Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Sozialversicherungen BSV

Ergänzende Anhänge

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

Stand: 20. April 2026

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

Änderungsverzeichnis

VERSION	DATUM	VERFASSER	BEMERKUNGEN
1.0	14.01.2026	Markus Moog (BSV)	Anhänge aus W-ISDS 2.3 übernommen

Zweck und Abgenzung

Dieses Dokument enthält Unterlagen und Anhänge zur W-ISDS, die nicht Bestandteil der Weisungen sind und keinen Weisungscharakter haben. Die Inhalte dienen der Information, Erläuterung und fachlichen Unterstützung und entfalten keine rechtliche Verbindlichkeit. Sie begründen insbesondere keine Rechte oder Pflichten.

Für den Vollzug massgebend sind ausschliesslich die Weisungen W-ISDS sowie die darin ausdrücklich als weisungsrelevant bezeichneten Anhänge.

Inhaltsverzeichnis

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)[1] kam eine zusätzliche Regulierung dazu.

B. Auf kantonaler Ebene

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

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.

[1] BBl **2020** 9975

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[2] 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.

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

Anhang 2: ISDS-Basisdokumentation

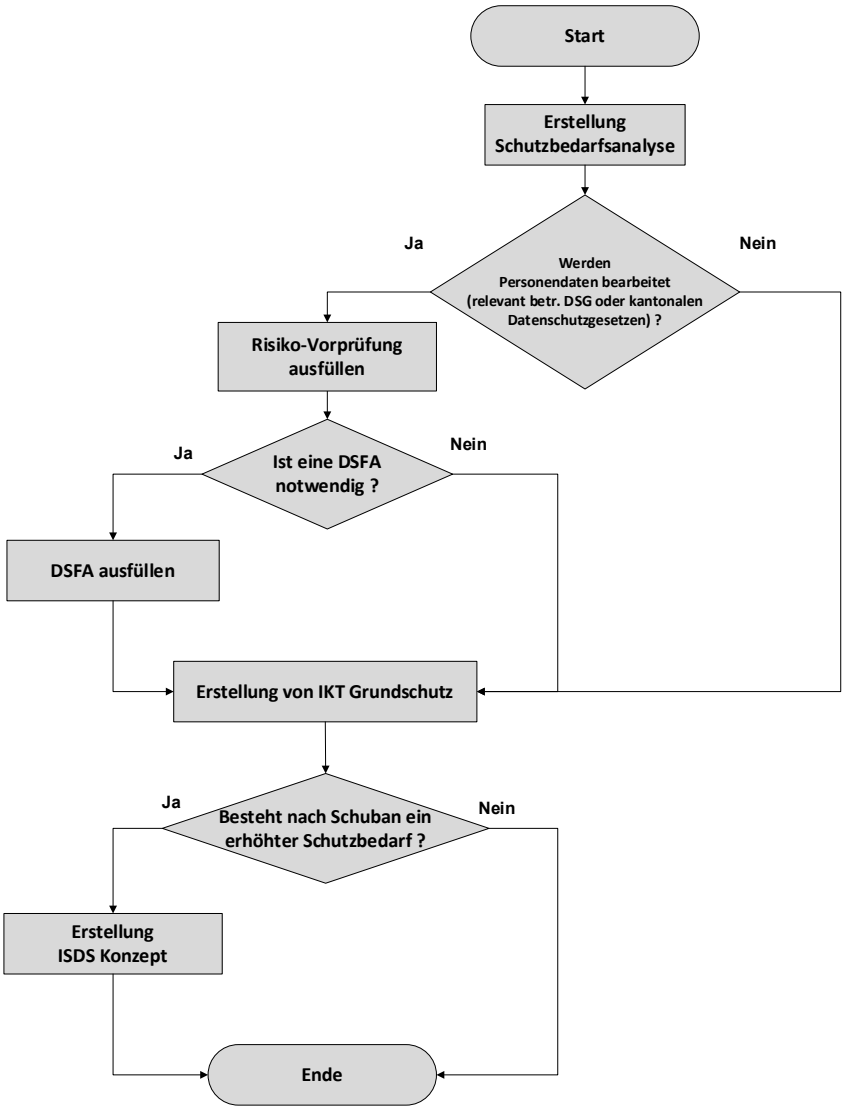
Für jedes Schutzobjekt sind mindestens die Schutzbedarfsanalyse sowie der IT-Grundschutz auszufüllen. Falls erforderlich, sind darüber hinaus eine Risikovorprüfung sowie gegebenenfalls eine Datenschutz-Folgenabschätzung zu erstellen.

Links zu den Mustervorlagen der zu erstellenden Dokumentationen siehe Anhang . Kantonale oder eigene Vorlagen können ebenfalls verwendet werden.

