: Inventar, ISDS-Dokumentationen und weitere Anforderungen**	A.5.9, A.5.10	
2.8.1	Die Durchführungsstellen verfügen über ein **Inventar** aller Informationssysteme (vgl. Rz 2.2 Bst. c). Dieses wird laufend aktualisiert. Ein Informationssystem ist immer ein Wert, welcher adäquat zu schützen ist. Es handelt sich damit um ein Schutzobjekt.	A.5.9	
2.8.2	**ISDS-Basisdokumentation** 1. Bei allen IS-Projekten (Rz. 2.5) ist vorab eine Analyse zur Informationssicherheit und zum Datenschutz zu erstellen. Als Template kann die Risikovorprüfung verwendet werden (siehe Anhang 6). 2. Eine ISDS-Basisdokumentation muss sich mit Blick auf Informationssicherheit und Datenschutz mindestens auf folgende Themen erstrecken: a. Abklärung der datenschutzrechtlichen Rahmenbedingungen, insbesondere in Bezug auf die Rechtskonformität der Datenbearbeitung nach DSG und allenfalls zusätzlichen geltenden kantonalen Datenschutzgesetzen und Bestimmungen der Sozialversicherungsgesetze siehe Leitfaden in Anhang 3); b. Klassifizierung des Schutzobjektes nach Verfügbarkeit (inkl. Beurteilung des Schutzobjekts in Bezug auf die Einteilung als geschäftskritische Anwendung);	A.5.10, A.5.12, 5.13	Hilfsmittel und Vorlagen [Anhang 6]

	c. Klassifizierung des Schutzobjektes nach Vertraulichkeit; d. Klassifizierung des Schutzobjektes nach Integrität und Nachvollziehbarkeit (in Bezug auf die Datenzugriffe in Schreibmodus); e. Ort der Datenhaltung; f. Beschreibung des Schutzobjekts; g. die Klärung der Aufnahme in das Verzeichnis bzw. der Meldung beim EDÖB (Art 12 Abs. 4 DSG). Durchführungsstellen, welche kantonale Einrichtungen sind, klären die Anmeldung bei einem kantonalen Register gemäss kantonalem Datenschutzgesetz; h. die Klärung der Notwendigkeit einer Datenschutz-Folgenabschätzung nach Art. 22 DSG; i. Zuweisung zu einer Schutzgruppe. 3. Zeigt sich aufgrund der Analyse nach Ziffer 2, dass mit dem Schutzobjekt besonders schützenswerte Personendaten oder sonstige Daten mit besonderen Vertraulichkeitsanforderungen bearbeitet werden, ist die ISDS-Basis-Dokumentation gemäss Rz 2.8.3 zu erweitern. 4. Eine ISDS-Basisdokumentation orientiert sich qualitativ und quantitativ am Muster gemäss Anhang 3.		
2.8.3	**Erweiterte ISDS-Dokumentation** Die erweiterte ISDS-Dokumentation ist zu erstellen, wenn mit dem Schutzobjekt besonders schützenswerte Personendaten bearbeitet werden, d.h. die Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen kann (vgl. RZ 2.8.2 Ziff. 3). Sie umfasst wenigstens folgende Themen: a. Zusammenfassung der relevanten Ergebnisse der ISDS-Basisdokumentation b. Sicherheitsrelevante Systembeschreibung b.1 Ansprechpartner / Verantwortlichkeiten b.2 Beschreibung des Gesamtsystems b.3 Beschreibung der zu bearbeitenden Daten (Bearbeitungsreglement mit Rollenkonzept und Handhabung von Datenträgern) b.4 Architekturskizze / Kommunikationsmatrix b.5 Beschreibung der zugrundeliegenden Technik c. Risikoanalyse, Schutzmassnahmen und verbleibende Restrisiken (gegebenenfalls mit Stellungnahme des EDÖB) d. Wiederherstellung des Geschäftsbetriebes/ Notfall-Konzept (Katastrophen-Vorsorge) e. Einhaltung / Überprüfung / Abnahme der Schutzmassnahmen f. Ausserbetriebnahme	A.5.10, A.5.12, 5.13	

	Die erweiterte ISDS-Dokumentation orientiert sich qualitativ und quantitativ am Muster gemäss Anhang 4.		
2.8.4	**Aktualität der ISDS-Dokumentationen** Bestehende (betriebene) Informationssysteme müssen über ISDS-Dokumentationen (Rz 2.8.2 und 2.8.3) verfügen, welche den aktuellen Verhältnissen entsprechen.		Änderungen an Informationssystemen siehe Rz 2.14
2.8.5	**Anwendungsverantwortlicher** Die Durchführungsstellen bezeichnen für jedes allein oder gemeinsam genutzte Informationssystem einen Anwendungsverantwortlichen. Der Anwendungsverantwortliche legt zusammen mit dem ISB die Sicherheitsanforderungen für das Informationssystem fest. Der Anwendungsverantwortliche verantwortet die Umsetzung der Sicherheitsmassnahmen.	A.5.9	
2.9	**2.9 Zugriffssteuerung zu den Informationssystemen** Die Durchführungsstellen steuern den Zugriff auf ihre Informationssysteme. Das Zugriffssteuerungskonzept beinhaltet wenigstens: a. eine Benutzerverwaltung mit einer zweifelsfreien Benutzeridentifikation; b. ein Berechtigungsmodell anhand der Funktionen/Aufgaben der Benutzer; c. Prozesse zur Vergabe, Mutation und zum Entzug von Benutzerkonten und Berechtigungen; und stellt sicher, dass d. sämtliche Zugriffe (inkl. automatisierten Prozessen mit machine-to-machine-Zugriff) auf Informationssysteme mit einer dem Schutzbedarf entsprechenden Authentifikation und nötigenfalls adäquate kryptographischen Massnahmen (ISO A.8.24) gemäss der Zugriffmatrix geschützt werden (siehe auch Rz 2.13.2); e. den Benutzern der Zugriff auf Informationssysteme nur die Rechte eingeräumt werden, die sie zur Erfüllung ihrer Aufgaben benötigen; f. eine Protokollierung der Zugriffe nach Art. 4 DSV erfolgt (siehe Anhang 3 Ziffer 7); g. die Richtigkeit und Zweckmässigkeit der erteilten Benutzerrechte wenigstens jährlich durch den AV geprüft werden	A.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.3, A.8.4, A.8.5	
2.10	**2.10 Kryptographie**		
2.10.1	Die von den Durchführungsstellen eingesetzten kryptografischen Verfahren und Methoden müssen dem Stand der Technik entsprechen. Beim Einsatz asymmetrischer Kryptosysteme müssen die Zertifikate, abhängig vom jeweiligen Anwendungsfall und den damit verbundenen gesetzlichen Anforderungen von einer anerkannten Certificate Authority (CA) ausgestellt sein. Unter anderem erfüllen SAS-anerkannte Zertifikate für elektronische Signaturen gemäss Verordnung über Zertifizierungsdienste im Bereich der	A.8.24	

	elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (VZertES SR 943.032)[9]. Die ausgewählte Lösung ist in der ISDS-Dokumentation (Rz 2.8.2 bzw. 2.8.3) zu beschreiben. Die Durchführungsstellen stellen die sichere Verwaltung und Gültigkeit der kryptografischen Schlüssel sicher.		
2.11	**2.11 Physischer Schutz**		
2.11.1	**Sicherheitsdispositiv für Räumlichkeiten** Die Durchführungsstellen verfügen über ein Sicherheitsdispositiv zum physischen Schutz ihrer Informationssysteme. Dabei sind verschiedene Massnahmen vorzusehen, welche den adäquaten Schutz der einzelnen Schutzobjekte gewährleisten, und zwar unter Berücksichtigung der Ergebnisse der ISDS-Prüfung (Rz 2.8.2 bzw. 2.8.3) hinsichtlich der Schutzgruppen (vgl. Rz 2.8.2 Ziffer 2 Bst. i). Die im Sicherheitsdispositiv vorzusehenden Massnahmen müssen sich auf folgende Punkte beziehen: • Physische Sicherheitsperimeter (Lage der Umgebung und bauliche Massnahmen) • Physische Zutrittssteuerung • Sichern von Büros, Räumen und Einrichtungen • Schutz vor externen und umweltbedingten Bedrohungen	A.7.1, A.7.2, A.7.3, A.7.5	
2.11.2	**Massnahmen für Geräte und Betriebsmittel** Die Durchführungsstellen und ihre Dienstleister (vgl. Rz 2.15.1) verfügen über dokumentierte Massnahmen zum Schutz von Geräten und Betriebsmittel gegen Verlust, Beschädigung, Diebstahl oder Gefährdung. Die vorzusehenden Massnahmen für Geräte müssen sich auf folgende Punkte beziehen: • Platzierung und Schutz von Geräten und Betriebsmitteln • Versorgungseinrichtungen • Sicherheit der Verkabelung • Instandhalten von Geräten und Betriebsmitteln • Entfernen von Werten • Sicherheit von Geräten, Betriebsmitteln und Werten ausserhalb der Räumlichkeiten • Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln • Unbeaufsichtigte Benutzergeräte • Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren	A.7.7 - A.7.14, A.8.1	

[9] siehe dafür die BAKOM Webseite

2.12	**2.12 Massnahmen für die Betriebssicherheit** Die Durchführungsstellen und ihre Dienstleister (vgl. Rz 2.15) verfügen über dokumentierte Massnahmen zur Betriebssicherheit. Die vorzusehenden Massnahmen müssen sich auf folgende Punkte beziehen: A. Betriebsabläufe und –verantwortlichkeiten • Dokumentierte Bedienabläufe • Änderungssteuerung • Kapazitätssteuerung • Trennung von Entwicklungs-, Test- und Betriebsumgebungen B. Schutz vor Schadsoftware durch geeignete Massnahmen C. Datensicherung D. Protokollierung und Überwachung • Ereignisprotokollierung • Schutz der Protokollinformation • Administratoren- und Benutzeraktivitäten • Uhrensynchronisation E. Steuerung von Software zur Installation von Software auf Systemen, die sich im Betrieb befinden F. Technische Schwachstellen • Handhabung von technischen Schwachstellen • Einschränkung von Softwareinstallation G. Integritätsprüfung bei erhöhtem Schutzbedarf (vgl. Anhang 4, erweiterte ISDS-Dokumentation Bst. D) H. Audit von Informationssystemen Sowie Massnahmen für Audits von Informationssystemen, um die negativen Auswirkungen der Audittätigkeit zu minimieren. Das heisst, Audit-Tätigkeiten, wie Penetration Test, K-Vorsorge-Tests können negative Auswirkungen auf die Informationssysteme, Daten und Benutzer haben. Es sind entsprechend Massnahmen, u.a. detaillierte Planung, Kommunikation etc. vorzusehen, um derartige Auswirkungen zu minimieren.	A.5.37, A.8.6, A.8.31, A.8.32 A.8.7 A.8.13, A.8.15, A.8.17 A.8.19 A.8.19 A.8.8 A.8.34	

