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: 20. April 2026

Hinweis

- Nicht weisungsrelevante Anhänge zur W-ISDS werden in einem separaten Dokument auf der BSV-Vollzug-Webseite unter «eGov/Vorlagen» geführt und sind nicht Bestandteil der Weisungen. Sie dienen der fachlichen Vertiefung, Illustration und Unterstützung des Vollzugs. Verbindlich sind ausschliesslich die Weisungen W-ISDS sowie deren weisungsrelevante Anhänge.

- Zur einfacheren Lesbarkeit wurde im gesamten Dokument die männliche Form verwendet. Selbstverständlich sind dabei Personen aller Geschlechter mitgemeint.

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
2.2	12.12.2025	Markus Moog Markus Burri	Ergänzungen, Anpassungen, Präzisierungen Rz. 2.4, 2.8.2, Rz 2.15.1. Anpassung der Anhänge 2, 3, 4 und 5
2.3	20.04.2026	Markus Moog Markus Burri	Nicht weisungsrelevante Anhänge ausgelagert (Ergänzende Anhänge W-ISDS, eGov/Vorlagen), Rollenbeschreibung (Anhang 2) angepasst; Präzisierung zur Auslagerung von Schutzobjekten an externe Dienstleister ergänzt (Rz 2.17), Abkürzungsverzeichnis aktualisiert

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)**:** 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)**:** 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

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-Managementsystem (ISMS)** Als Grundlage für die Erfüllung der Anforderungen sollte den Durchführungsstellen ein von ihnen zu betreibendes Informationssicherheits-Managementsystem (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 Rz 3604 WÜWA möglich ist.

[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
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 E1 der ergänzenden Anhänge zur W-ISDS: 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 Informationssicherheitsmanagement-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.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»

	a. zum internen Kontrollsystem (IKS) 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 1). 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 Anhang 1
2.4	**2.4 Anforderungen an die Informationssicherheitsorganisation** Die Sicherheitsorganisation sieht mindestens vor, dass die Durchführungsstelle (DS) eine oder mehrere verantwortliche Rollen für die Informationssicherheit bezeichnet. In der Regel umfasst dies eine zentrale Rolle, wie z. B. Informationssicherheitsbeauftragte (ISB) sowie weitere Personen, die Schlüsselaufgaben in der Umsetzung der Informationssicherheit wahrnehmen. Für sämtliche Rollen sind sowohl die jeweiligen Verantwortlichkeiten als auch die Zuweisung an konkrete Personen oder Stellen zu dokumentieren. Die für die Informationssicherheit zuständigen Rollen bzw. Stellen nehmen insbesondere folgende Aufgaben wahr:	A.5.2	Gängige Bezeichnungen für solche Rollen sind z.B. Chief Information Security Officer (CISO), Informationssicherheits-beauftragte(r), Information Security Officer oder ISMS-Beauftragte(r)

	• Koordination der Aspekte der Informationssicherheit innerhalb der Durchführungsstelle sowie mit allfälligen beauftragten Leistungserbringern (z. B. ICT-Beauftragte, Lieferanten). • Ansprechstelle für die Informationssicherheitsverantwortlichen der IT-Leistungserbringer. • Ansprechstelle gegenüber dem BSV für Informationssicherheitsvorfälle, bei denen die Informationssicherheitsleitlinien der Durchführungsstelle eine Information des BSV vorsehen (vgl. Rz. 2.3 Ziff. 3). • Prüfung der Dokumentationen zur Informationssicherheit (insbesondere ISDS-Dokumentationen, vgl. Rz. 2.8.2 und 2.8.3) sowie der weiteren Umsetzungsnachweise. • Regelmässige Information der Leitung der Durchführungsstelle über den Stand der Informationssicherheit in der Organisation. • Abgabe von Empfehlungen an die Geschäftsleitung der Durchführungsstelle.		
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.	A.8.1, A.6.7	

	• 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.		
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 durchzuführen. Als Template können die Risikovorprüfung gemäss Anhang E5 der ergänzenden Anhänge zur W-ISDS oder kantonale bzw. eigene Vorlagen verwendet werden.	A.5.10, A.5.12, 5.13	Hilfsmittel und Vorlagen siehe Anhang E5 der ergänzenden Anhänge W-ISDS

