Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Sozialversicherungen BSV

Empfehlung zu den Mindestanforderungen an die Informationssysteme der Durchführungsstellen der 1. Säule/FamZ

Gültig ab 1. Januar 2022

Stand: 1. Januar 2022

Vorbemerkungen

Die Empfehlungen richten sich an die Durchführungsstellen der 1. Säule/FamZ. Sie werden publiziert mit Blick darauf, dass voraussichtlich am 1.1.2024 eine AHVG-Gesetzesrevision in Kraft tritt, welche derzeit im Parlament behandelt wird (Botschaft des Bundesrates vom 20. November 2019 zur Modernisierung der Aufsicht in der 1. Säule und Optimierung der 2. Säule der Alters-, Hinterlassenen- und Invalidenvorsorge, Gesetzes-Entwurf BBl 2020 109).

Gestützt auf diese Gesetzesrevision ist damit zu rechnen, dass das Bundesamt für Sozialversicherungen (BSV) Weisungen zu den Mindestanforderungen im Bereich der Informationssicherheit und des Datenschutzes (ISDS) der Informationssysteme (IS) der 1. Säule/FamZ erlassen wird. Mit den vorliegenden Empfehlungen soll bereits im heutigen Zeitpunkt sichergestellt werden, dass sich die Durchführungsstellen (DS) optimal auf die kommenden BSV Weisungen zu den ISDS Mindestanforderungen vorbereiten können. Deshalb wurden die IT Vertreter der DS (Projekt eAHV/IV Information Security) eng in die Ausarbeitung der vorliegenden Fassung der Empfehlung einbezogen.

Bis zum voraussichtlichen Inkrafttreten der AHVG-Gesetzesrevision am 1.1.2024 dürfte auch die bereits beschlossene Revision des Datenschutzgesetzes (nDSG) vom 25. September 2020 (BBl 2020 7639) Geltung haben. Die Verordnungsbestimmungen zum nDSG (nVDSG) sind noch nicht definitiv und werden in einem Zeitpunkt nach Publikation diese Empfehlungen bekannt. Die vorliegenden Empfehlungen berücksichtigen bereits die nDSG Bestimmungen, es muss aber damit gerechnet werden, dass die nVDSG noch inhaltliche Änderungen mit sich bringen können, welche dann in die Weisungen zu den ISDS Mindestanforderungen einfliessen werden. Auch diese Änderungen werden mit den IT Vertretern der DS (Projekt eAHV/IV Information Security) ausgearbeitet und besprochen werden.

Folgende Themen werden bei der weiteren Ausarbeitung von Bedeutung sein:

- **ISDS Basis- und erweiterte Dokumentation** (Ziff. 2.8.2 und 2.8.3 bzw. Anhänge 5 und 6): Die Mindestanforderungen müssen auf Kompatibilität mit der neuen nVDSG überprüft werden.
- **Auftrag Dritter/Subunternehmer** (Ziff. 2.15, 2. Bullet): In Bezug auf die Einschaltung von Subunternehmen (Art. 9 Abs. 3 nDSG) ist die Genehmigung des Auftraggebers notwendig. Diesem gesetzlichen Erfordernis muss auch die kommende Weisung genügen. Die jetzige Empfehlung müsste allenfalls verschärft werden.
- **Auftragsbearbeiter im Ausland** (Ziff. 2.15, 3. Bullet und Anhang 5 Bst. E)**:** Gemäss dieser Empfehlung ist die Datenhaltung grundsätzlich in der Schweiz vorgesehen, und auch die Dienstleistungen für den Betrieb müssen grundsätzlich im Inland erfolgen und Ausnahmen müssen begründet sein. Werden Personendaten von einem Auftragsbearbeiter im Ausland bearbeitet, kommt es zu einer Datenbekanntgabe ins Ausland, und es kommen komplexe Bestimmungen des nDSG 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 nDSG. In die definitiven Weisungen (Ziff. 2.15) ist ein Hinweis auf die Einschränkungen nach nDSG aufzunehmen, der letztlich für alle DS Geltung haben muss (keine Ausnahmen für kantonale Stellen vorgesehen).
- **Clouddienste Dritter mit Datenhaltung in der Schweiz** (Ziff. 2.15): Es geht hier nicht um eine direkte (Massen-) Datenlieferung – und Auftragsbearbeitung ins Ausland, sondern um die Verletzung des schweizerischen Datenschutzes durch einen in der Schweiz domizilierten Auftragsbearbeitenden. Aktuelles Grundproblem ist die Auftrags-Datenbearbeitung durch Microsoft Schweiz, welche aus Schweizer Sicht dem Schweizer Recht untersteht, jedoch aufgrund des US-amerikanischen Cloud-Acts von amerikanischen Gerichten gezwungen werden kann, bestimmte Daten gegenüber amerikanischen Behörden offen zu legen. Grundsätzlich erlaubt die Schweizer Gesetzgebung die Bekanntgabe von Daten im Rahmen einer Strafuntersuchung (vgl. z.B. Art. 50 Abs. 1 Bst. d AHVG). Aufgrund des Territorialprinzips geht die Information aber nur an eine

schweizerische Untersuchungsbehörde. Will eine ausländische Untersuchungsbehörde Auskunft, muss sie die Information auf dem Weg der Rechtshilfe – gestützt auf entsprechende internationale Abkommen – einfordern. Die zuständige Schweizer Behörde wird dann an die Durchführungsstelle gelangen. Allerdings erst nach Prüfung des Rechtshilfebegehrens. Rechtshilfebegehren für Straftatbestände, die es nach Schweizer Recht gar nicht gibt, wird nicht stattgegeben. In Bezug auf den Cloud-Act bedeutet dies in der Praxis eine «eigenmächtige Rechtshilfe», so dass das Territorialprinzip ausgeschaltet und das US-amerikanische Straf- Verfahren schneller wird. Der EDÖB kommt in seiner aktuellen Einschätzung[1] und auf der Basis des heute geltenden DSG zu einer eher negativen Beurteilung und hält insbesondere fest: ***«Falls aufgrund der Risikoeinschätzung bezüglich der Verarbeitung von Personendaten in der Cloud Zweifel bestehen, ist von einer Auslagerung der Daten abzusehen.»***

In der Stellungnahme des EDÖB[2] zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6 Abs. 1 nDSG vom 8.9.2020 wird ausgeführt, dass bei den US-Zugriffen ein wesentlicher Schutzmechanismus unklar sei und die Grundsätze der rechtmässigen Datenbearbeitung nach DSG verletzt würden. Für die Betroffenen in der Schweiz bei Datenzugriffen von US-Behörden würde es an durchsetzbaren Rechtsansprüche fehlen, zumal sich die Wirksamkeit des sog. Ombudsperson-Mechanismus, der einen indirekt durchsetzbaren Rechtsbehelf garantieren soll, mangels Transparenz nicht beurteilen lässt und dass die Entscheidkompetenzen der Ombudsperson gegenüber den US-Geheimdiensten sowie ihre tatsächliche Unabhängigkeit ohne hinreichend konkrete und schlüssige Informationen unbelegt bleiben. Dieser Mangel an Transparenz und das daraus abzuleitende Fehlen von Garantien bei Eingriffen der US-Behörden in die Privatsphäre und informationelle Selbstbestimmung von Personen in der Schweiz erachtet der EDÖB als unvereinbar mit dem Anspruch dieser Personen auf einen Rechtsweg nach Art. 29 ff. BV und Art. 15 DSG für die Durchsetzung der ihnen nach Art. 13 Abs. 2 BV sowie Art. 8 EMRK zustehenden Rechte; mit den Grundsätzen einer rechtmässigen Personendatenbearbeitung i.S.v. Art. 4 DSG.