2.13	**2.13 Netzwerk- und Kommunikationssicherheit**		
2.13.1	**Architekturdokumentation** Die Durchführungsstellen verfügen über eine Architekturdokumentation der Umgebung ihrer Informationssysteme. Diese gibt Auskunft über • die grundlegenden eigenen und fremden Netzwerktopologien der im Rahmen ihres Werteinventars (vgl. Ziff. 2.8.1) genutzten Netze. • die grundlegende Netztopologie beinhaltet ihre aktiven Komponenten und deren Konfigurationen.		
2.13.2	**Zugriffsmatrix** Die Durchführungsstellen verfügen über eine verbindliche Zugriffmatrix, die festlegt, wie Personen und automatisierte Prozesse (Maschinen/Software) auf die in den verschiedenen Netzzonen (vgl. Ziff. 2.13.3) betriebenen Informationssysteme zugreifen können, bzw. wie diese zu authentifizieren und allenfalls auch zu autorisieren sind (vgl. Ziff. 2.10, Kryptographie).		
2.13.3	**Netzwerksicherheit und -dokumentation** 1. Die Durchführungsstellen sehen Richtlinien zur Netzwerksicherheit vor und legen die Zuständigkeiten zur Verwaltung von Netzwerken und Netzwerkübergängen fest. 2. Für Netze, welche in der Verantwortlichkeit der Durchführungsstellen liegen, verfügen die Durchführungsstellen über ein Nutzungsreglement, welches wenigstens die folgenden Punkte vorsieht: • Anschluss von fremden Kommunikationsendgeräten • Regelung der Netzübergänge • Remote Access 3. Die Durchführungsstellen legen fest, dass durch eine geeignete Netzwerkstruktur (z. B. Zonierung und Segmentierung) sowie durch den geeigneten Aufbau und die Konfiguration die Daten im Zusammenhang mit der 1. Säule geschützt sind. 4. Die Durchführungsstellen schützen die Netze in ihrer Verantwortlichkeit vor Angriffen und unberechtigtem Zugriff. 5. Für Netze, welche nicht in den Verantwortlichkeitsbereich der Durchführungsstellen liegen und deren Nutzung nicht vertraglich geregelt sein kann (Internet), müssen Sicherheitsmassnahmen umgesetzt werden. 6. Die Netzwerkstrukturen sowie die Zuständigkeiten sind zu dokumentieren.	A.8.20 - A.8.22 A.5.14, A.6.6 A.8.21	
2.13.4	**Geschützte Informationsübertragung** 1. Für die Informationsübertragung treffen die Durchführungsstellen Massnahmen, welche sicherstellen, dass die Daten entsprechend den Anforderungen des Datenschutzes und der Datensicherheit (Informationssicherheit, Rz 2.8.2 / 2.8.3) ausreichend geschützt	A.5.14, A.6.6	

	sind, unabhängig davon, ob sie für den Datenaustausch ein eigenes Netz, ein vertraglich geregeltes Netz oder ein fremdes Netz benutzen (vgl. Ziff. 2.10 Kryptographie). 2. Die Durchführungsstellen sorgen dafür, dass die verschiedenen Schutzniveaus (vgl. Rz. 2.8.2 und 2.8.3) bei der Datenübermittlung bei den Mitarbeitenden bekannt sind (vgl. 2.7.2) und diese entsprechende Übertragungsmittel nutzen (z. B. E-Mail-Verschlüsselung). 3. Für den elektronischen Datenaustausch besonderes schützenswerte Personendaten (gemäss DSG) zwischen den Durchführungsstellen und der Zentralen Ausgleichsstelle (ZAS) stehen mehrere technische Lösungsansätze zur Verfügung: 1 Sedex-Netzwerk: siehe dazu die BSV Weisungen für die elektronische Datenaustauschplattform der AHV-Ausgleichskassen und IV-Stellen (318.106.07 DAP). 2 Verschlüsselte Uebermittlung (beispielsweise Incamail, welches alle Durchführungsstellen über den Verein eAHV/IV als gemeinsamen Standard vereinbart haben) 3 Versand direkt aus der Applikation statt via e-Mail.		
2.14	**2.14 Änderungen an Informationssystemen** Die Durchführungsstellen stellen sicher, dass die Sicherheit über den gesamten Lebenszyklus von Informationssystemen hinweg fester Bestandteil dieser Systeme ist. Spezifische Sicherheitsanforderungen, welche sich aus der Informationssicherheit und dem Datenschutz (vgl. Rz 2.5, 2.8.2 und 2.8.3) ergeben, sind zu berücksichtigen. Die ISDS-Dokumentationen (Rz 2.8.2 bzw. 2.8.3) sind bei Änderungen zu aktualisieren. Werden keine Änderungen am Informationssystem vorgenommen, sollen die ISDS-Dokumentationen wenigstens alle 5 Jahre auf ihre Aktualität überprüft werden. Für Änderungen an Informationssystemen gelten die Anforderungen, wie sie nach Rz 2.5 für neue Projekte gelten. Damit ist grundsätzlich sichergestellt, dass die Sicherheitsanforderungen bei der Entwicklung der Informationssysteme berücksichtigt werden. Zusätzlich sind die Anforderungen nach Rz 2.12 Bst. A, Punkt 4 hinsichtlich Trennung von Entwicklungs-, Test- und Betriebsumgebungen zu berücksichtigen, und der Schutz der für Tests verwendeten Daten ist sicherzustellen. Sind die Durchführungsstellen nicht selber verantwortlich für die Umsetzung der Änderungen an ihren Informationssystemen, müssen die Anforderungen an die mit den Änderungen betrauten Dritten kommuniziert und deren Einhaltung überwacht und kontrolliert werden.	A.5.8, A.8.26 A.8.25, A.8.27, A.8.29 - A.8.32 A.8.33 A.8.30	

2.15	**2.15 Verträge mit Dritten**		
2.15.1	• Schliessen die Durchführungsstellen Verträge mit Dritten zur Erbringung von Dienstleistungen ab, welche potentiellen Zugang zu sozialversicherungsrechtlichen Daten voraussetzt oder die Bearbeitung solcher Daten betrifft, stellen sie vertraglich sicher, dass sämtliche Schutzvorschriften (Verschwiegenheitspflicht, Datenbearbeitung etc.) sowie die Anforderungen, welche die Leistungen konkret betreffen, beachtet werden und sehen im Vertrag entsprechende Kontrollmassanahmen, sowie bei nicht von den Durchführungsstellen beherrschten Dritten Konventionalstrafen für den Fall der Verletzung dieser Vorschriften vor. Bei diesen Verträgen kann es sich sowohl um Lieferantenbeziehungen im IT-Umfeld als auch um Dienstleistungen im Nicht-IT Umfeld handeln. • Grundsätzlich müssen Verträge mit Dritten vorsehen, dass der Vertrag durch den Dritten selber zu erfüllen ist, und eine Auslagerung der übernommenen Verpflichtungen (ganz oder teilweise) in jedem Falle nur dann zulässig ist, wenn die Durchführungsstelle die Möglichkeit haben, sich dagegen auszusprechen. Auch im Falle einer Auslagerung der Verpflichtung muss durch entsprechende Abreden sichergestellt werden, dass die Anforderungen vollumfänglich eingehalten werden. Dies gilt ausdrücklich auch für die Verpflichtung, ein Inventar zu führen (Rz 2.8.1). • Die Dienstleistungen für den Betrieb müssen grundsätzlich im Inland erbracht werden. Dienstleistungen für den Betrieb aus dem Ausland sind auszuweisen und zu begründen. • Es muss jederzeit sichergestellt werden, dass keine Personendaten von Versicherten im Ausland bearbeitet werden, ausser es handelt sich um eine Bearbeitung, welche von Gesetzes wegen mit einem internationalen Datenaustausch verbunden ist (z. B. Art. 32 Abs. 3 ATSG, bzw. KSBIL (vgl. Bilaterale Abkommen Schweiz-EU. Abkommen mit der EFTA. Kreisschreiben über das Verfahren zur Leistungsfestsetzung in der AHV/IV)).	A.5.19 - A.5.21	Angaben zu: - Geforderten Servicezeiten - Anforderungen Verfügbarkeit Die Durchführungsstellen ermitteln den Schutzbedarf der Daten, welche durch Dritte bearbeitet werden sollen und erstellen falls nötig die Risikovorprüfung sowie die DSFA. Auf Basis der so erstellten Dokumentation dokumentieren potentielle Dritte, wie sie die Datenschutzvorgaben bezüglich der Daten der Durchführungsstelle einhalten (Grundschutz und allenfalls erweiterte ISDS Dokumentation)
2.15.2	Bei der Verwendung von M365, wobei ein Vertrag mit der Firma Microsoft als Dritte eingegangen wird, sind generell folgende Punkte zu beachten: • Grundsätzlich dürfen M365 Daten in der Cloud nur verschlüsselt gespeichert werden. Durch die von Microsoft standardmässig implementierte Verschlüsselungsfunktion, welche dem aktuell gültigem Industriestandard entspricht, kann M365 ohne weitere Massnahmen verwendet werden. • Es ist durch die Durchführungsstellen bei der Initialisierung zwingend ein Tenant (Speicherplatz) in der Schweiz zu wählen • Es muss jeweils eine Multi-Factor Authentication (MFA[10]) implementiert sein (für Zugriffe von ausserhalb der Organisation sowie über das Internet) • Die jeweilige Durchführungsstelle muss sicherstellen, dass die möglichen Risiken analysiert, bewertet und entsprechende		

[10] Microsoft MFA: https://learn.microsoft.com/de-de/entra/identity/authentication/concept-mfa-howitworks

	Massnahmen ergriffen wurden. Dies betrifft insbesondere die Bearbeitung und Speicherung von besonders schützenswerten Personendaten, welche die folgenden Massnahmen erfordert: • Erstellung einer Schutzbedarfsanalyse • Erstellung einer Risiko-Vorprüfung • Falls nötig, Erstellung einer Datenschutz-Folgen-Abschätzung • Erstellung von IKT-Grundschutz • Falls nötig, Erstellung von Risikoanalyse und ISDS-Konzept Details zu den Analysen und Bewertungen finden sich in Anhang 3 und 4. Falls die getroffenen Schutzmassnahmen und Risikominderungen eine Bearbeitung & Speicherung der Daten in der Cloud zulassen, können diese mit den M365 Applikationen bearbeitet und gespeichert werden. Vorbehalten bleibt die Bearbeitung und Speicherung von klassierten Daten gemäss Art 18, 19 und 20 ISV, für welche gemäss Art 2 ISV die Cloud Prinzipien[11] der Bundesverwaltung gelten (siehe I. **Zuweisung zu einer Schutzgruppe**) Zudem können kantonale Vorschriften die Verwendung von M365 einschränken, ungeachtet der vorliegenden Weisung. Die Verwendung von Microsoft Exchange Online ist im Rahmen der oben beschriebenen Limitationen wie Analyse und Bewertung für besonders schützenswerte Personendaten möglich. Der Zugriff auf Exchange Online von ausserhalb der Organisation, respektive über das Internet, muss mittels einer MFA-Lösung abgesichert sein. Für den Versand von besonders schützenswerten Daten muss zudem zwingend eine entsprechende Verschlüsselungstechnologie nach Stand der Technik eingesetzt werden. (Beispielsweise IncaMail oder gleichwertig) Eine Abhängigkeit von Microsoft-Cloud-Diensten sowie anderen Cloud-Diensten ist mit Risiken verbunden. Die Durchführungsstellen entwickeln eine Austrittsstrategie und dokumentieren Massnahmen, um im Notfall (beispielsweise einer Nichtverfügbarkeit von Microsoft Cloud Services) handlungsfähig zu bleiben.		
2.16	**2.16 Management von Informationssicherheitsvorfällen** Der ISB der Durchführungsstellen stellt sicher, dass Meldungen über Sicherheitsvorfälle in Zusammenhang mit Informationssystemen adäquat bearbeitet, dokumentiert und ausgewertet werden, um die Eintrittswahrscheinlichkeit oder Auswirkungen von künftigen Vorfällen zu minimieren. Er verfügt über einen vorbereiteten Reaktions- und Kommunikationsplan für Sicherheitsvorfälle und stellt damit sicher, dass die geeigneten	A.5.24 - A.5.28, A.6.8	