	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 E2 der ergänzenden Anhänge zur W-ISDS); b. Klassifizierung des Schutzobjektes nach Verfügbarkeit (inkl. Beurteilung des Schutzobjekts in Bezug auf die Einteilung als geschäftskritische Anwendung); 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 E2 der ergänzenden Anhänge zur W-ISDS.		
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	A.5.10, A.5.12, 5.13	

	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 Die erweiterte ISDS-Dokumentation orientiert sich qualitativ und quantitativ am Muster gemäss Anhang E3 der ergänzenden Anhänge zur W-ISDS.		
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 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;	A.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.3, A.8.4, A.8.5	

	f. eine Protokollierung der Zugriffe nach Art. 4 DSV erfolgt (siehe Anhang E2 Ziffer 7 der ergänzenden Anhänge zur W-ISDS); g. die Richtigkeit und Zweckmässigkeit der erteilten Benutzerrechte wenigstens jährlich durch den AV geprüft werden		
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 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.	A.8.24	
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 Ziff. 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.	A.7.7 - A.7.14, A.8.1	

[9] siehe dafür die BAKOM Webseite: https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrstellensuchesas/pki1.html

	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		
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 E2, Buchstabe D der ergänzenden Anhänge zur W-ISDS) H. Audit von Informationssystemen	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	

	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.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.	A.8.27	
2.13.2	**Zugriffsmatrix** Die Durchführungsstellen verfügen über eine verbindliche Zugriffmatrix, die festlegt, wie Personen und automatisierte Prozesse (Machinen/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 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	A.5.14, A.6.6	
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 fünf 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. Weiter stellen die Durchführungsstellen mittels entsprechender Vertragsklausel sicher, dass die Durchführungsstellen berechtigt sind, bei ihren jeweiligen Vertragspartnern externe Audits durchführen zu lassen. Vorbehalten bleibt Kapitel 2.2, Rz 7 WAID wonach in bestimmten Fällen kein separates externes Audit bei Dritten erforderlich ist. • 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. • Sofern das BSV über Rahmenverträge mit Dienstleistern der IV-Stellen verfügt, orientieren sich die IV-Stellen bezüglich ISDS-Vorgaben an diesen Verträgen. • 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)). • Zusätzlich zur Einhaltung der datenschutzrechtlichen Bestimmungen haben Vertragspartner der Durchführungsstellen eine entsprechende Geheimhaltungsvereinbarung zu unterzeichnen, sofern diese Zugriff auf Daten der 1. Säule/FamZ erhalten.	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 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
	  • Erstellung einer Datenschutz-Folgenabschätzung (falls gemäss Risikovorprüfung verlangt)
	  • Erstellung von IKT-Grundschutz
	  • Erstellung von Risikoanalyse und ISDS-Konzept (falls gemäss Schutzbedarfsanalyse verlangt)
	
	Details zu den Analysen und Bewertungen finden sich in Anhang E2 und E3 der ergänzenden Anhänge zur W-ISDS.
	
	Falls die getroffenen Schutzmassnahmen und Risikominderungen eine Bearbeitung und 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 Anhang E2 Bst. I Zuweisung zu einer Schutzgruppe der ergänzenden Anhänge zur W-ISDS).
	