In der Bundesverwaltung wird derzeit die Problematik der Cloud-Dienste jedoch vertieft geprüft, und es bleibt zu hoffen, dass die nötige Transparenz hergestellt werden kann. Im Rahmen der Cloud-Strategie der Bundesverwaltung sollte in einem der nächsten Meilensteine die rechtlichen Fragen geklärt werden können. Bei den Verträgen zwischen dem Bund (WTO 20007, Beschaffung Public Cloud Bund) und Microsoft handelt es sich noch um ein laufendes Verfahren. Zuständig ist die Bundeskanzlei. Insofern sollte bis zum Inkrafttreten der BSV ISDS Weisungen eine Ergänzung zum Thema «Aufträgen an Dritten» in Bezug auf Clouddienste möglich sein.

[1] Siehe Erläuterungen zu Cloud Computing (admin.ch)
[2] Siehe Stellungnahme des EDÖB

1 ISDS Empfehlungen zu den Mindestanforderungen

Rz-Nr.	Empfehlungen BSV zur Informationssicherheit	Verweise auf DIN ISO/IEC 27001: 2015-03 (A=Normativer Anhang)	Kommentar
1	**Ziel, Zweck, Gegenstand, Grundsätze, Geltungsbereich und Grundsätze sowie Bezüge im Rechtssystem**		
1.1	**Ziel, Zweck und Gegenstand** Mit Blick auf die Botschaft des Bundesrates vom 20. November 2019[3] und den Gesetzesentwurf[4] zur Modernisierung der Aufsicht in der 1. Säule und Optimierung der 2. Säule der Alters-, Hinterlassenen- und Invalidenvorsorge empfiehlt das BSV den Durchführungsstellen, bei ihren Informationssystemen laufend auf die nachfolgend umrissenen, kommenden neuen Rahmenbedingungen zu achten.. Ein zentrales Anliegen der noch laufenden 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. E- Art. 49a Abs. 2 AHVG). In Bezug auf Informationssicherheit und Datenschutz müssen die Durchführungsstellen aber künftig zusätzlich die von der Aufsichtsbehörde festgelegten Mindestanforderungen erfüllen (E- Art. 49a Abs. 3 AHVG). Sollte es dazu kommen, dass gemäss neuer Gesetzgebung die Fachorganisationen der Durchführungsstellen Regeln zur Umsetzung der Mindestanforderungen erarbeiten, welche durch die Aufsichtsbehörde anerkannt werden (E- Art. 49a Abs. 4 AHVG),wären auch diese anerkannten Umsetzungsregeln von den Durchführungsstellen zu beachten, soweit sie unter deren Geltungsbereich fallen (vgl. Rz 1.2). Mit dieser Empfehlung werden die künftigen Mindestanforderungen an die Informationssysteme für die Informationssicherheit und den Datenschutz skizziert (Art. 49a Abs. 3 in Verbindung mit Art. 72a Abs. 2 bst. b E-AHVG), welche von den		

[3] BBl **2020** 1
[4] BBl 2020 109

	Durchführungsstellen erfüllt sein sollten (alle Rz von Kapitel 2).		
1.2 **1.2.1**	**Geltungsbereich** Die vorliegende Empfehlung zu den Mindestanforderungen nach Rz 2 richtet sich an alle Durchführungsstellen der AHV, IV, EO, und EL (vgl. E-Art. 66 Abs. 1 Bst. a IVG, E-Art. 21 Abs. 2 EOG, E-Art. 26 Abs. 1 Bst. a ELG). Sie richtet sich auch an alle Zweigstellen nach Artikel 65 AHVG. Die Empfehlung gilt zudem für die Durchführung der Familienzulagen (E-Art. 25 Bst. a i. V. m. E-Art. 27 Abs. 3 FamZG sowie Art. 25 FLG)		
1.3	**Definition eines Informationssystems (IS)** Ein Informationssystem ist ein Hilfsmittel für die Datenbearbeitung, Datenbekanntgabe sowie für das Profiling (nach nDSG) zur Aufgabenerfüllung[5] 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.8.1.1	
1.4	**Grundsatz Informationssicherheits-Management-System (ISMS)** Als Grundlage für die Erfüllung der Mindestanforderungen sollte den Durchführungsstellen ein von ihnen zu betreibendes Informationssicherheits-Management-System (ISMS) dienen. Dieses orientiert sich an den nationalen[6] und		E-Art. 68a AHVG gilt nicht für das FamZG (anders FLG). Die Regelung der Kassenrevision und der

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

[6] insbesondere die Vorgaben IKT-Grundschutz in der Bundesverwaltung, bzw. Informationssicherheitsgesetzes ISG vom 18. Dezember 2020 (BBl 2020 9975) nach dessen Inkrafttreten

	internationalen[7] Standards und muss wenigstens den nachfolgenden Vorgaben entsprechen. Ein ISMS besteht aus Vorgaben, Rollen und Verantwortlichkeiten, Prozessen, Prozeduren, die zur Erreichung von definierten Zielsetzungen einer Organisation dienen. Das ISMS wird voraussichtlichGegenstand der Prüfung der Revisionsstelle im Sinne von Artikel 68a, Absatz 2 Buchstabe c E-AHVG werden. Die Revisionsstelle wird dann prüfen, ob das ISMS der Durchführungsstellen den in dieser Empfehlung umrissenen Mindestanforderungen entspricht. Davon ausgenommen werden die Familienausgleichskassen nach Artikel 14 Buchstabe a FamZG sein, sofern die kantonalen Familienzulagengesetze nichts anderes vorsehen.		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.
1.5 **1.5.1** **1.5.2**	**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.		Es handelt sich um technische und organisatorische Massnahmen. Diese sind nicht zu

[7] ISO/EC 27001, 2013 + Cor 1:2014) betreffend Informationstechnologie – IT Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (mit normativem Anhang 1 betr. Referenzmassnahmenziele und –massnahmen, welche aus ISO/IEC 27002 (Informationstechnologie – IT-Sicherheitsverfahren – Leitfaden für Informationssicherheits-Massnahmen [ISI/IEC27002: 2013 + Cor 1:2014 + Cor 2:2015] abgeleitet wurden).