[11] Siehe dazu die Cloud Webseite der Bundesverwaltung: https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html

	Massnahmen durch die zuständigen Personen getroffen werden (siehe Beispiel in Anhang 2).		
2.17	**2.17 Aufrechterhaltung der Informationssicherheit (Business Continuity Management BCM)** Die Durchführungsstellen verfügen - entsprechend des Bedarfs ihrer IS-Schutzobjekte (vgl. Rz 2.8.2 und 2.8.3) - über getestete Wiederanlauf-Verfahren um bei Störfällen und Katastrophenfällen den Betrieb der geschäftskritischen IKT-Systeme aufrechtzuerhalten und wiederherzustellen.	A.5.29, A.5.30, A.8.14	
2.18	**2.18 Richtlinienkonformität** Die Durchführungsstellen stellen sicher, dass die mit ihrem internen Kontrollsystem, Qualitätsmanagement oder Risikomanagement (vgl. auch Rz 2.3) erkannten Mängel in Zusammenhang mit den Informationssystemen behoben werden, unabhängig davon ob diese bereits in einer aufsichtsrechtlichen Revision festgestellt worden sind.	A.5.31-A.5.34, A.5.35, A.5.36, A.8.8	

Anhang

Anhang 1: Rechtsbezüge zum Thema Informationssicherheit

1. Nationale Rechtsquellen

Die rechtlichen Grundlagen für die Informationssicherheit (und die dazugehörigen Themen Datenschutz und Datensicherheit) finden sich in unterschiedlichen Rechtsquellen.

A. Auf Bundesebene

1. Die Bundesverfassung garantiert mit Artikel 13 Abs. 2 den Schutz vor Missbrauch der persönlichen Daten und verpflichtet in Artikel 35 letztlich die Durchführungsstellen dazu, dass sie ihren Anteil an die Verwirklichung dieses Grundrechts beitragen.
2. Das **formelle Datenschutzgesetz** (DSG, SR 235.1) mit der Verordnung DSV (SR 235.11)
   - reguliert formelle Aspekte (Begriffe wie Personendaten, besonders schützenswerte Personendaten, Profiling etc.)
   - gibt Einschränkungen für die Bearbeitung und Bekanntgabe von Personendaten vor (Rechtmässigkeit, Verhältnismässigkeit, Zweckbindung, Datenrichtigkeit etc.),
   - garantiert dem Individuum gewisse Rechte in Bezug auf Daten (Auskunftsrecht),
   - verlangt nach „organisatorisch-technischen“ Mitteln in Bezug auf die Datensicherheit (Vertraulichkeit, Integrität, Verfügbarkeit).
3. Die **sozialversicherungsrechtliche Spezialgesetzgebung**
   - ermöglicht mit ihren Erlaubnisnormen (im Verhältnis zum DSG) erst die Bearbeitung von besonders schützenswerten Personendaten (und ein Profiling) in den Sozialversicherungen und den für den Einsatz von Informationssystemen nötigen Datenfluss
   - stellt auch die vorliegenden Anforderungen für die Informationssysteme in technischer und organisatorischer Hinsicht auf
   - gewährt (auch in Verbindung mit dem VwVG [172.021]) gewisse verfahrensbezogene und individuelle Informationsrechte (z.B. Akteneinsicht)
4. Soweit es sich um Informationssysteme von Bundesbehörden (z.B. der ZAS) handelt, gelten zahlreiche weitere Vorschriften (RVOG SR 172.10, VDTI SR 172.010.58, Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee (Informationssicherheitsverordnung, ISV) und weitere Vorgaben des nationalen Zentrums für Cybersicherheit NCSC[2]). Mit Inkrafttreten des Informationssicherheitsgesetzes vom 18. Dezember 2020 (ISG)[12] kam eine zusätzliche Regulierung dazu.

B. Auf kantonaler Ebene

Sowohl für die Informationssicherheit wie für den Datenschutz können auch kantonale Regeln massgebend sein.

[12] BBl **2020** 9975

C. Geltung des DSG für die Durchführungsstellen

In Bezug auf den Geltungsbereich ist festzuhalten, dass die Durchführungsstellen

- alle Normen aus der Sozialversicherungsgesetzgebung anwenden müssen. Das DSG erfasst neben den Durchführungsorganen, die der Bundesverwaltung angehören, auch verbandlich organisierten Durchführungsstellen) und sie sind den Bundesorganen gleichgestellt;
- als Durchführungsstellen der Kantone der kantonalen Datenschutzgesetzgebung unterstehen.

2. ISO-Normen und ihr Stellenwert

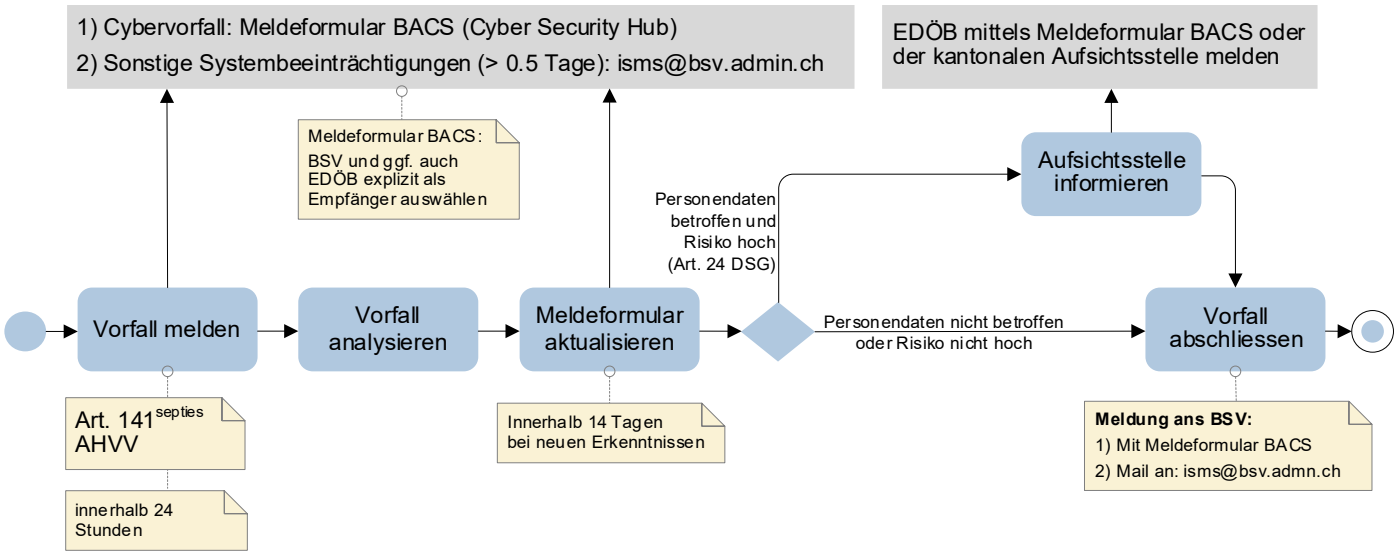
Die Internationale Organisation für Normung (ISO) ist die internationale Vereinigung von Normungsorganisationen und erarbeitet internationale Normen. ISO 27001 und 27002 betreffen die Informationstechnik, bzw. die IT-Sicherheitsverfahren. Sie stellen das Informationssicherheits-Management ins Zentrum. Definiert werden insbesondere die Anforderungen, die ein solches Management-System erfüllen muss. Dabei geht es immer um Ziele und Massnahmen. Diese sind fortlaufend nummeriert. In der Folge steht sozusagen ein Referenz-Nummern-System zur Verfügung.
Da es sich bei Informationstechnik- und –sicherheit nicht um ein national beschränktes Thema handelt, stützen sich weltweit Handelsunternehmen, staatliche Organisationen und Non-Profitorganisationen auf diese Normen ab. In der Schweiz hat dies zur Folge, dass Inhalte der ISO-Normen in die Gesetzgebung und deren Umsetzung einfliessen.

Als Beispiele seien erwähnt

5. dass die Vorgaben IKT-Grundschutz in der Bundesverwaltung auf die ISO-Standards verweisen
6. dass die Zertifizierung nach Artikel 13 DSG (welche z.B. für die Datenannahmestellen Krankenversicherer gemäss Art. 59a Abs. 6 KVV[13] obligatorisch ist) insbesondere davon abhängt, ob die ISO-Normen 27001 erfüllt sind (vgl. Ziffer 4 der Richtlinien über die Anforderungen an ein Datenschutzmanagementsystem vom 19. März 2014). Die Richtlinien über die Anforderungen an ein Datenschutzmanagementsystem und deren Anhang stellen zwischen den nationalen Datenschutzvorschriften (DSG und DSV), welche thematisch mit den ISO-Normen übereinstimmen, und der Nummerierung der ISO-Normen einen Konnex her, indem sie auf das ISO-Nummern-System abstellen (vgl. insbes. Ziffer 4 der Richtlinie und Bst. g des Anhangs zum Thema Datensicherheit nach Artikel 8 DSG). Zusätzliche auf rein nationaler Gesetzgebung beruhende Massnahmen werden explizit analog zu ISO 27002 strukturiert.