- 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:

Flussdiagramm Schutzbedarfsanalyse



A. Leitfaden zur Abklärung der rechtlichen Rahmenbedingungen (nach W-ISDS 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

#	Fragestellung/Thema	Rechtliche Grundlage	Konsequenz, Beispiel
			Daten im vorliegenden Fall bearbeitet werden, ist der Grundsatz verletzt. **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.	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

#	Fragestellung/Thema	Rechtliche Grundlage	Konsequenz, Beispiel
		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 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.	Identität des Empfängers von Daten klären können.
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)	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

#	Fragestellung/Thema	Rechtliche Grundlage	Konsequenz, Beispiel
		Bearbeiten mehrere Verantwortliche Personendaten gemeinsam, so kann die betroffene Person ihr Auskunftsrecht bei jedem Verantwortlichen geltend machen.	Einwilligung der betroffenen Person - über die von ihr bezeichnete - Gesundheitsfachperson mitgeteilt werden (Art. 25 Abs. 3 DSG). **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 (alle nicht kantonalen Durchführungsstellen) müssen die Vorschriften zum Verzeichnis ihrer Bearbeitungstätigkeiten einhalten und die Verzeichnisse dem EDÖB melden (Art. 12 DSG). Die kantonalen Organe unterliegen den Registrierungs-/Meldepflichten ihrer jeweiligen Kantone.	
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.	

#	Fragestellung/Thema	Rechtliche Grundlage	Konsequenz, Beispiel
		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 Departemente 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	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
		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 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 W-ISDS Rz 2.8.2, Bst. b)

#	Fragestellung bzw. Anforderung	Kriterien	**Schutzbedarf erhöht? > erweiterte ISDS-Dokumentation nach W-ISDS 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 W-ISDS 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 W-ISDS 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 (W-ISDS Rz 2.8.3) zu eruieren.

Fragestellung bzw. Anforderung	**Kriterien**	**Schutzbedarf erhöht? > erweiterte ISDS-Dokumentation nach W-ISDS 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)?[3] 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.

[3] 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 W-ISDS Rz 2.8.2, Bst. d)

Klassifizierungen	Beschreibung	Massnahmen	Erweiterte ISDS-Dokumentation nach W-ISDS Rz 2.8.3 nötig?	Kriterien für die Klassifizierung
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 (W-ISDS Rz 2.11.2 und 2.12.2) müssen die «normale Integrität» gewährleisten.	Nein	Keine geschäftskritischen Prozesse, keine sicherheitsrelevanten Auswirkungen bei unbemerkten Änderungen, keine Anforderungen an Protokollierung oder Revisionssicherheit.
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.	Prüfung der Auswirkungen fehlerhafter Änderungen (Release-Wechsel, Konfigurationsfehler etc.); bei kritischen Auswirkungen sind Tests, Dokumentation und Umsetzung nach Qualitätsmanagement erforderlich (vgl. W-ISDS Rz 2.5, 2.14).	Ja	Änderungen an den Daten könnten negative Auswirkungen auf Aufgabenerfüllung, Aussenwirkung oder Finanzen haben. Anforderungen an Freigaben, Qualitätssicherung und Change Control bestehen. Keine systematische Nachverfolgbarkeit erforderlich.
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.	Geeignete Protokollierungs- und Überwachungsmechanismen (z. B. Audit Logs, Hash-Werte, Change-Tracking) müssen eingesetzt werden, um Integritätsverletzungen erkennen und dokumentieren zu können. Diese Massnahmen sollen sicherstellen, dass nicht nur unbefugte Änderungen verhindert, sondern auch retrospektiv nachvollzogen und analysiert werden können.	Ja	Bearbeitung betrifft personenbezogene oder geschäftsrelevante Daten, bei denen eine Nachvollziehbarkeit gesetzlich oder organisatorisch gefordert ist. Protokollierung von Datenzugriffen und -änderungen ist zwingend.
Signierte Integrität	Für Bereiche der ICT-Umgebung, die in der Stufe «Signierte Integrität» eingeordnet sind, müssen zusätzlich digitale Signaturen eingesetzt werden.	Digitale Signaturen (z. B. qualifiziert gem. VZertES), gleichwertige kryptografische Prüfmechanismen (bspw. HMAC) oder Integritätsverifikationen müssen verwendet werden, um nachweislich eine Authentizität und Unveränderbarkeit der Daten sicherzustellen. Die Integritätsprüfung muss durch automatisierte oder manuelle Verifikationsverfahren regelmässig erfolgen. Diese Anforderung gilt nur, wenn die digitale Version eines Dokuments Beweiskraft hat oder als Referenzversion verwendet wird.	Ja	Es besteht ein hoher Beweiswert für Daten oder Dokumente (z. B. Leistungsentscheide, Bescheide). Rechtsverbindlichkeit, Authentizität und Integrität müssen zweifelsfrei nachgewiesen werden können.