1.5.3	- Datensicherheit umfasst in praktischer Hinsicht alle Massnahmen zur Sicherstellung der Vertraulichkeit, Integrität, Nachvollziehbarkeit und Verfügbarkeit der Informationen. - Datenschutz umfasst in praktischer Hinsicht alle Massnahmen zur Verhinderung einer unerwünschten Bearbeitung von Personendaten und deren Folgen. Der Schutz zielt auf die Person und nicht die Daten an sich ab. Grundsätzlich sind bei der Informationssicherheit die Vorschriften aus ganz verschiedenen Rechtsquellen anwendbar und von den Durchführungsstellen zu beachten (vgl. Anhang 1: Übersicht nationale Rechtsquellen, ISO-Normen). Die vorliegende Weisung konzentriert sich auf die Anforderungen an ein ISMS und behandelt 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 dieser für die Durchführungsstellen geltenden Empfehlung 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.		verwechseln mit den technischen und organisatorischen Massnahmen nach Artikel 153d E-AHVG[8], welche nur von Behörden, Organisationen und Personen eingehalten werden müssen, die ausserhalb der Sozialversicherungen zur Nutzung der AHV-Versichertennummer berechtigt sind.
2	**Mindestanforderungen**		
2.1	**Informationssicherheits-Management-System (ISMS)[9]** Jede Durchführungsstelle verfügt über ein ISMS (vgl. Rz 1.4).	4.4	
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	4.1	

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

[9] Für den Aufbau des ISMS werden folgende Leitfäden empfohlen:
- ISACA Leitfaden: https://www.isaca.de/sites/default/files/attachements/isaca_leitfaden_i_gesamt_web.pdf
- Zusätzlich sind heute schon Informationssysteme/Tools auf dem Markt mit welchen ein digitales ISMS aufgebaut werden kann (siehe Beispiel https://swissgrc.com/)

	EOG (SR 834.1), ELG (SR 831.30), FLG (SR 836.1) und FamZG (SR 836.2).		
b	Sie identifizieren die involvierten Stellen und analysieren ihre Anforderungen in Bezug auf Informationssicherheit auf der Basis des standardisierten Fachdomänenmodells des BSV (vgl. Anhang 2).	4.2	
c	Sie haben eine aktuelle Übersicht über alle Informationssysteme und IT-relevanten Aktivitäten (vgl. auch Inventar nach Ziff. 2.8), strukturiert auf der Basis des standardisierten Fachdomänenmodells des BSV (betriebene Informationssysteme, IT-Projekte und laufende Anpassungen der bestehenden Anwendungen), welche in das ISMS integriert ist.	A.8.1.1	
d	Gleichzeitig legen sie die diejenigen Bereiche fest, für welche die Mindestanforderungen 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.	4.3	
e	Die Durchführungsstellen sorgen für eine laufende Aktualisierung und Verbesserung des ISMS (einschliesslich BCM vgl. Rz. 2.17) und seiner Komponenten (vgl. Bild Anhang 3). Sie nehmen wenigstens jährlich eine Überprüfung der Aktualität vor.	4.4	
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 E-AHVG): a. zum internen Kontrollsystem (IKS), b. zum Qualitätsmanagementsystem (insbesondere kontinuierlicher Verbesserungsprozess KVP) c. zum Risikomanagementsystem (RM)	A.5.1 / A.5.1.1 A.6.1.2	

	2. Die Regelung der adäquaten Information der Geschäftsleitung und weiterer involvierten Stellen (vgl. Rz 2.2 Bst. b und d) sowie gegebenenfalls: a. des EDÖB nach Artikel 24 nDSG (bei einer entsprechenden Verletzung der Datensicherheit) oder des Datenschutzbeauftragten nach kantonalem Recht; b. des BSV durch die Informationssicherheitsorganisation und die Beschreibung eines Informations-sicherheitsvorfallbearbeitungsprozesses (Als Beispiel vgl. Anhang 4). 3. Die Regelung der adäquaten Information des BSV (und/oder der jeweils zuständigen Aufsichtsbehörde) über Informations-sicherheitsvorfälle ist wenigstens in folgenden Fällen 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.		
2.4	**Anforderungen an die Informations-sicherheitsorganisation** Die Sicherheitsorganisation sieht wenigstens vor, dass die Durchführungsstelle einen Informationssicherheitsbeauftragten (ISB) bezeichnet und weitere Personen, die eine Schlüsselrolle in der Umsetzung der Informationssicherheit haben. Der ISB hat namentlich die folgenden Aufgaben:	A 6.1 (A.6.1.1-A.6.1.3)	

	• Er koordiniert die Aspekte der Informationssicherheit innerhalb der Durchführungsstelle sowie mit allfälligen beauftragten Leistungserbringern (z.B. IT-Beauftragten, Lieferanten, etc.). • Er ist Ansprechpartner der Informationssicherheitsbeauftragten der IT-Leistungserbringer. • Er ist Ansprechpartner gegenüber dem BSV für Informationssicherheitsvorfälle für welche die von den Durchführungsstellen erlassenen Informationssicherheitsleitlinien die Information des BSV vorsehen (Rz 2.3 Ziff 3). • Er prüft die Dokumentationen zur Informationssicherheit (insbesondere die ISDS-Dokumentationen vgl. Rz 2.8.2 und 2.8.3) und zur weiteren Umsetzung der Mindestanforderungen sowie der anerkannten Umsetzungsregelung der Fachorganisation der Durchführungsstellen im Bereich der Informationssicherheit. Für FAK nach Art. 14 Bst. a FamZG ist die Dokumentation in Bezug auf die anerkannte Umsetzungsregelung nur zu prüfen, wenn dies die kantonalen Vorschriften vorsehen. • Er informiert den Leiter der Durchführungsstelle regelmässig über den aktuellen Stand der Aspekte der Informationssicherheit in ihrer Organisation. • Er gibt Empfehlungen zuhanden der Geschäftsleitung der Durchführungsstelle ab.		Besondere Regelung bei FAK (evt. Kanton)
2.5.	**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 regeln die Abwicklung von Projekten im Bereich Informationssysteme. 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	A.6.1.5 A.8.1.3 A.8.2 (A.8.2.1, A.8.2.2, A.8.2.3)	