	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
		A 5.23	

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

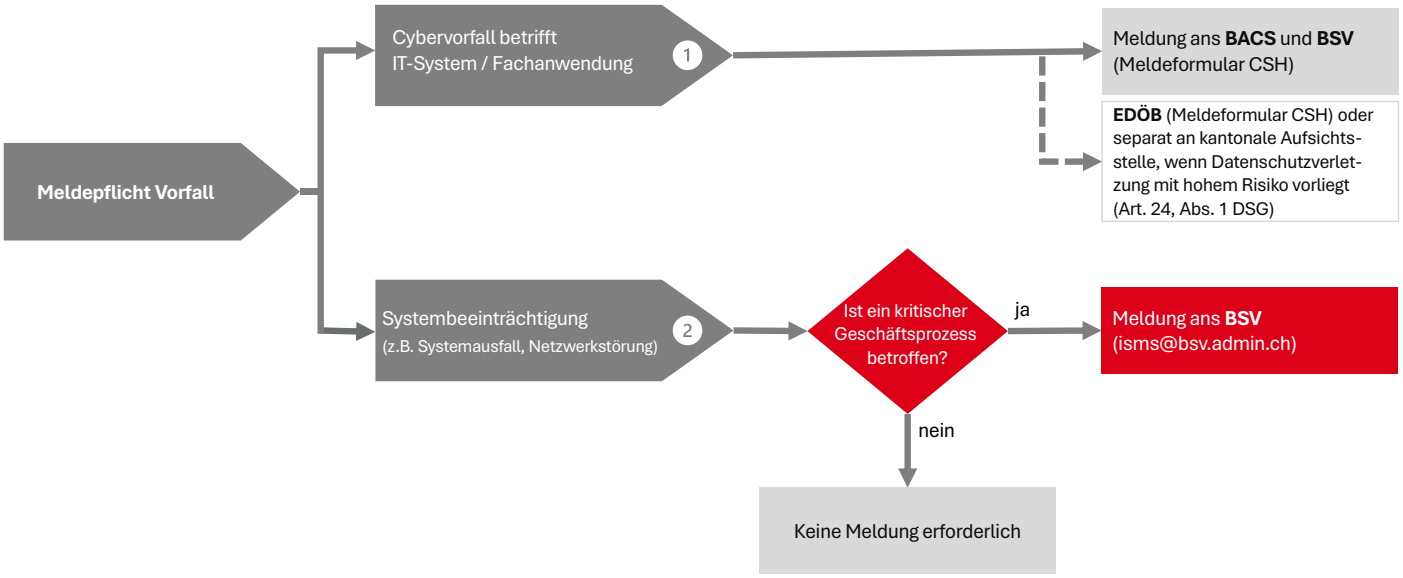
[11] Siehe dazu die Cloud Webseite der Bundesverwaltung:
https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html

	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 (unabhängig von der verwendeten Applikation) 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 Informationssicherheitsverantwortliche 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 Massnahmen durch die zuständigen Personen getroffen werden.	A.5.24 - .5.28, A.6.8	
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. Sofern die Durchführungsstelle den Betrieb eines oder mehrerer Schutzobjekte an externe Dienstleister vergeben hat, ist der entsprechende Dienstleister für die Einhaltung der Rz 2.17 verantwortlich. Die Durchführungsstelle prüft in diesem Fall das Vorhandensein der BCM Verfahren des jeweiligen Dienstleisters.	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 1: Meldepflicht Cybervorfälle und Systembeeinträchtigungen (weisungsrelevant)