[13] Verordnung über die Krankenversicherung vom 27. Juni 1995, SR 832.102

Anhang 2: Meldeprozess Sicherheitsvorfall



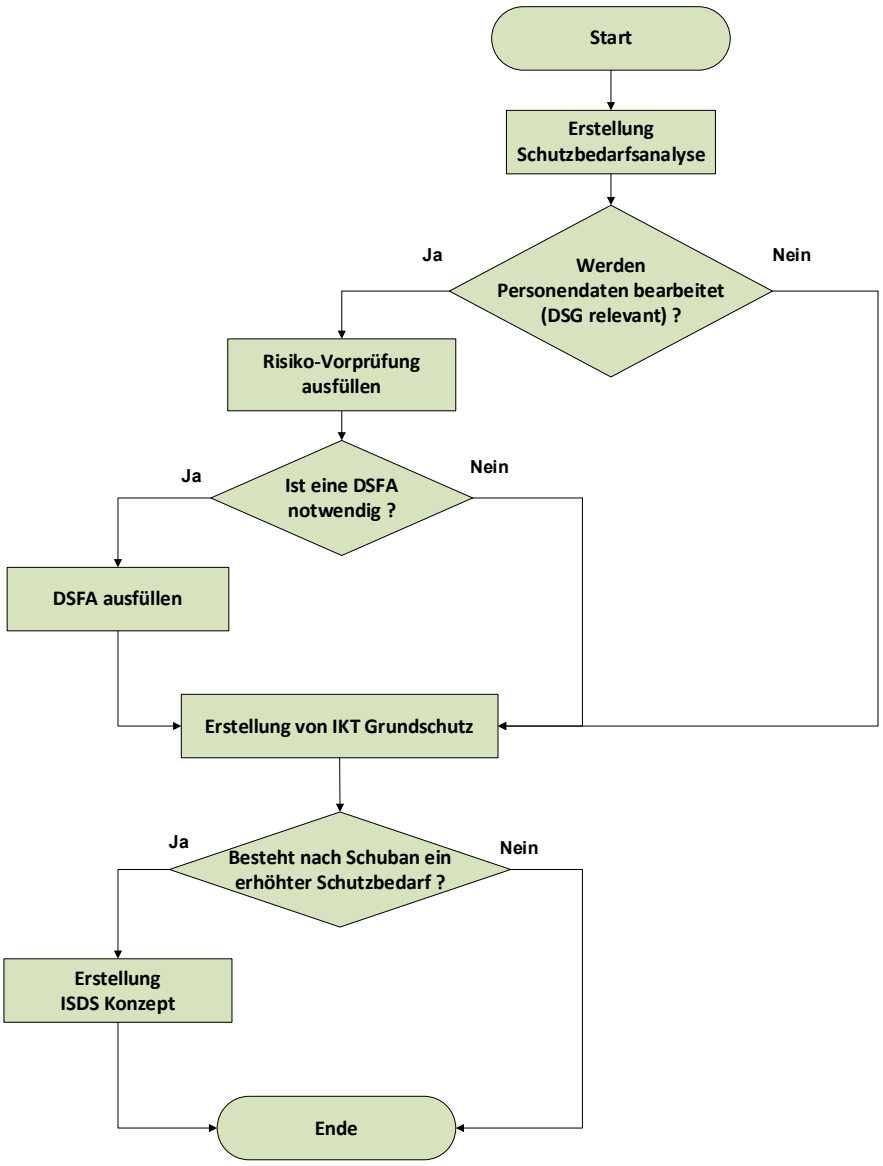
Anhang 3 ISDS-Basisdokumentation

Für jedes Schutzobjekt sind mindestens die Schutzbedarfsanalyse sowie der IT-Grundschutz auszufüllen. Falls erforderlich, sind darüber hinaus eine Risikovorprüfung sowie gegebenenfalls eine Datenschutz-Folgenabschätzung zu erstellen.

Links zu den Mustervorlagen der zu erstellenden Dokumentationen siehe Anhang 6:

- Risikovorprüfung
- Datenschutz-Folgenabschätzung
- Schutzbedarfsanalyse

Das Resultat der Schutzdebarfsanalyse ist eine Einstufungsbeurteilung des Informatikschutzobjektes oder des Projektes. Falls ein erhöhter Schutzbedarf festgestellt wird, muss zusätzlich zur Schutzbedarfsanalyse sowie dem IT-Grundschutz auch ein ISDS Konzept erstellt werden. Das folgende Diagramm erläutert diese Regelung:



A. Leitfaden zur Abklärung der rechtlichen Rahmenbedingungen nach Rz 2.8.2, Bst. a

Allgemeine Vorbemerkungen / Erläuterung

Jede Durchführungsstelle ist Organ einer bundesrechtlich geregelten Sozialversicherung, und insofern ist sie zur Ausübung der gesetzlich vorgesehenen Aufgabe berechtigt und verpflichtet (Legalitätsprinzip). Als Grundlage ihres Handelns dient das jeweilige Spezialgesetz (AHVG, IVG etc.). Setzt sie zur Aufgabenerfüllung Informationssysteme ein, kommen aus anderen Bereichen als aus dem Spezialgesetz Rechtseinflüsse hinzu. Einesteils gilt das ATSG – beispielsweise für die Amts- und Verwaltungshilfe (Art 32 ATSG), die Schweigepflicht (Art. 33 ATSG) und den elektronischen Datenaustausch (Art. 76a ATSG). Andererseits sind Vorschriften zur Informationssicherheit bzw. zum Datenschutz und zur Datensicherheit aus dem DSG, der DSV oder aus der kantonalen Gesetzgebung zu beachten. Diese wirken sich regelmässig auf den Umgang mit Daten und deren Sicherheit aus:

- In der 1. Säule tätige Bundesorgane (also z.B. die Eidg. Ausgleichskasse oder die Schweizerische Ausgleichskasse der AHV) sowie Durchführungsstellen, die vom DSG als «Bundesorgane» betrachtet werden (also alle Durchführungsstellen, die nicht kantonal sind) müssen beispielsweise die Vorschriften zum Verzeichnis ihrer Bearbeitungstätigkeiten (Art. 12 DSG), zur Erstellung einer Datenschutz-Folgenabschätzung (Art. 22 DSG), zur Meldung von Verletzungen der Datensicherheit (Art. 24 DSG), zur Ernennung eines Datenschutzberaters (Art. 25 DSV) sowie zu der Protokollierung der Personendaten (Art. 4 DSV) einhalten.
- Soweit die kantonalen Datenschutzgesetzgebungen vergleichbare Regelungen kennen, haben die kantonalen Durchführungsstellen zu prüfen welche Verpflichtungen sich daraus für sie ergeben.

Leitfaden zu den rechtlichen Rahmenbedingungen und zur Abklärung der Rechtskonformität der Datenbearbeitung

#	Fragestellung/Thema	Rechtliche Grundlage	Konsequenz, Beispiel
1	Einhaltung der Grundsätze des Datenschutzes: • Rechtmässigkeit der Bearbeitung nach Art. 6 Abs. 1 DSG, • Verhältnismässigkeit und Zweckmässigkeit der Datenbeschaffung und Datenbearbeitung, unter Einhaltung des Grundsatzes von Treu und Glauben Art. 6 Abs. 2 und 3 DSG	Artikel 49b AHVG bzw. neu Art. 49f - AHVG erlaubt den Durchführungsorganen die Bearbeitung von Personendaten, einschliesslich besonders schützenswerter Daten und Profiling, soweit dies für die gesetzlich übertragenen Aufgaben nötig ist. Für alle andern Durchführungsorgane gilt diese Erlaubnis ebenfalls (Art. 66a IVG bzw. neu 66 E-IVG, Art. 25 FamZG, Art. 25 Abs. 2 FLG, Art. 29 EOG, Art. 26 ELG). Im Tätigkeitsbereich der Durchführungsstellen genügt die ausreichende rechtliche Grundlage regelmässig (DSG 34ff.)	In der ISDS-Basis-Dokumentation ist zu prüfen: ob das Informationssystem tatsächlich für die Erfüllung einer gesetzlich übertragenen Aufgabe verwendet wird und geeignet und angemessen ist, um die Aufgabe zu erfüllen. **Rechtmässigkeit**: Angaben zu den gesetzlichen Grundlagen zur Datenbearbeitung (z. B. Art. 49b AHVG) **Zweckmässigkeit**: Welcher gesetzlichen Aufgabe wird gedient (Gesetz oder VO)? **Verhältnismässigkeit:** Könnte das gleiche Ziel mit einer weniger intensiven Bearbeitung von Daten erreicht werden in derselben Qualität? **Treu und Glauben:** Wenn eine betroffene Person keinesfalls damit rechnen muss, dass ihre Daten im vorliegenden Fall bearbeitet werden, ist der Grundsatz verletzt.

#	Fragestellung/Thema	Rechtliche Grundlage	Konsequenz, Beispiel
			Beispiel Einordnung E-Mail Applikation einer Verbandsausgleichkasse in der ISDS-Basis-Dokumentation: E-Mails werden regelmässig von Versicherten zur Einholung von Auskünften bzw. zur Beratung im Sinne von Art. 27 ATSG benutzt. Die verwendeten Daten können besonders schützenswert sein. Diesem Umstand ist bei der Klassifizierung (vgl. Schema Bst. C und D) in technischer Hinsicht Rechnung zu tragen. Aufgrund von Art. 49a (künftig 49f AHVG) ist die Bearbeitung der Daten **grundsätzlich rechtmässig.** Soweit in E-Mails nur die im Einzelfall relevanten Daten verwendet werden**, ist die Zweckmässigkeit und Verhältnismässigkeit und der Grundsatz von Treu und Glauben gewährleistet.**
2	Datenzufluss (Datenbeschaffung) und Datenabfluss (Datenbekanntgabe) sowie Verschwiegenheitspflicht	Sowohl die Beschaffung von Daten wie deren Bekanntgabe fallen unter besondere rechtliche Einschränkungen, und jede Beschaffung beruht ihrerseits auf einer Bekanntgabe. Formal ist die Datenbekanntgabe auch eine Bearbeitung (Art. 5 Bst. d DSG). Die Datenbeschaffung wird durch das DSG zwar eingeschränkt (in Art. 6 Abs. 3, Art. 19), indessen sind diese Einschränkungen bei einer entsprechenden gesetzlichen Grundlage obsolet (inbes. Art. 20 DSG). Im Rahmen der Mitwirkungs- und Meldepflichten wird in den Sozialversicherungsgesetzen jedoch oft ein Teil des Datenzuflusses reglementiert. Darüber hinaus bestehen aufgrund von Regelungen zu einzelnen Informationssystemen automatisierte Meldungen (z. B. Zivilstandsmeldungen an die AHV). Schliesslich garantiert das ATSG die Amts- und Verwaltungshilfe in Einzelfällen. Für die Datenbekanntgabe sieht das DSG in Artikel 36 Absatz 1 vor, dass wiederum eine gesetzliche Grundlage (wie für die Bearbeitung der Daten) vorgesehen sein	In der ISDS-Basis-Dokumentation ist zu prüfen: ob der Datenzufluss und Datenabfluss rechtlich zulässig ist. Bei Informationssystemen, welche einen automatischen Zu- oder/und Abfluss von Daten vorsehen ist die rechtliche Grundlage zu ermitteln und zu dokumentieren. **Beispiel Einordnung E-Mail Applikation einer Verbandsausgleichskasse in der ISDS-Basis-Dokumentation:** Die E-Mails werden ausschliesslich für die Übermittlung von Daten in Einzelfällen genutzt. Die Frage der rechtlichen Zulässigkeit des Datenzu- und abflusses muss vom entsprechend ausgebildeten Nutzer geprüft werden. Es ist sicherzustellen, dass die Nutzer diese Ausbildung erhalten und allenfalls mit technischen und organisatorischen Massnahmen die die Identität des Empfängers von Daten klären können.