	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.[10]	Bei Ziff. 2 zusätzlich nationaler Datenschutz	
2.6	**Informationssicherheit bei Mobilgeräten und Telearbeit** Die Durchführungsstellen regeln • Die Rahmenbedingungen, unter welchen Telearbeit 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. • Die sichere Telearbeit mit unterstützenden Sicherheitsmassnahmen zum Schutz von Informationen, auf die von Telearbeitsplätzen aus zugegriffen wird oder die dort verarbeitet oder gespeichert werden. Dabei müssen für private Geräte, die geschäftlich genutzt werden, mindestens die gleichen Bedingungen hinsichtlich Informationssicherheit und Datenschutz gelten, wie für die von der Durchführungsstelle bereitgestellten Geräte.	A.6.2.1, A.6.2.2	
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),	A.7 (A.7.1-A.7.3)	Wir müssen sicherstellen, dass die Vorgaben nicht inkompatibel sind mit andere Vorschriften (z.B. Personal VO)

[10] Bei Verwendung von Hermes als Projektmanagementmethode sind die Anforderungen an die Datenschutz-Folgenabschätzung nach nDSG (vgl. Rz 2.8.2 Bst. h und Rz 2.8.3 Bst. c) wohl grundsätzlich erfüllt (vgl. Botschaft des Bundesrates zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse vom 15. September 2017 (BBl 2017 7059))

	der Risiken in Bezug auf die persönliche Integrität erkennen lässt und adäquate Massnahmen erlaubt.		
2.7.2	**Information und Schulung** Die Durchführungsstellen sorgen dafür, dass das eingesetzte Personal regelmässig über die Pflichten bezüglich der Informationssicherheit im Bilde ist und diesbezüglich sensibilisiert ist.	A.7.2	
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.7.1-A.7.3	
2.8	**IS-Schutzobjekte: Inventar, ISDS-Dokumentationen und weitere Anforderungen**	A.8.1	
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.8.1.1	
2.8.2	**ISDS-Basisdokumentation** 1. Bei allen IS-Projekten (Rz. 2.5) ist vorab eine Analyse zur Informationssicherheit und zum Datenschutz zu erstellen. 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; b. Klassifizierung der Verfügbarkeitsanforderungen (inkl. Beurteilung des Schutzobjekts in Bezug auf die Einteilung als geschäftskritische Anwendung); c. Klassifizierung der Vertraulichkeitsanforderungen;	A.8.1.3 A.8.2 (A.8.2.1, A.8.2.2, A.8.2.3)	

	d. Klassifizierung der Integritäts- und Nachvollziehbarkeitsanforderungen (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 nDSG). 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 nDSG 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 5.		
2.8.3	**Erweiterte ISDS-Dokumentation** Die erweiterte ISDS-Dokumentation ist zu erstellen, wenn mit dem Schutzobjekt besonders schützenswerte Personendaten bearbeitet werden (RZ 2.8.2 Ziff. 3). Sie umfasst wenigstens folgende Themen:: a. Zusammenfassung der relevanten Ergebnisse der ISDS-Basisdokumentation b. Sicherheitsrelevante Systembeschreibung b.1 Ansprechpartner / Verantwortlichkeiten b.2 Beschreibung des Gesamtsystems b.3 Beschreibung der zu bearbeitenden Daten (Bearbeitungsreglement mit Rollenkonzept und Handhabung von Datenträgern) b.4 Architekturskizze / Kommunikationsmatrix b.5 Beschreibung der zugrundeliegenden Technik c. Risikoanalyse (soweit notwendig mit Datenschutz-Folgenabschätzung), Schutzmassnahmen und verbleibende	A.8.1.3 A.8.2 (A.8.2.1, A.8.2.2, A.8.2.3)	

	Restrisiken (gegebenenfalls mit Stellungnahme des EDÖB) d. Wiederherstellung des Geschäftsbetriebes/ Notfall-Konzept (Katastrophen-Vorsorge, K-Vorsorge) e. Einhaltung / Überprüfung / Abnahme der Schutzmassnahmen f. Ausserbetriebnahme 3. Die erweiterte ISDS-Dokumentation orientiert sich qualitativ und quantitativ am Muster gemäss Anhang 6.		
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.		
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.8.1.2	
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 Benutzerkonen und Berechtigungen; und stellt sicher, dass d. sämtliche Zugriffe (inkl. automatisierten Prozessen mit machine-to-machine-Zugriff) auf Informationssysteme mit einer dem Schutzbedarf entsprechenden Authentifikation und nötigenfalls adäquate kryptographischen Massnahmen (ISO A.10) gemäss der Zugriffmatrix geschützt werden (siehe auch Rz 2.13.2); e. den Benutzern der Zugriff auf Informationssysteme nur die Rechte	A.9 (A.9.1, A.9.2, A.9.3, A.9.4)	

	eingeräumt werden, die sie zur Erfüllung ihrer Aufgaben benötigen; f. die Richtigkeit und Zweckmässigkeit der erteilten Benutzerrechte wenigstens jährlich durch den AV geprüft werden.		
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 Autorithy (CA) ausgestellt sein. Als Beispiele können folgende nicht abschliessend aufgezählte Anwendungsfälle erwähnt werden: - Mozilla-anerkannte Zertifikate für WEB-Technologielösungen, etc. - SAS-anerkannte Zertifikate für elektronische Signaturen gemäss Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (VZertES SR 943.032)[11]. - 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.10.1.1 A.10.1.2	
2.11 2.11.1	**Physischer Schutz** **Sicherheitsdispositiv für Räumlichkeiten** Die Durchführungsstellen verfügen über ein Sicherheitsdispositiv zum physischen Schutz ihrer Informationssysteme. Dabei sind verschiedene Massnahmen vorzusehen, welche den adäquaten Schutz der einzelnen Schutzobjekte gewährleisten, und zwar unter Berücksichtigung der Ergebnisse der ISDS-Prüfung (Rz 2.8.2. bzw. 2.8.3) hinsichtlich der Schutzgruppen (vgl. Rz. 2.8.2 Ziffer 2 Bst. i). Die im Sicherheitsdispositiv vorzusehenden Massnahmen müssen sich auf folgende Punkte beziehen: • Physische Sicherheitsperimeter (Lage der Umgebung und bauliche Massnahmen)	A.11.1.1-A.11.1.4	

[11] siehe dafür die BAKOM Webseite

	• Physische Zutrittssteuerung • Sichern von Büros, Räumen und Einrichtungen • Schutz vor externen und umweltbedingten Bedrohungen		
2.11.2	**Massnahmen für Geräte und Betriebsmittel** Die Durchführungsstellen und ihre Dienstleister (vgl. Rz 2.15) verfügen über dokumentierte Massnahmen zum Schutz von Geräten und Betriebsmittel gegen Verlust, Beschädigung, Diebstahl oder Gefährdung. Die vorzusehenden Massnahmen für Geräte müssen sich auf folgende Punkte beziehen: • Platzierung und Schutz von Geräten und Betriebsmitteln • Versorgungseinrichtungen • Sicherheit der Verkabelung • Instandhalten von Geräten und Betriebsmitteln • Entfernen von Werten • Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten • Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln • Unbeaufsichtigte BenutzergeräteRichtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren	A.11.2.1-11.2.9	
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. technischer Schwachstellen	A.12 A.12.1(A.12.1.1-A.12.1.4) A.12.2 A.12.3 A.12.4 A.12.5 A.12.6.	