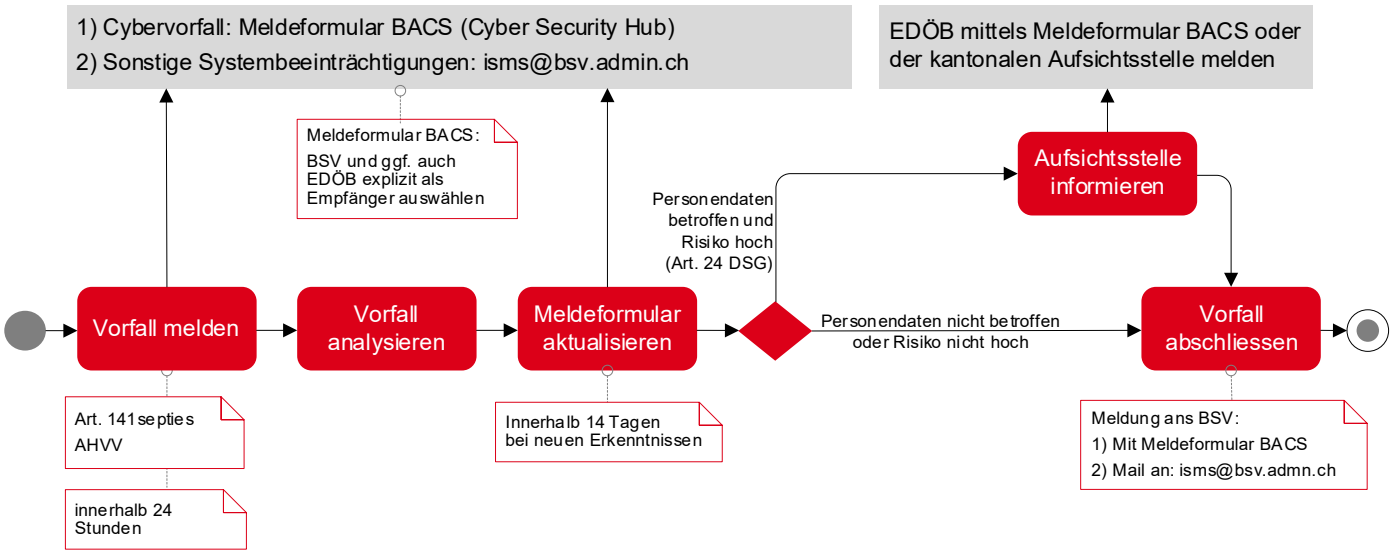
Übersicht Meldepflicht

Gemäss Art. 141septies AHVV wird zwischen Cybervorfällen und Systembeeinträchtigungen unterschieden. Systembeeinträchtigungen (z. B. Systemausfälle oder Netzwerkstörungen), die einen kritischen Geschäftsprozess betreffen (gemäss Rz 2.8.2 Ziff. 2 Bst. b), sind dem BSV per E-Mail an isms@bsv.admin.ch zu melden. Das Meldeformular BACS[12] ist ausschliesslich für Cybervorfälle vorgesehen.



Meldung Cybervorfall

Cybervorfälle sind dem BSV mittels Meldeformular BACS zu melden.



[12] Website NCSC (BACS) mit Link zu Meldeformular: https://www.ncsc.admin.ch

Anhang 2: Rollenanforderungen an die Durchführungsstellen (weisungsrelevant)

#	Abkürzung	Rolle	Beschreibung
1	GL	Geschäftsleitung / Leitung der Durchführungsstelle	Die GL / Leitung 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.
2	ISB / CISO	Informationssicherheitsbeauftragte/r oder andere gängige Bezeichnungen für solche Rollen sind z.B. Chief Information Security Officer (CISO), Information Security Officer oder ISMS-Beauftragter	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).
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.
4	PL	Projektleiter/in	Leitung der entsprechenden Projekte im Bereich Informationssysteme
5	NSA	Netzwerk- / Systemadministrator	Verwaltet das Netzwerk und/oder die Serverinfrastruktur, implementiert technische Sicherheitsmassnahmen
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

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
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
BCM	Business Continuity Management	
Bst.	Buchstabe	
CA	Certificate Authority, Zertifizierungsstelle	
DS	Durchführungsstellen	
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
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	Informationssicherheitsbeauftragte/r (im Sinne dieser Weisungen)	
ISDS	Informationssicherheit und Datenschutz	
ISG	Informationsschutzgesetz vom 20. Dezember 2020	https://www.fedlex.admin.ch/eli/cc/2022/232/de
ISMS	Informationssicherheitsmanagement-System	
ISO	Internationale Organisation für Normung	
ISO 27001	ISO/EC 27001 betreffend Informationstechnologie – IT Sicherheitsverfahren – Informationssicherheits-management-Systeme – Anforderungen (mit normativem Anhang 1 betr. Referenzmassnahmenziele und –massnahmen, welche aus ISO/IEC 27002 abgeleitet wurden)	

Abkürzung	Benennung	Link
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
NSA	Netzwerk- / Systemadministrator	
QMS	Qualitätsmanagementsystem	
RM	Risikomanagementsystem	
Rz / Rzn	Randziffer, Randziffern	
SAS	Schweizerische Akkreditierungsstelle	https://www.sas.admin.ch/
VO	Verordnung	
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
Ziff.	Ziffer	