#	Fragestellung/Thema	Rechtliche Grundlage	Konsequenz, Beispiel
		muss. Die einzelnen Sozialversicherungsgesetze regeln die Datenbekanntgabe in eigenen Katalogen zur Datenbekanntgabe jeweils einlässlich, und unterscheiden dabei auch, ob es sich um Datenabflüsse im Einzelfall oder um Massenverfahren handelt. Dies regelmässig als Abweichung von der in Art. 33 ATSG vorgesehenen generellen Schweigepflicht.	
3	Datenrichtigkeit und Datenberichtigung (Art. 6 Abs. 5 und 41 Abs. 2 DSG)	Das DSG verlangt bei der Datenbearbeitung • eine Vergewisserung über die Richtigkeit der Daten • angemessene Massnahmen für die Richtigkeit der Daten • die Berichtigung unrichtiger Daten	In der ISDS-Basis-Dokumentation ist zu analysieren, wie viel Gewähr für die Richtigkeit der Daten besteht und welche Plausibilisierungsmöglichkeiten und Prüfmethoden vorhanden sind und wie notwendige Korrekturen erfolgen. Dafür sind Prozesse zu definieren. **Beispiel Einordnung E-Mail Applikation einer Verbandsausgleichskasse in der ISDS-Basis-Dokumentation:** Die in E-Mails verwendeten Daten sind einzelfallbezogen und sind systemisch nicht überprüfbar. Es liegt in der Verantwortung des Nutzers, soweit notwendig, eine Plausibilisierung durch Abklärung im Einzelfall vorzunehmen. Es ist sicherzustellen, dass die Nutzer diese Ausbildung erhalten und allenfalls mit technischen und organisatorischen Massnahmen die richtigen Daten verwenden.
4	Auskunftsrecht (Art. 25 DSG und Art. 16 DSV)	Art. 25 DSG postuliert ein Auskunftsrecht jeder Person. Dieses verpflichtet den Verantwortlichen, Auskunft zu geben. Eingeschränkt wird dieses Auskunftsrecht durch Art. 26 und 27 DSG. Zudem kann die Person verlangen, dass die Daten herausgegeben werden, wiederum unter gewissen Einschränkungen (Art. 28 und 29 DSG) Bearbeiten mehrere Verantwortliche Personendaten gemeinsam, so kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen.	In der ISDS-Basis-Dokumentation ist zu analysieren, wie sämtliche einer Person zuzuordnenden Daten im Informationssystem eruierbar sind. Der Prozess für die Behandlung von Auskunftsbegehren ist zu dokumentieren. In der ISDS-Basis-Dokumentation ist zu klären, ob im Informationssystem Daten über die Gesundheit enthalten sein können, welche – mit Einwilligung der betroffenen Person - über die von ihr bezeichnete - Gesundheitsfachperson mitgeteilt werden (Art. 25 Abs. 3 DSG).

#	Fragestellung/Thema	Rechtliche Grundlage	Konsequenz, Beispiel
			Beispiel Einordnung E-Mail Applikation einer Verbandsausgleichskasse in der ISDS-Basis-Dokumentation: Im Rahmen der ISDS-Basis-Dokumentation ist sicherzustellen, dass auf die E-Mails einer bestimmten Person zugegriffen werden kann. Dies kann auch über die Definition eines Prozesses bei einem andern Informationssystem wie einer Geschäftsverwaltung sichergestellt werden. In der SSDS-Basis-Dokumentation zur E-Mail-Applikation ist darauf zu verweisen.
5	Klärung der Aufnahme in das Verzeichnis bzw. Meldung bei einer Behörde des Datenschutzes	In der 1. Säule tätige Bundesorgane (also z. B. die Eidg. Ausgleichskasse oder die Schweizerische Ausgleichskasse der AHV) sowie Durchführungsstellen, die vom DSG als «Bundesorgane» betrachtet werden (also alle nicht kantonalen Durchführungsstellen) müssen die Vorschriften zum Verzeichnis ihrer Bearbeitungstätigkeiten einhalten und die Verzeichnisse dem EDÖB melden (Art. 12 DSG).	
6	Datenschutzberater	Die Durchführungsstellen ernennen einen Datenschutzberater, welcher den Verantwortlichen bei der Erstellung der Datenschutz-Folgenabschätzung berät und deren Ausführung überprüft (Art. 25 sowie Art. 26 Abs. 2 Bst. a Ziffer 2 DSV). Der Datenschutzberater kann Kritikpunkte im Rahmen der Datenschutz-Folgenabschätzung formulieren. Diese Kritikpunkte sind integraler Bestandteil der Datenschutzfolgeabschätzung. Der Verantwortliche stellt dem Datenschutzberater die notwendigen Ressourcen zu Verfügung und gewährt ihm Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten, die dieser zur Erfüllung seiner Aufgaben benötigt (Art. 23 Bst. a und b DSV). Mehrere Bundesorgane können gemeinsam einen Datenschutzberater bezeichnen. Kleinere Bundesorganen oder De-	

#	Fragestellung/Thema	Rechtliche Grundlage	Konsequenz, Beispiel
		partemente mit zentralisierter Organisationsstruktur nutzen so ressourceneinsparende Synergien.	
7	Protokollierung	Das verantwortliche Bundesorgan und sein Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten. Die Protokollierung muss Aufschluss darüber geben über die Identität der Person, die die Bearbeitung vorgenommen hat, die Art, das Datum und die Uhrzeit der Bearbeitung sowie gegebenenfalls die Identität des Empfängers der Daten (Art. 4 Abs. 2 und 4 DSV). Gemäss Art. 4 DSV muss zur Sicherstellung der Nachvollziehbarkeit der Bearbeitung von Personendaten auch der Vorgang des «Lesens» innerhalb der Datenbearbeitungssysteme protokolliert werden. Die gesetzliche Pflicht zum Protokollieren von Lesezugriffen besteht unabhängig vom (wahrgenommen) Nutzen und unabhängig von der allfälligen Performance-Einbusse, die durch die Protokollierung verursacht wird. In diesem Zusammenhang gelten Übergangsbestimmungen. Solange das Datenbearbeitungssystem ohne Erweiterung des Funktionsumfangs und weiterhin wie beim Inkrafttreten der DSV (1.9.2023) betrieben wird, gilt Art. 4 Abs. 2 DSV noch nicht. Reine Sicherheitsupdates ändern auch nichts daran. Sobald funktionale Erweiterungen, welche Auswirkungen auf die Bearbeitung von Personendaten haben (wie z. B. die Ablösung von Modulen) fällt es nicht unter die Übergangsbestimmung und eine Protokollierung gemäss Art. 4 Abs. 2 DSV hat zu erfolgen. Die Protokolle müssen während mindestens einem Jahr getrennt vom System, in welchem die Personendaten bearbeitet	Aus Sicht der Datensicherheit hilft die Auswertung der Protokolldaten die Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit sicherzustellen. Es können Abweichungen vom normalen Nutzungsverhalten, potenzielle Sicherheitsvorfälle – beispielsweise der Missbrauch eines Systems – sowie gezielte Angriffe festgestellt werden.

#	Fragestellung/Thema	Rechtliche Grundlage	Konsequenz, Beispiel
		werden, aufbewahrt werden. Sie dürfen ausschliesslich den Organen und Personen zugänglich sein, denen die Überprüfung der Anwendung der Datenschutzvorschriften oder die Wahrung oder Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegt, und dürfen nur für diesen Zweck verwendet werden (Art. 4 Abs. 5 DSV).	

B. Muster zur Klassifizierung der Verfügbarkeitsanforderungen (nach Rz 2.8.2, Bst. b)

#	Fragestellung bzw. Anforderung	Kriterien	Schutzbedarf erhöht? > erweiterte ISDS-Dokumentation nach Rz 2.8.3 nötig? *(statt Dokumentation, insbesondere Risikoanalysen und Sicherheitsanforderungen)*
1	Max. zulässige Ausfalldauer pro Ausfall	Ausfalldauer max. 2 Stunden	**ja**
		Ausfalldauer grösser 2 Stunden	**nein**
2	Maximaler Datenverlust pro Ausfall	Datenverlust kleiner 1 Stunde	**ja**
		Datenverlust grösser 1 Stunde	**nein**
3	Geschäftsrelevanz/geschäftskritischer Prozess? (Aufgrund von Rz 2.8.2 Ziff. 2 Bst. b): müssen für das Schutzobjekt Katastrophen-Vorsorge-Massnahmen (K-Vorsorge) getroffen werden?	Katastrophen-Vorsorge erforderlich	**ja**
		keine K-Vorsorge erforderlich	**nein**

C. Leitfaden zur Vertraulichkeitsanforderungen (nach Rz 2.8.2, Bst. c)

In der ISDS-Basis-Dokumentation sind die Daten zu klassifizieren, um einen allenfalls erhöhten Schutzbedarf und die Notwendigkeit einer erweiterten Dokumentation (Rz 2.8.3) zu eruieren.

Fragestellung bzw. Anforderung	**Kriterien**	**Schutzbedarf erhöht? > erweiterte ISDS-Dokumentation nach Rz 2.8.3 nötig?** *(statt Dokumentation , insbesondere Risikoanalysen und Sicherheitsanforderungen)*	**Schutzmassnahmen**
Werden Daten gemäss Datenschutzgesetzgebung bearbeitet? Wenn ja, welche Art von Personendaten sind betroffen?	keine Personendaten	nein	Umschreibung der vorhandenen Basis-Schutzmassnahmen
	Personendaten	nein	Umschreibung der vorhandenen Schutzmassnahmen
	besonders schützenswerte Personendaten (Art. 5 Bst. c DSG? und /oder Profiling (automatisierte Bewertung; vgl. Art. 5 Bst. f DSG)?[14] Wenn ja Profiling: mit hohem Risiko (vgl. Art. 5 Bst. g DSG?)	Ja Ja Ja	Umschreibung der besonderen Schutzmassnahmen
In welcher Klassifizierungsstufe befinden sich die Daten des Schutzobjektes?	Öffentlich Intern Vertraulich Streng vertraulich	Nein Nein Ja Ja	Die Klassifizierung sollte in einer Folgeversion definiert werden.