	• Handhabung von technischen Schwachstellen • Einschränkung von Softwareinstallation G. Integritätsprüfung bei erhöhtem Schutzbedarf (vgl. Anhang 5, erweiterte ISDS-Dokumentation bst. D) H. Audit von Informationssystemen • 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.12.7	
2.13	**Kommunikationssicherheit (Informationsübertragung)**		
2.13.1	**Architekturdokumentation** Die Durchführungsstellen verfügen über eine Architekturdokumentation der Umgebung ihrer Informationssysteme. Diese gibt Auskunft über • die grundlegenden eigenen und fremden Netzwerktopologien der im Rahmen ihres Werteinventars (vgl. Ziff. 2.8.1) genutzten Netze. • die grundlegende Netztopologie beinhaltet ihre aktiven Komponenten und deren Konfigurationen,		
2.13.2	**Zugriffsmatrix** Die Durchführungsstellen verfügen über eine verbindliche Zugriffmatrix, die festlegt, wie Personen und automatisierte Prozesse (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 müssen Richtlinien zur Netzwerksicherheit vorsehen und die Zuständigkeiten zur Verwaltung von Netzwerken und Netzwerkübergängen festlegen. 2. Für Netze, welche in der Verantwortlichkeit der Durchführungsstellen liegen, verfügen die	A.13.1	

	Durchführungsstellen über ein Nutzungsreglement, welches wenigstens die folgenden Punkte vorsieht: • Anschluss von fremden Kommunikationsendgeräten • Regelung der Netzübergänge • Remote Access 3. Die Durchführungsstellen müssen festlegen, 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.13.1, A.13.2 A.13.1.2 A.13.1.2	
2.13.4	**Geschützte Informationsübertragung** 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). 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. Email Verschlüsselung).	A.13.2 (A.13.2.1-A.13.2.4)	
2.14	**Anschaffung, Entwicklung und Instandhaltung von Informationssystemen** Die Durchführungsstellen stellen sicher, dass die Sicherheit über den gesamten Lebenszyklus von Informationssystemen hinweg fester Bestandteil dieser Systeme ist. Spezifische	A.14.1	

	Sicherheitsanforderungen, welche sich aus der Informationssicherheit und dem Datenschutz (vgl. Rz 2.5, 2.8.2 und 2.8.3) ergeben, sind zu berücksichtigen. Die ISDS-Dokumentationen (Rz. 2.8.2 bzw. 2.8.3) sind bei Änderungen zu aktualisieren. Werden keine Änderungen am Informationssystem vorgenommen, sollen die ISDS-Dokumentationen wenigstens alle 5 Jahre auf ihre Aktualität überprüft werden. Für Änderung 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.	A.14.2 A.14.3	
2.15	**Verträge mit Dritten (Lieferantenbeziehungen)** • 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 Mindestanforderungen, welche die Leistungen konkret betreffen, beachtet werden und sehen im Vertrag entsprechende Kontrollmassanahmen, sowie Konventionalstrafen für den Fall der Verletzung dieser Vorschriften vor. • 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 und das Vertragsverhältnis im Falle einer Nichtbeachtung ihres Votums entsprechend	A.15.1, A.15.2	Siehe Link Strategie Cloud Bund (wenn die Public Cloud entsprechende sichernde Massnahmen hat, ist auch die Bearbeitung besonders schützenswerter Daten zulässig wenn die zuständigen Stellen informiert sind: z.B. EDöB beim Bund). Siehe auch Beispiel FINMA: Finanzmarktaufsichtsbeh

	den Regelungen des Grundvertrages aufzulösen. Auch im Falle einer Auslagerung der Verpflichtung muss durch entsprechende Abreden sichergestellt werden, dass die Mindestanforderungen vollumfänglich eingehalten werden. Dies gilt ausdrücklich auch für die Verpflichtung, ein Inventar zu führen (Rz 2.8.1) • Die Dienstleistungen für den Betrieb müssen grundsätzlich im Inland erbracht werden. Dienstleistungen für den Betrieb aus dem Ausland sind auszuweisen und zu begründen. • Es muss jederzeit sichergestellt werden, dass keine Personendaten von Versicherten im Ausland bearbeitet werden, ausser es handelt sich um eine Bearbeitung, welche von Gesetzes wegen mit einem internationalen Datenaustausch verbunden ist (z.B. Art. 32 Abs. 3 ATSG, bzw. KSBIL (vgl. Bilaterale Abkommen Schweiz-EU. Abkommen mit der EFTA. Kreisschreiben über das Verfahren zur Leistungsfestsetzung in der AHV/IV)).		örde (FINMA) Schweiz - Microsoft Compliance | Microsoft Docs
2.16	**Management von Informationssicherheitsvorfällen** Der ISB der Durchführungsstellen stellt sicher, dass Meldungen über Sicherheitsvorfälle in Zusammenhang mit Informationssystemen adäquat bearbeitet, dokumentiert und ausgewertet werden, um die Eintrittswahrscheinlichkeit oder Auswirkungen von künftige Vorfälle 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.16.1	
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 Pläne um bei Störfällen, Notfällen und Katastrophenfällen den Betrieb des IS-Schutzobjektes aufrechtzuerhalten und wiederherzustellen.	A.17.1, A.17.2	
2.18	**Richtlinienkonformität** Die Durchführungsstellen stellen sicher, dass die mit ihrem internen Kontrollsystem, Qualitätsmanagement oder Risikomanagement	A.18.1, A.18.2	

	(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.		

Rechtsbezüge zum Thema Informationssicherheit

Anhang 1

1. Nationale Rechtsquellen

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

A. Auf Bundesebene

- 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.
- Das **formelle Datenschutzgesetz** (DSG, SR 235.1) mit der Verordnung VDSG (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).
- 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 neu auch die vorliegenden Mindestanforderungen 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)
- Soweit es sich um Informationssysteme von Bundesbehörden (z.B. der ZAS) handelt, gelten zahlreiche weitere Vorschriften (RVOG SR 172.10, BinfV SR 172.010.58, Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung CyRV SR 120.73 und weitere Vorgaben des nationalen Zentrums für Cybersicherheit NCSC[2]). Mit Inkrafttreten des Informationssicherheitsgesetzes vom 18. Dezember 2020 (ISG)[12] kommt 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.