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 W-ISDS 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 W-ISDS 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 W-ISDS 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.

Beispiele von Schutzgruppen		**Beschreibung / Beispiel**	**Informationsbeispiele**
S1	**öffentlich**	Öffentliche Daten und Informationen	▪ Internetauftritt ▪ Social Media ▪ News- und Presseinformationen
S2	**intern**[4]	Personendaten der Mitarbeitenden und Kunden sowie interne Geschäfts- und Projektdaten	▪ Adressverzeichnis ▪ «nicht-sensible» Personendaten ohne besondere Schutzwürdigkeit
S3	**vertraulich**[5]	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[6] 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».

[4] Nicht im Sinne von Art. 18 ISV
[5] Nicht im Sinne von Art. 19 ISV
[6] Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee (ISV)

Anhang 3: Erweiterte ISDS-Dokumentation
(nach W-ISDS Rz 2.8.3)

Falls die Schutzbedarfsanalyse einen erhöhten Schutzbedarf des Schutzobjektes ergibt (siehe Flussdiagramm im Anhang 2), ist die Erstellung eines ISDS Konzepts sowie einer Risikoanalyse notwendig.

Links zu den Mustervorlagen der zu erstellenden Dokumentationen siehe Anhang 5. Kantonale oder eigene Vorlagen können ebenfalls verwendet werden.

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. W-ISDS Rz 2.9), Betriebssicherheit (vgl. W-ISDS Rz 2.12) und Leistungen der Dritten (vgl. W-ISDS Rz 2.15). Es können auch Verweise auf entsprechende Dokumentationen gemacht werden (z.B. Netzwerksicherheit- und Dokumentation vgl. W-ISDS Rz 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 2, 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 . 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.[7] 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.

[7] 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, in der Excel-Datei des BACS (zum Download auf der Webseite des BACS) oder gemäss eigenen oder kantonalen Vorlagen 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. W-ISDS 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. W-ISDS 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 4: Responsible-Rollen für die Umsetzung der W-ISDS-Anforderungen

Exemplarische Rollenzuordnung (Responsible) für die Umsetzung der Anforderungen der W-ISDS

Dieses Beispiel dient als Hilfestellung; die konkrete Umsetzung kann bei den Durchführungsstellen abweichen.

Randziffer	Anforderungen	GL	ISB	AV	DSB	PL	NSA
2.2	Grundaufbau des ISMS der Durchführungsstelle		X				
2.3	Informationssicherheitsleitlinien	(X)	X				
2.4	Anforderungen an die Informationssicherheitsorganisation		X				
2.5	Anforderungen an Projekte im Bereich Informationssysteme					X	
2.6	Informationssicherheit bei Mobilgeräten und Mobile Working						X
2.7.1	Personalsicherheit		X				
2.7.2	Information und Schulung		X				
2.7.3	Änderung der Verhältnisse						X
2.8.1	Inventar aller Informationssysteme		X				
2.8.2	ISDS-Basisdokumentation		X				
2.8.3	Erweiterte ISDS-Dokumentation		X				
2.8.4	Aktualität der ISDS-Dokumentation		X				
2.8.5	Anwendungsverantwortlicher			X			
2.9	Zugriffssteuerung zu den Informationssystemen						X
2.10.1	Kryptographie						X
2.11.1	Sicherheitsdispositiv für Räumlichkeiten						X
2.11.2	Massnahmen für Geräte und Betriebsmittel						X
2.12	Massnahmen für die Betriebssicherheit						X
2.13	Netzwerk- und Kommunikationssicherheit (W-ISDS Rz 2.13.1 - 2.13.4)						X
2.14	Änderungen an Informationssystemen					X	
2.15.1	Verträge mit Dritten	X					
2.15.2	Verwendung von M365		X		(X)		
2.16	Management von Informationssicherheitsvorfällen		X				
2.17	Aufrechterhaltung der Informationssicherheit (BCM)						X
2.18	Richtlinienkonformität		X				

Rollenkombinationen sind zulässig, sofern Funktionstrennungen gewahrt bleiben, keine sicherheitsrelevanten Interessenskonflikte entstehen und die Unabhängigkeit risikorelevanter Kontrollfunktionen sichergestellt ist. Die Durchführungsstelle dokumentiert getroffene Rollenkombinationen nachvollziehbar und stellt sicher, dass fachliche Kompetenz sowie Ressourcen für jede Rolle gewährleistet sind.

Anhang 5: 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