[14] Profiling: Gemäss Botschaft des Bundesrates zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse vom 15. September 2017 wird unter Profiling folgendes verstanden: «Das *(terminologisch nicht mehr gesetzlich definierte)* Persönlichkeitsprofil ist das Ergebnis eines Bearbeitungsprozesses und erfasst damit etwas Statisches. Hingegen umschreibt das Profiling eine bestimmte Form der Datenbearbeitung, mithin einen dynamischen Prozess. Darüber hinaus ist der Vorgang des Profilings auf einen bestimmten Zweck ausgerichtet…. Der Begriff des Profilings wird aufgrund der Stellungnahmen in der Vernehmlassung inhaltlich an die europäische Terminologie angepasst und erfasst nun insbesondere nur noch die automatisierte Bearbeitung von Personendaten. So ist Profiling definiert als die Bewertung bestimmter Merkmale einer Person auf der Grundlage von automatisiert bearbeiteten Personendaten, insbesondere um die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, das Verhalten, die Interessen, den Aufenthaltsort oder die Mobilität zu analysieren oder vorherzusagen. Diese Analyse kann beispielsweise erfolgen, um herauszufinden, ob eine Person für eine bestimmte Tätigkeit geeignet ist. Ein Profiling ist mit anderen Worten dadurch gekennzeichnet, dass Personendaten automatisiert ausgewertet werden, um auf der Grundlage dieser Auswertung, ebenfalls in automatisierter Weise, die Merkmale einer Person zu bewerten. Ein Profiling liegt somit nur vor, wenn der Bewertungsprozess vollständig automatisiert ist. Als automatisierte Auswertung ist jede Auswertung mit Hilfe von computergestützten Analysetechniken zu betrachten. Dazu können auch Algorithmen verwendet werden, aber deren Verwendung ist nicht konstitutiv für das Vorliegen eines Profilings. Vielmehr ist lediglich verlangt, dass ein automatisierter Auswertungsvorgang stattfindet; liegt hingegen lediglich eine Ansammlung von Daten vor, ohne dass diese ausgewertet werden, erfolgt noch kein Profiling. Die automatisierte Bewertung erfolgt insbesondere, um bestimmte Verhaltensweisen dieser Person zu analysieren oder vorherzusagen. Das Gesetz nennt beispielhaft einige Merkmale einer Person wie die Arbeitsleistung, die wirtschaftliche Lage oder die Gesundheit,»

D. Leitfaden zur Klassifizierung Integritäts- und Nachvollziehbarkeitsanforderungen (nach Rz 2.8.2, Bst. d)

Klassifizierungen	Beschreibung	Massnahmen	erweiterte ISDS-Dokumentation nach Rz 2.8.3 nötig?
Normale Integrität	Für Bereiche der ICT-Umgebung, die in der Stufe „Normale Integrität“ eingeordnet werden, sind keine besonderen Massnahmen zur Wahrung der Integrität vorzusehen.	Die allgemeinen Massnahmen für Geräte und Betriebsmittel (Rz 2.11.2 und 2.12.2) müssen die «normale Integrität» gewährleisten.	Nein
Gesicherte Integrität	Für Bereiche der ICT-Umgebung die in der Stufe „Gesicherte Integrität“ eingeordnet sind, müssen Vorkehrungen zum Schutz gegen Veränderungen durch Unbefugte implementiert sein.	In Rahmen der ISDS-Basis-Dokumentation wird geprüft, wie stark die Auswirkungen von fehlerhaften Änderungen an Informationssystemen (neuer Release) sind. Kriterien für die Stärke der Auswirkungen sind z.B. Beeinträchtigung der Aufgabenerfüllung, negative Aussenwirkungen, finanzielle Auswirkungen für die Versicherung.	Ja Um die Korrektur von Auswirkungen möglicher Fehler zu ermöglichen, sind – je nach Stärke der möglichen Auswirkungen – die Änderungen intensiv zu testen und zu dokumentieren – und so durchzuführen, dass sie den Anforderungen an Projekte entsprechen, und insbesondere den dafür geltenden Qualitätsmanagement- und Risikomanagementvorgaben entsprechen (vgl. Rz 2.5 Punkt 1 und Rz 2.14 Abs. 3).
Prüfbare Integrität	Für Bereiche der ICT-Umgebung die in der Stufe „Prüfbare Integrität“ eingeordnet werden, müssen zusätzlich Funktionalitäten implementiert sein, welche Verletzungen der Integrität feststellen und festhalten.		Definitive Fassung folgt später.
Signierte Integrität	Für Bereiche der ICT-Umgebung die in der Stufe „Signierte Integrität“ eingeordnet sind, müssen zusätzlich digitale Signaturen eingesetzt werden.		Definitive Fassung folgt später.

E. Datenhaltung

In Bezug auf die Datenhaltung sind wenigstens folgende Tatsachen zu beschreiben:

- Geografische Angaben (Ort in der Schweiz, mit Adresse)
- Verantwortliche Organisation
- Nennung des ISB

F. Beschreibung des Schutzobjekts / Projekts

- Ziel und Zweck
- Unterstütze Geschäftsprozesse
- Art und Umfang der Daten
- Benutzer
- Mengengerüst der Benutzer

G. Verzeichnispflicht/Meldepflicht

Grundsätzlich besteht nach Rz 2.8.1 für alle Informationssysteme eine Inventarpflicht. Darüber hinaus gilt nach Artikel 12 DSG eine Verzeichnungspflicht. Letztere betrifft die Bundesorgane/Durchführungsstellen (also alle, ausser die kantonalen Durchführungsstellen), ebenso wie die Meldepflicht an den EDÖB. Für die kantonalen Durchführungsstellen gilt eine allfällige kantonale Verzeichnis- und Meldepflicht. Im Rahmen der ISDS-Basisdokumentation ist festzustellen, ob und welche Verzeichnis- und Meldepflichten bestehen und es ist zu dokumentieren, wie diese Pflichten erfüllt werden.

H. Notwendigkeit einer Datenschutz-Folgenabschätzung

Gemäss Art. 22 DSG ist eine Datenschutz-Folgenabschätzung ein Instrument, um Risiken zu erkennen und zu bewerten, welche für die betroffene Person durch den Einsatz bestimmter Datenbearbeitungen entstehen können. Auf der Basis dieser Abschätzung sollen gegebenenfalls angemessene Massnahmen definiert werden, um diese Risiken für die betroffene Person zu bewältigen.

In der ISDS-Basisdokumentation geht es in erster Linie darum, festzustellen, ob eine Notwendigkeit dafür besteht.

Die Regulierung des DSG (Art. 22) gilt auch hier für die Durchführungsstellen (ausser die kantonalen Durchführungsstellen). Für die kantonalen Durchführungsstellen gilt eine allfällige kantonale Pflicht für die Datenschutz-Folgenabschätzung.

In einem ersten Schritt ist daher in der Basisdokumentation festzuhalten, ob die Normen zur Datenschutz-Folgenabschätzung zum Tragen kommen. **Durchführungsstellen der Kantone** halten anhand der kantonalen Datenschutzgesetzgebung in der Basisdokumentation ihre Abklärungen zur Notwendigkeit einer Datenschutz-Folgenabschätzung fest.

In der ISDS- Basisdokumentation ist – **gestützt auf die übrigen Abklärungen gemäss Rz 2.8.2 Ziffer 2 Bst. a-g** ausdrücklich festzuhalten, ob eine Notwendigkeit für die Vornahme einer Datenschutz-Folgenabschätzung besteht. Entscheidend dabei ist,

- ob eine besonders umfangreiche Bearbeitung besonders schützenswerter Daten erfolgt
- ob neue Technologien verwendet werden
- die beschriebene Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen darstellt (vgl. Art. 22 Abs. 1 bis 3 DSG)
- welche bereits bekannten oder noch zu entwickelnden Massnahmen zum Schutz der Persönlichkeit und der Grundrechte vorgesehen sind.

I. Zuweisung zu einer Schutzgruppe

Die Durchführungsstellen verfügen über eine Definition von Schutzgruppen (in der Regel 3 bis 4), welche dem unterschiedlichen Schutzbedarf Rechnung tragen. Aufgrund der Ergebnisse gemäss Rz. 2.8.2, Ziffer 2 ist abschliessend eine Zuweisung vorzunehmen.

Beispiele für Schutzgruppen und Zuweisungen (nicht abschliessend).

Wichtig: Die untenstehenden Beispiele sind nicht zu verwechseln mit den Klassifizierungsstufen gemäss Art 18-20 ISV. Die Benennung von Schutzgruppen kann nach eigenem Ermessen erfolgen.

Schutzgruppen		Beschreibung / Beispiel	Informationsbeispiele
S1	**öffentlich**	Öffentliche Daten und Informationen	▪ Internetauftritt ▪ Social Media ▪ News- und Presseinformationen
S2	**intern**[15]	Personendaten der Mitarbeitenden und Kunden sowie interne Geschäfts- und Projektdaten	▪ Adressverzeichnis ▪ «nicht-sensible» Personendaten ohne besondere Schutzwürdigkeit
S3	**vertraulich**[16]	Daten im Zusammenhang mit der Unternehmensstrategie, Finanz- und Personaldaten, Kunden- bzw. Versichertendaten (Stammdaten)	▪ Strategiedokumente ▪ Finanzbuchhaltung ▪ Personaldossiers/-dokumente: Bewerbungen, Beurteilungen, Arbeitsverträge, etc. ▪ Netzwerkpläne der Informatik
S4	**streng vertraulich**	Alle hochsensible Personendaten, die nach dem anwendbaren Datenschutzgesetz als besonders schützenswert gelten	Besonders schützenswerte Personendaten wie: ▪ Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten ▪ Gesundheitsdaten ▪ Intimsphäre ▪ Ethnische Zugehörigkeit oder Herkunft ▪ Genetische und biometrische Daten ▪ Daten über Massnahmen der Sozialhilfe ▪ Straf- und Disziplinarverfahren ▪ Lohnpfändung

Die Bundesverwaltung hat in der Informationssicherheitsverordnung[17] ISV die folgenden Klassierungen definiert:

- Intern
- Vertraulich
- Geheim

Speziell im Bereich Cloud-Computing (wozu auch die Verwendung vom M365 gehört) existieren Einschränkungen für die Speicherung und Bearbeitung von Daten der Stufe «Vertraulich» und «Geheim».

Im Gegensatz zu kantonalen Ausgleichskassen KAK sind Verbandsausgleichskassen VAK der ISV unterstellt und bearbeiten daher potentiell Daten gemäss Klassifizierung der Bundesverwaltung. Die nachstehende Matrix verdeutlicht die Unterschiede der Klassifizierung von DSG und ISV und zeigt auf, welche Daten mit M365 und Exchange Online bearbeitet und gespeichert werden dürfen:

[15] Nicht im Sinne von Art. 18 ISV

[16] Nicht im Sinne von Art. 19 ISV

[17] Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee (ISV)

		Klassifizierung gemäss Bundesverwaltung (Art 18, 19, 20 ISV)			
		Nicht klassiert	**Intern**	**Vertraulich**	**Geheim**
Kategorisierung gemäss Art 5 DSG	**Keine Personendaten** ***(Beispielsweise Schutzgruppen S1, S2)***	Erlaubt	Erlaubt	Nicht Erlaubt	Nicht Erlaubt
	Personendaten ***(Beispielsweise Schutzgruppe S3)***	Erlaubt	Erlaubt	Nicht Erlaubt	Nicht Erlaubt
	Besonders schützenswerte Personendaten ***(Beispielsweise Schutzgruppe S4)***	Erlaubt	Erlaubt	Nicht Erlaubt	Nicht Erlaubt

Anhang 4: Erweiterte ISDS-Dokumentation

(nach Rz 2.8.3)

Falls die Schutzbedarfsanalyse einen erhöhten Schutzbedarf des Schutzobjektes ergibt (siehe Prozessdokumentation im Anhang 3), ist die Erstellung eines ISDS Konzepts sowie einer Risikoanalyse notwendig.