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

[12] BBl **2020** 9975

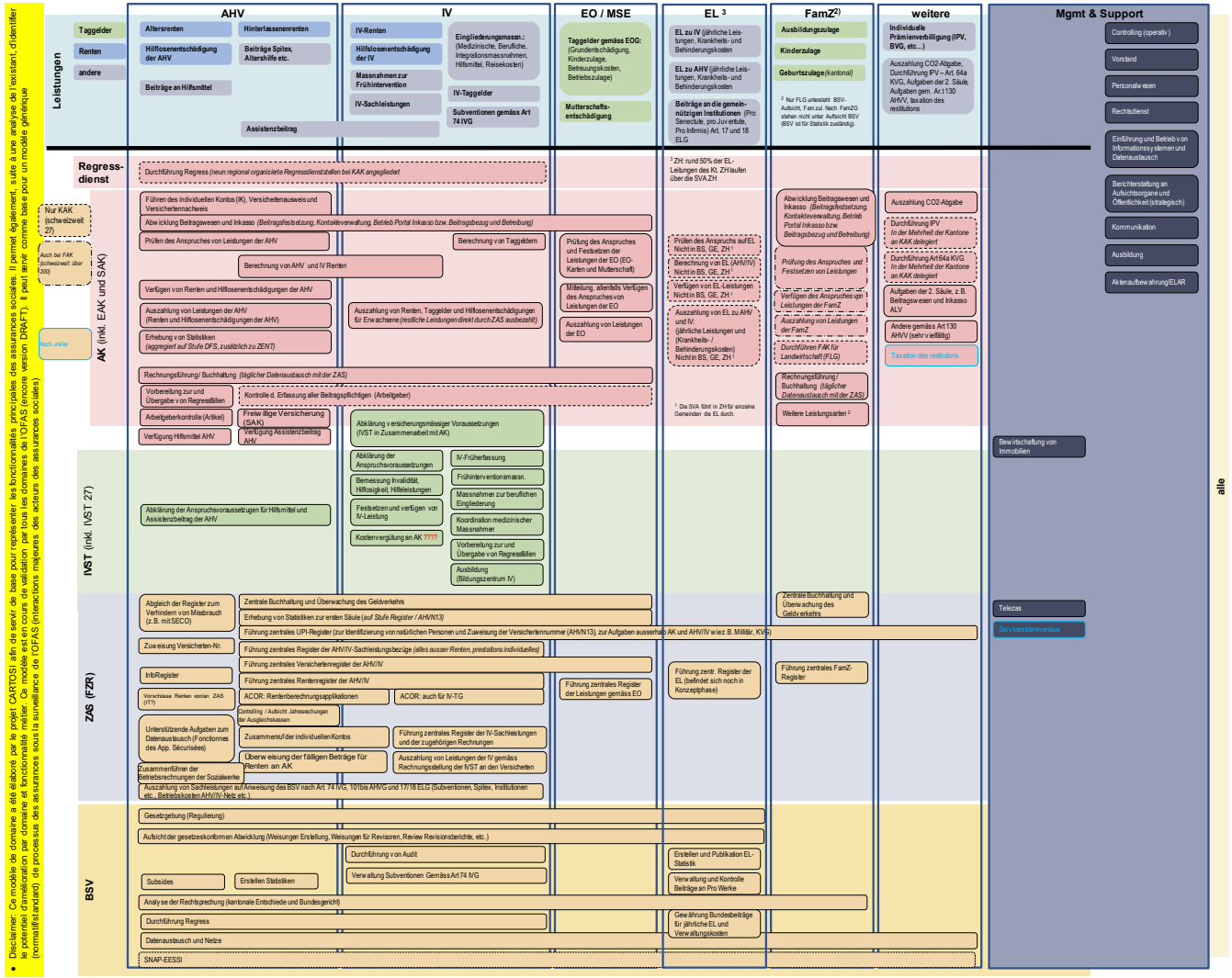
Da es sich bei Informationstechnik- und –sicherheit nicht um ein national beschränktes Thema handelt, stützten sich weltweit Handelsunternehmen, staatliche Organisationen und Non-Profitorganisationen auf diese Normen ab. In der Schweiz hat dies zur Folge, dass Inhalte der ISO-Normen in die Gesetzgebung und deren Umsetzung einfliessen. Als Beispiele seien erwähnte

- dass die Vorgaben IKT-Grundschutz in der Bundesverwaltung auf die ISO-Standards verweisen
- dass die Zertifizierung nach Artikel 11 DSG (welche z.B. für die Datenannahmestellen Krankenversicherer gemäss Art. 59a Abs. 6 KVV[13] obligatorisch ist) insbesondere davon abhängt, ob die ISO-Normen 27001 erfüllt sind (vgl. Ziffer 4 der Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem vom 19. März 2014). Die Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem und deren Anhang stellen zwischen den nationalen Datenschutzvorschriften (DSG und VDSG), 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 7 DSG). Zusätzliche auf rein nationaler Gesetzgebung beruhende Massnahmen werden explizit analog zu ISO 27002 strukturiert.