Links zu den Mustervorlagen der zu erstellenden Dokumentationen siehe Anhang 6

a. Die Zusammenfassung der relevanten Ergebnisse der ISDS-Basis-Dokumentation

Die Zusammenfassung dient als Ausgangslage für das ISDS-Konzept mit **Risikoanalyse** und erstreckt sich auf die Einstufung des Schutzobjekts hinsichtlich Vertraulichkeit, Verfügbarkeit, Integrität/Nachvollziehbarkeit, Datenhaltung, Beschreibung des Schutzobjekts, Ergebnisse betr. Verzeichnis der Bearbeitungstätigkeiten (gegebenenfalls mit Meldung beim EDÖB bzw. Datenschutzberatung) und betr. Datenschutz-Folgenabschätzung.

b. Sicherheitsrelevante Systembeschreibung

Verdichtete Beschreibung der sicherheitsrelevanten Elemente aus dem System, den Anwendungen, den vorhandenen und bearbeiteten Daten und den dazugehörenden Prozessen.

b.1 Ansprechpartner / Verantwortlichkeiten

Wer	Name
Anwendungsverantwortlicher	
Inhaber der Daten	
Leistungserbringer LE (Systembetreiber)	
Projektleiter Durchführungsstelle	
Ansprechpartner beim LE	
ISB	
Benutzerkreis	
weitere involvierte Stellen	

b.2 Beschreibung des Gesamtsystems

Beschreibung der sicherheitsrelevanten Funktionalitäten wie Zugangssteuerung (vgl. Rz 2.9), Betriebssicherheit (vgl. Rz 2.12) und Leistungen der Dritten (vgl. Rz 2.15). Es können auch Verweise auf entsprechende Dokumentationen gemacht werden (z.B. Netzwerksicherheit- und Dokumentation vgl. 2.13.3).

Die Beschreibung sollte einer unbeteiligten Person einen Überblick verschaffen, gleichzeitig verständlich und nachvollziehbar formuliert sein.

b.3 Beschreibung der zu bearbeitenden Daten

Beschreibung der Daten und Strukturen (z. B. verwendete Datenbank) und Feststellung der Rechtmässigkeit der vorgesehenen Datenbearbeitung gemäss Anhang 4, Bst. A insbesondere:

- Erfüllung einer allfälligen Anmeldepflicht beim Datenschutzbeauftragten des Kantons oder des EDÖB
- Erstellung eines Bearbeitungsreglements

  Hilfe dazu finden Sie im Template «Bearbeitungsreglement» sowei im Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes im Anhang 6.

  Das Bearbeitungsreglement muss die Archivierungsvorschriften des BSV beachten (vgl. WAF)

b.4 Architekturskizze / Kommunikationsmatrix

Das Konzept enthält eine Architekturskizze und eine Kommunikationsmatrix, oder es ist hier auf das entsprechende aktuell gehaltene Dokument zu verweisen.

b.5 Beschreibung der zugrundeliegenden Technik

Beschreibung der verwendeten Techniken wie Serverplattform, Betriebssystem(e), Systemumfeld, verwendete Netzwerke, Kryptographische Funktionen etc. Sie sollen so beschrieben sein, dass es vollständig ist und auch für Unbeteiligte verständlich und nachvollziehbar. Oder es ist hier auf das entsprechende aktuell gehaltene Dokument zu verweisen.

c. Risikoanalyse, Schutzmassnahmen, und Restrisiken

Steht aufgrund der bereits erfolgten Analysen (Risikovorprüfung und/oder Schutzbedarfsanalyse) fest, dass eine Bearbeitung besonders schützenswerter Personendaten erfolgt, muss eine detaillierte Risikoanalyse erstellt werden werden.

Das ISDS Konzept gibt Auskunft über die Restrisiken, die nach einer Risikoanalyse anhand der Excel-Datei vom BACS (zum Download auf der Webseite des BACS) und den berücksichtigten Schutzmassnahmen verbleiben. Die Risikoanalyse berücksichtigt unter anderem das (hohe) Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, das sich ergibt aus:

- der Verwendung neuer Technologie
- dem Umfang der Bearbeitung besonders schützenswerter Personendaten
- der Art, den Umständen und dem Zweck der Bearbeitung der Daten

In der Risikoanalyse werden die relevanten Risikofaktoren mit Blick auf die Konsequenzen bei Verfügbarkeit, Vertraulichkeit, Integrität und Nachvollziehbarkeit beurteilt. Als Ergebnis werden die Risiken aufgelistet und bewertet sowie eine Risikomatrix erstellt.

Datenschutz-Folgenabschätzung (DSFA)

Diese enthält gemäss Gesetz (Art. 22 Abs. 3 DSG):

- eine Beschreibung der geplanten Bearbeitung
- eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen
- die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte

Im Rahmen der DSFA sind folgende Schritte vorzunehmen:

- Beschreibung der geplanten Datenbearbeitung
- Bewertung der Risiken für die Grundrechte der betroffenen Person
- Identifizierung der Massnahmen zum Schutz der Grundrechte
- Bewertung der Auswirkungen der vorgesehenene Massnahmen, um zu beurteilen, ob ein hohes Risiko besteht

Persönlichkeitsschutz (privatrechtlich; Art. 28 ZGB)

Die Persönlichkeit umfasst alle physischen, psychischen, moralischen und sozialen Werte einer Person, die ihr kraft ihrer Existenz zukommen.[18] Damit ergibt sich ein weites Feld für mögliche Verletzungen, und es muss bewertet werden, wie hoch das Risiko ist, dass die betroffenen Personen eine Beeinträchtigung erleiden, und mit welchen Massnahmen letztere allenfalls vermieden werden können.

Beispiel: Risiko, dass Unberechtigte Kenntnis vom Gesundheitsschaden erfahren, was per se bereits eine moralische Beeinträchtigung ist, aber zusätzlich die Chancen auf dem Arbeitsmarkt beeinträchtigt, sollte die Information zu einem möglichen Arbeitgeber gelangen (und zu finanziellem Schaden führt). Mögliche Massnahmen: vor Weiterleitung der Daten an Arbeitgeber wird routinemässig die Einwilligung der betroffenen Person eingeholt.

[18] Fey Marco, in: Baeriswyl Bruno/Pärli Kurt (Hrsg.), Datenschutzgesetz (DSG), Bern 2015, Art. 1 N 16)

Grundrechtsschutz (öffentlichrechtlich)

Die Grundrechte sind in den Artikeln 7-35 der Bundesverfassung umschrieben. Im Zusammenhang mit Informationssystemen ist zu bewerten, wie hoch das Risiko ist, dass Grundrechte als Folge einer Datenbearbeitung beeinträchtigt werden könnten, und mit welchen Massnahmen solche Beeinträchtigungen begegnet werden könnte.

Beispiel: Rechtsgleichheit mit dem Diskriminierungsverbot gemäss Artikel 8 BV:

Risiko, dass Unberechtigte Kenntnis von der Lebensform (z.B. gleichgeschlechtliche Partnerschaft) erhalten, und deshalb Betroffene womöglich Diskriminierung bei der Arbeit zu gewärtigen haben.

Mögliche Massnahmen: vor Weiterleitung der Daten an Arbeitgeber wird routinemässig die Einwilligung der betroffenen Person eingeholt.

Weitere Hilfen/Hinweise

Merkblatt Datenschutz-Folgenabschätzung (DSFA) BSV und Vorlage

Die Risikomatrix

Die detaillierte Risikoanalyse kann anhand der eingebetteten Excel-Datei «DSFA Risikoanalyse» in der DSFA Vorlage vom BSV oder in der Excel-Datei des BACS (zum Download auf der Webseite des BACS) vorgenommen werden. Als Ergebnis der Risikoanalyse sind Schutzmassnahmen zu definieren und die Restrisiken zu beschreiben (siehe DSFA Vorlage BSV). Risiken die nicht oder ungenügend reduziert werden (aus der Restrisikomatrix rot oder gelb markiert), müssen im ISDS-Konzept ausgewiesen werden. Verbleiben im Rahmen der Datenschutz-Folgenabschätzung für die betroffenen Personen hohe Risiken für die Persönlichkeit oder die Grundrechte, ist der EDÖB nach Artikel 23 DSG zu konsultieren.

Der Entscheid darüber, ob bekannte Restrisiken in Kauf genommen werden, obliegt der Durchführungsstelle. Die Restrisiken sollen in das Risikomanagementsystem (RM) einfliessen (vgl. Rz 2.3 Ziff 1.c).

d. Wiederherstellung des Geschäftsbetriebes/Notfall Konzept (Quelle: BACS)

Bei einem Schutzobjekt, das kritische Geschäftsprozesse unterstützt, ist ein Notfallkonzept zu erstellen.

Das Template auf der Webseite des BACS bietet dazu eine Referenz.

Dies beschreibt die Notfallplanung und Katastrophenvorsorge des Schutzobjekts, um die Aufrechterhaltung und Wiederherstellung der Geschäftsfähigkeit in ausserordentlichen Situationen zu gewährleisten. Das Notfallkonzept hat auch zum Ziel die Überprüfung der schon mit dem Leistungserbringer bestehenden SLAs und allenfalls die Nachführung notwendiger Ergänzungen. In jedem Fall ist hier ein Verweis zu den BCM Dokumenten (vgl. Rz 2.17) auf Stufe Durchführungsstelle zu machen.

e. Einhaltung / Überprüfung / Abnahme der Schutzmassnahmen

Zu beschreiben ist, wie die Einhaltung der Schutzmassnahmen geprüft wird. Dies gilt in Bezug auf angemeldete oder unangemeldete Revisionen und in Bezug auf Überprüfungen der Informationssicherheitsaktivitäten im Projekt und anschliessend im Betrieb.

Beschrieben wird auch die Systemabnahmeprüfung:

Neue und aktualisierte Systeme müssen während der Entwicklungsprozesse eine gründliche Überprüfung und Verifizierung erfahren, einschliesslich der Vorbereitung einer detaillierten Planung der Aktivitäten, Testeingaben und erwarteten Ausgaben unter verschiedenen Bedingungen. Wie bei internen Entwicklungsvorhaben sollten derartige Prüfungen zunächst vom Entwicklungsteam durchgeführt werden. Danach sollten unabhängige Abnahmeprüfungen unternommen werden (sowohl bei internen als auch bei ausgelagerten Entwicklungsvorhaben), um sicherzustellen, dass das System wie erwartet (und nur wie erwartet) funktioniert (siehe ISO/IEC 27002:2022, A.5.8 und A.8.26). Der Umfang der Prüfungen sollte der Bedeutung und der Beschaffenheit des Systems entsprechen.