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

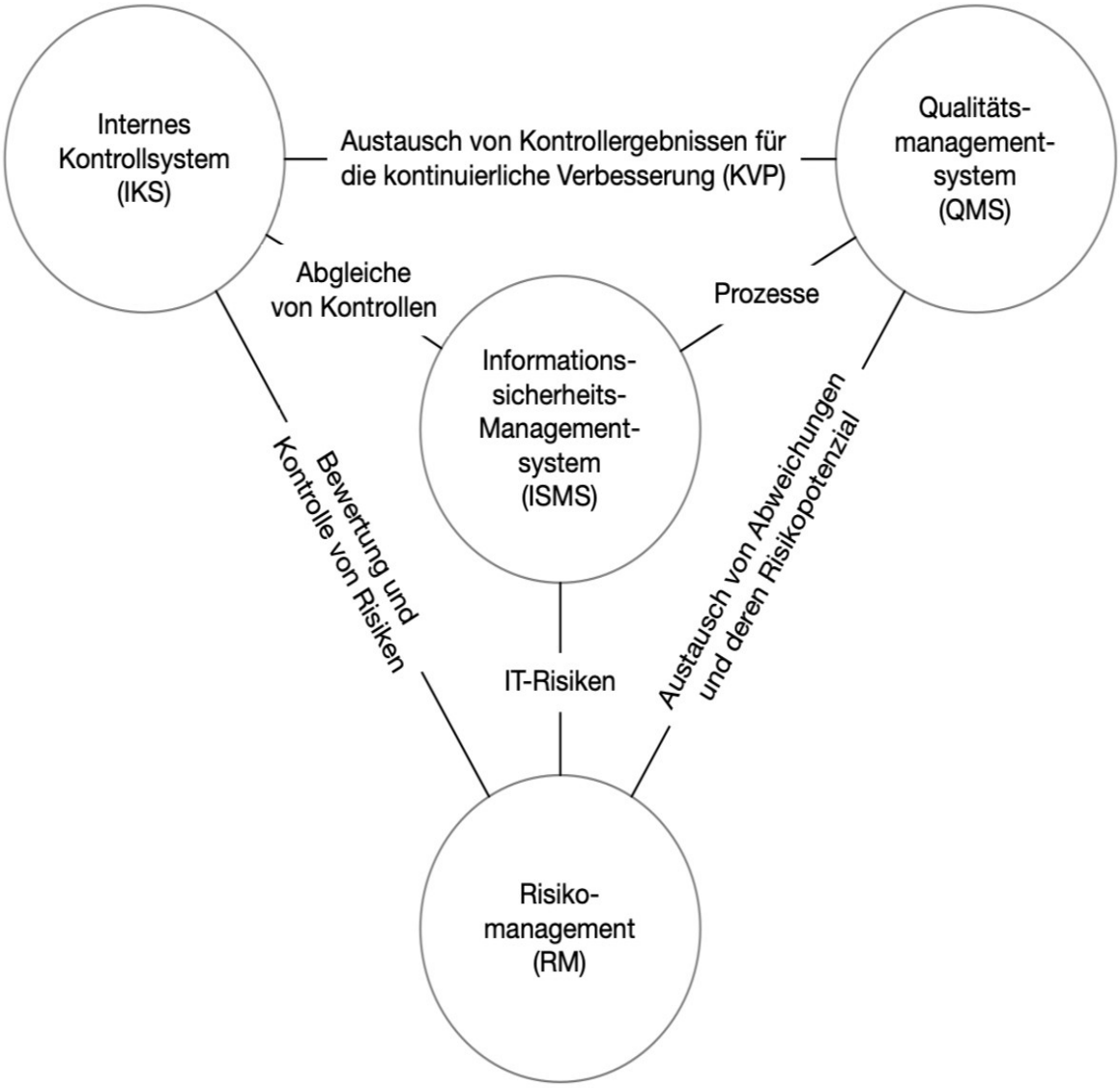
Fachdomänenmodell 1. Säule/FamZ (Stand Feb. 2021)

Anhang 2



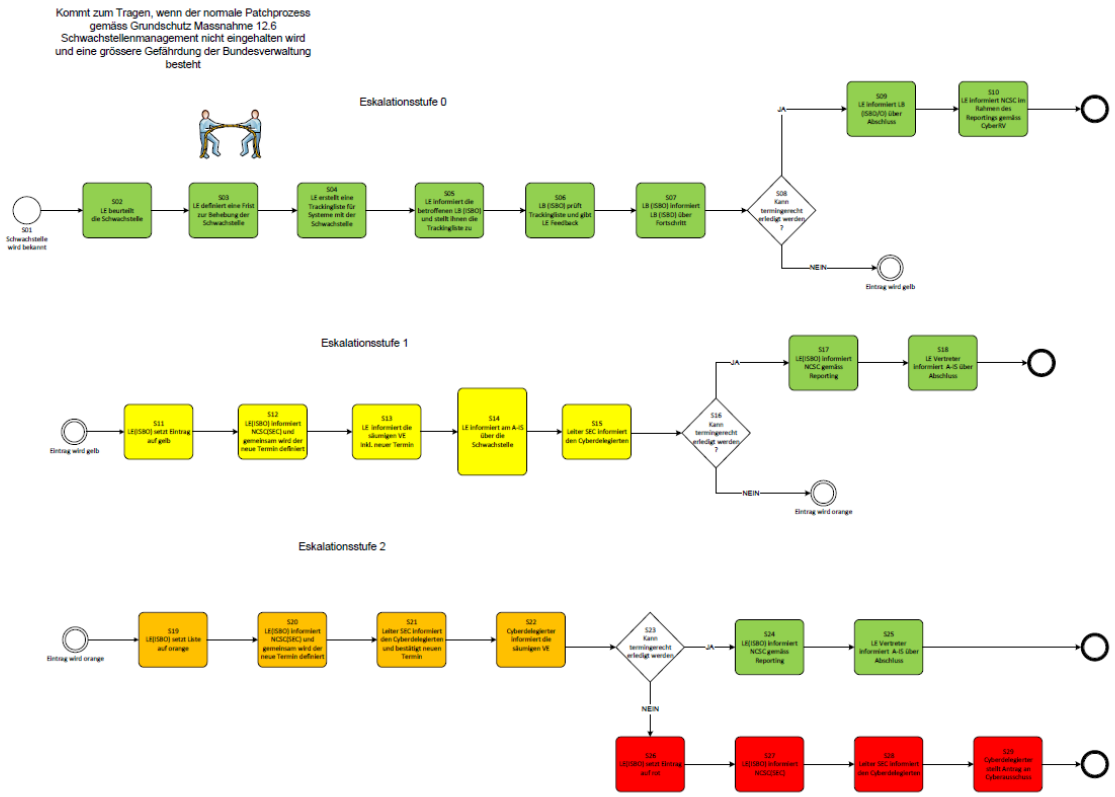
Anhang 3

Quelle: eAHV/IV Information security Konzept



Anhang 4

Beispiel zur Sicherheitsvorfallbearbeitungsprozess nach Ziffer 2.3: der Prozess sollte die Entscheidungen zur Information des BSV und des EDÖB enthalten (definitives Beispiel folgt später).



Anhang 5

Muster ISDS-Basisdokumentatiom

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

Allgemeine Vorbemerkungen / Erläuterung
Jede Durchführungsstelle ist Organ einer bundesrechtlich geregelten Sozialversicherung, und insofern ist sie zur Ausübung der gesetzlich vorgesehenen Aufgabe berechtigt und verpflichtet (Legalitätsprinzip). Als Grundlage ihres Handelns dient das jeweilige Spezialgesetz (AHVG, IVG etc.). Setzt sie zur Aufgabenerfüllung Informationssysteme ein, kommen aus anderen Bereichen als aus dem Spezialgesetz Rechtseinflüsse hinzu. Einesteils gilt das ATSG – beispielsweise für die Amts- und Verwaltungshilfe (Art 32 ATSG), die Schweigepflicht (Art. 33 ATSG) und den elektronischen Datenaustausch (E-Art. 76bis E-ATSG). Andererseits sind Vorschriften zur Informationssicherheit bzw. zum Datenschutz und zur Datensicherheit aus dem DSG 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 nDSB), zur Erstellung einer Datenschutz-Folgenabschätzung (Art. 22 nDSG) oder zur Meldung von Verletzungen der Datensicherheit (Art. 24 nDSG) einhalten.
- Soweit die kantonalen Datenschutzgesetzgebungen vergleichbare Regelungen kennen, haben die kantonalen Durchführungsstellen zu prüfen welche Verpflichtungen sich daraus für sie ergeben.