Zusammenfassung des durchgeführten Audits (wer, wann, was, Resultat).

f. Ausserbetriebnahme

Beschreibt die zu beachtenden Punkte bei der Ausserbetriebnahme unter Berücksichtigung der Archivierungsvorschriften (vgl. WAF Weisungen). Die Ausserbetriebnahme wird in der erweiterten ISDS Dokumentation beschrieben.

Anhang 5: Rollenanforderungen an die Durchführungsstellen

#	Abkürzung	Rolle	Beschreibung	Randziffer
1	GL	Geschäftsleitung	Die GL erlässt basierend auf ihrem Grundaufbau des ISMS (Ziff. 2.2) Informationssicherheitsleitlinien und sorgt für deren Bekanntmachung innerhalb der Durchführungsstelle und gegenüber den involvierten externen Stellen, sowie die regelmässige Aktualisierung.	2.3
2	ISB	Informationssicherheitsbeauftragte/r	Unter anderem Ansprechpartner gegenüber dem BSV für Informationssicherheitsvorfälle für welche die von den Durchführungsstellen erlassenen Informationssicherheitsleitlinien die Information des BSV vorsehen (Rz 2.3 Ziff. 3).	2.4
3	AV	Anwendungsverantwortliche/r	Die Durchführungsstellen bezeichnen für jedes allein oder gemeinsam genutzte Informationssystem einen Anwendungsverantwortlichen. Der Anwendungsverantwortliche legt zusammen mit dem ISB die Sicherheitsanforderungen für das Informationssystem fest. Der Anwendungsverantwortliche verantwortet die Umsetzung der Sicherheitsmassnahmen.	2.8.5
4	PL	Projektleiter/in	Leitung der entsprechenden Projekte im Bereich Informationssysteme	2.5
5	Sysadmin	Netzwerk- / Systemadministrator	Verwaltet das Netzwerk und/oder die Serverinfrastruktur	2.4
6	DSB	Datenschutzberater:in	(Art. 25 sowie Art. 26 Abs. 2 Bst. a Ziffer 2 DSV) Wird bei Erstellung der erweiterten ISDS-Dokumentation (wenn mit dem Schutzobjekt besonders schützenswerte Personendaten bearbeitet werden) miteinbezogen	2.8.3
7	VP	Vertrauensperson	Stellt sicher, dass Mitarbeitern die korrekten Berechtigungsrollen für die Ausführung ihrer Arbeit zugewiesen wird (Zugriff auf Register). Die VP wird von der jeweiligen Durchführungsstelle ernannt und der ZAS gemeldet. ZAS darf Berechtigungen an Mitarbeiter der Durchführungsstelle nur vergeben, wenn die Vertrauensperson den Antrag mitunterschrieben hat.	Weisung SGA 2111 - 2112 2311 - 2313
8	RIO	Registration Identification Officer	(Art. 59 Abs. 1 AHVG) Der/Die RIO ist bei jeder Abgabe eines Authentifizierungsmittels verpflichtet, die Identifikation des Benutzers/der Benutzerin vorzunehmen (Rz 2203 SGA).	Weisung SGA, 2121 - 2125 2201 - 2203 2321 - 2330

Anhang 6: Hilfsmittel und Vorlagen

#	Hilfsmittel / Vorlage	Quelle	Download
1	Instrument für die Risikovorprüfung	BJ	https://www.bj.admin.ch/bj/de/home/staat/datenschutz/info-bundesbehoerden.html
2	Merkblatt und Vorlage Datenschutz-Folgenabschätzung (DSFA)	BSV	https://sozialversicherungen.admin.ch/de/f/20762
3	Schutzbedarfsanalyse (Schuban)	BSV	https://sozialversicherungen.admin.ch/de/d/20903/download
4	IKT-Grundschutz	BSV	https://sozialversicherungen.admin.ch/de/d/20905/download
5	ISDS-Konzept	BSV	https://sozialversicherungen.admin.ch/de/d/20907/download
6	Risikoanalyse	BACS	https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren/erhoehter-schutz.html
7	Bearbeitungsreglement und Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes (TOM)	EDÖB	https://www.edoeb.admin.ch/de/informatiksicherheit
8	Technische Empfehlung für die Protokollierung gemäss Art. 4 DSV	EDÖB	https://backend.edoeb.admin.ch/fileservice/sdweb-docs-prod-edoebch-files/files/2024/11/05/7e0c13da-b62a-41c1-a299-bff403be5f04.pdf
9	Leitfaden Implementierung eines ISMS nach ISO/IEC 27001:2022	ISACA	https://www.isaca.de/publikationen/publikationen/leitfaeden.html

Abkürzungsverzeichnis

Abkürzung	Benennung	Link
Abs.	Absatz	
AHV	Alters- und Hinterlassenenversicherung	
AHVG	Bundesgesetz über die Alters- und Hinterlassenenversicherung, SR 831.10	https://www.fedlex.admin.ch/eli/cc/63/837_843_843/de
AHVV	Verordnung über die Alters- und Hinterlassenenversicherung, SR 831.101	https://www.fedlex.admin.ch/eli/cc/63/1185_1183_1185/de
AK	Ausgleichskasse	
Art.	Artikel	
ATSG	Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts, SR 830.1	https://www.admin.ch/opc/de/classified-compilation/20002163/index.html
AV	Anwendungsverantwortliche/r	
BACS	Bundesamt für Cybersicherheit	https://www.ncsc.admin.ch
BBl	Bundesblatt	
BCM	Business Continuity Management	
BIT	Bundesamt für Informatik und Telekommunikation	
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft, SR 101	https://www.admin.ch/opc/de/classified-compilation/19995395/201801010000/101.pdf
CA	Certificate Authority, Zertifizierungsstelle	
DS	Durchführungsstellen	
DSB	Datenschutzberater / Datenschutzberaterin	
DSFA	Datenschutz-Folgenabschätzung	https://sozialversicherungen.admin.ch/de/d/20813/download
DSG	Bundesgesetz über den Datenschutz, SR 235.1	https://www.fedlex.admin.ch/eli/cc/2022/491/de
DSV	Verordnung über den Datenschutz, SR 235.11	https://www.fedlex.admin.ch/eli/cc/2022/568/de
eAHV/IV	Verein der Durchführungsstellen der AHV und IV	https://www.eahv-iv.ch
eCH	Verein, der Standards setzt im e-Government	https://www.ech.ch
EDÖB	Eidgenössischer Datenschutz- und Öffenlichkeitsbeauftragter	https://www.edoeb.admin.ch
EL	Ergänzungsleistungen	
ELG	Bundesgesetz über Ergänzungsleistungen zur Alters-, Hinterlassenen- und Invalidenversicherung, SR 831.30	https://www.fedlex.admin.ch/eli/cc/2007/804/de
EO	Erwerbsersatzordnung	
EOG	Bundesgesetz über den Erwerbsersatz für Dienstleistende und bei Mutterschaft, SR 834.1	https://www.fedlex.admin.ch/eli/cc/1952/1021_1046_1050/de
FamZG	Bundesgesetz über die Familienzulagen, SR 836.2	https://www.fedlex.admin.ch/eli/cc/2008/51/de
FamZV	Verordnung über die Familienzulagen, SR 836.21	https://www.fedlex.admin.ch/eli/cc/2008/52/de
FISA	Foreign Intelligence Surveillance Act	https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286
FLG	Bundesgesetz über die Familienzulagen in der Landwirtschaft, SR 836.1	https://www.admin.ch/opc/de/classified-compilation/19520136/index.html
IKS	Internes Kontrollsystem	
IS	Informationssystem	
ISACA	Information Systems Audit and Control Association	https://www.isaca.ch/de/
ISB	Informationssicherheitsbeauftragter (im Sinne dieser Weisungen)	
ISDS	Informationssicherheit und Datenschutz	

Abkürzung	Benennung	Link
ISG	Informationsschutzgesetz vom 20. Dezember 2020	https://www.fedlex.admin.ch/eli/fga/2020/2696/de
ISMS	Informationssicherheits-Management-System	
ISO	Internationale Organisation für Normung	
ISO 27001	ISO/EC 27001 betreffend Informationstechnologie – IT Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (mit normativem Anhang 1 betr. Referenzmassnahmenziele und –massnahmen, welche aus ISO/IEC 27002 abgeleitet wurden)	
ISO 27002	ISO/IEC 27002 Informationstechnologie – IT-Sicherheitsverfahren – Leitfaden für Informationssicherheits-Massnahmen	
IT	Informationstechnologie	
IV	Invalidenversicherung	
IVG	Bundesgesetz über die Invalidenversicherung, SR 831.20	https://www.fedlex.admin.ch/eli/cc/1959/827_857_845/de
KSBIL	Kreisschreiben über das Verfahren zur Leistungsfestsetzung in der AHV/IV/EL	https://sozialversicherungen.admin.ch/de/d/6399/download
KSSD	Kreisschreiben über die Schweigepflicht und die Datenbekanntgabe in der AHV/IV/EO/EL/FamZLw/FamZ	https://sozialversicherungen.admin.ch/de/d/6435
KVV	Verordnung über die Krankenversicherung vom 27. Juni 1995, SR 832.102	https://www.fedlex.admin.ch/eli/cc/1995/3867_3867_3867/de
QMS	Qualitätsmanagementsystem	
RM	Risikomanagementsystem	
RVOG	Regierungs- und Verwaltungsorganisationsgesetz, SR 172.010	https://www.fedlex.admin.ch/eli/cc/1997/2022_2022_2022/de
Rz/Rzn	Randziffer, Randziffern	
SAS	Schweizerische Akkreditierungsstelle	https://www.sas.admin.ch/
SEPOS	Fachstelle für die Informationssicherheitsvorgaben des Bundes	https://www.sepos.admin.ch/de/informationssicherheit
SGA	Weisungen über die Sicherheit der gemeinsamen Anwendungen in den Bereichen AHV/IV/EO/EL/FamZLw/FamZ	https://sozialversicherungen.admin.ch/de/d/6867/download
Sysadmin	System- und Netzwerkadministrator	
VDTI	Verordnung über die digitale Transformation und die Informatik vom 25. November 2020, SR 172.010.58	https://www.fedlex.admin.ch/eli/cc/2020/988/de
VO	Verordnung	
VwVG	Bundesgesetz über das Verwaltungsverfahren, SR 172.021	https://www.admin.ch/opc/de/classified-compilation/19680294/index.html
WAF	Weisung über die Aktenführung in der AHV/IV/EO/EL/FamZLw/FamZ	https://sozialversicherungen.admin.ch/de/d/6921/download
WÜWA	Weisungen über die Übertragung weiterer Aufgaben an die Ausgleichskassen	https://sozialversicherungen.admin.ch/de/d/6956/download
ZAS	Zentrale Ausgleichsstelle	
ZertES	Bundesgesetz über die elektronische Signatur; SR 943.03	https://www.admin.ch/opc/de/classified-compilation/20131913/index.html