Muster-Schema 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 nDSG, • Verhältnismässigkeit und Zweckmässigkeit der Datenbeschaffung und Datenbearbeitung, unter Einhaltung des Grundsatzes von Treu und Art. 6 Abs. 2 und 3 nDSG	Artikel 49b AHVG bzw. neu Art. 49f E-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 (nDSG 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?

	Fragestellung/Thema	Rechtliche Grundlage	Konsequenz, Beispiel
			Treu und Glauben: Wenn eine betroffene Person keinesfalls damit rechnen muss, dass ihre Daten im vorliegenden Fall bearbeitet werden, ist der Grundsatz verletzt. **Beispiel Einordnung E-Mail Applikation einer privaten AHV-Ausgleichskasse 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 E-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 nDSG). Die Datenbeschaffung wird durch das nDSG zwar eingeschränkt (in Art. 6 Abs. 3, Art. 19), indessen sind diese Einschränkungen bei einer entsprechenden gesetzlichen Grundlage obsolet (inbes. Art. 20 nDSG). Im Rahmen der Mitwirkungs- und Meldepflichten wird in den Sozialversicherungsgesetzen jedoch oft	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 privaten AHV-Ausgleichskasse 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-

	Fragestellung/Thema	Rechtliche Grundlage	Konsequenz, Beispiel
		ein Teil des Datenzuflusses reglementiert. Darüber hinaus bestehen aufgrund von Regelungen zu einzelnen Informationssystemen automatisierte Meldungen (z.B. Zivilstandsmeldungen an die AHV). Schliesslich garantiert das ATSG die Amts- und Verwaltungshilfe in Einzelfällen. Für die Datenbekanntgabe sieht das nDSG 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.	und abflusses muss vom entsprechend ausgebildeten Nutzer geprüft werden. Es ist sicherzustellen, dass die Nutzer diese Ausbildung erhalten und allenfalls mit technischen und organisatorischen Massnahmen die die Identität des Empfängers von Daten klären können.
3	Datenrichtigkeit und Datenberichtigung (Art. 6 Abs. 5 und 41 Abs. 2 nDSG)	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 privaten AHV-Ausgleichskasse 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.

	Fragestellung/Thema	Rechtliche Grundlage	Konsequenz, Beispiel
4	Auskunftsrecht (Art. 25 nDSG)	Art. 25 nDSG postuliert ein Auskunftsrecht jeder Person. Dieses verpflichtet den Verantwortlichen, Auskunft zu geben. Eingeschränkt wird dieses Auskunftsrecht durch Art. 26 und 27 nDSG. Zudem kann die Person verlangen, dass die Daten herausgegeben werden, wiederum unter gewissen Einschränkungen (Art. 28 und 29 nDSG)	In der ISDS-Basis-Dokumentation ist zu analysieren, wie sämtliche einer Person zuzuordnenden Daten im Informationssystem eruierbar sind. Der Prozess für die Behandlung von Auskunftsbegehren ist zu dokumentieren. In der ISDS-Basis-Dokumentation ist zu klären, ob im Informationssystem Daten über die Gesundheit enthalten sein können, welche – mit Einwilligung der betroffenen Person - über die von ihr bezeichnete - Gesundheitsfachperson mitgeteilt werden (Art. 25 Abs. 3 nDSG). **Beispiel Einordnung E-Mail Applikation einer privaten AHV-Ausgleichskasse in der ISDS-Basis-Dokumentation:** Im Rahmen der ISDS-Basis-Dokumentation ist sicherzustellen, dass auf die E.Mails einer bestimmten Person zugegriffen werden kann. Dies kann auch über die Definition eines Prozesses bei einem andern Informationssystem wie einer Geschäftsverwaltung sichergestellt werden. In der SSDS-Basis-Dokumentation zur E-Mail-Applikation ist darauf zu verweisen.
5	Klärung der Aufnahme in das Verzeichnis bzw. Meldung bei einer Behörde des Datenschutzes	In der 1. Säule tätige Bundesorgane (also z.B. die Eidg. Ausgleichskasse oder die Schweizerische Ausgleichskasse der AHV) sowie Durchführungsstellen, die vom DSG als «Bundesorgane» betrachtet werden (also alle nicht kantonalen Durchführungsstellen) müssen die Vorschriften zum Verzeichnis ihrer Bearbeitungstätigkeiten einhalten und die Verzeichnisse dem EDÖB melden (Art. 12 nDSB),.	

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

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

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

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

Fragestellung bzw. Anforderung	**Kriterien**	**Schutzbedarf erhöht? > erweiterte ISDS-Dokumentation nach Rz 2.8.3 nötig?** *(statt Dokumentation , insbesondere Risikoanalysen und Sicherheitsanforderungen)*	**Schutzmassnahmen**
Werden Daten gemäss Datenschutzgesetzgebung bearbeitet? Wenn ja, welche Art von Personendaten sind betroffen?	keine Personendaten	nein	Umschreibung der vorhandenen Basis-Schutzmassnahmen
	Personendaten	nein	Umschreibung der vorhandenen Schutzmassnahmen
	besonders schützenswerte Personendaten (Art. 5 Bst c nDSG? und /oder Profiling (automatisierte	Ja Ja	Umschreibung der besonderen Schutzmassnahmen

	Bewertung; vgl. Art. 5 Bst. f nDSG)?[14] Wenn ja Profiling: mit hohem Risiko (vgl. Art. 5 Bst. g nDSG?)	Ja	
In welcher Klassifizierungsstufe befinden sich die Daten des Schutzobjektes?	Öffentlich Intern Vertraulich Streng vertraulich	Nein Nein Ja Ja	Die Klassifizierung sollte in einer Folgeversion definiert werden.

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

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

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

E. Datenhaltung

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

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

F: Beschreibung des Schutzobjekts / Projekts

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

G. Verzeichnispflicht/Meldepflicht

Grundsätzlich besteht nach Rz 2.8.1 für alle Informationssysteme eine Inventarpflicht. Darüber hinaus gilt nach Artikel 12 nDSG 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 Botschaft des Bundesrates zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse vom 15. September 2017[15] 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 nDSG (Art. 22) gilt auch hier für die Durchführungsstellen (ausser die kantonalen Durchführungsstellen). Für die kantonalen Durchführungsstellen gilt eine allfällige kantonale Pflicht für die Datenschutz-Folgenabschätzung.

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

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

- ob eine besonders umfangreiche Bearbeitung besonders schützenswerter Daten erfolgt
- ob neue Technologien verwendet werden
- die beschriebene Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen darstellt (vgl. Art. 22 Abs. 1 bis 3 nDSG)

[15] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (admin.ch), **BBl 2017** 7059

- welche bereits bekannten oder noch zu entwickelnden Massnahmen zum Schutz der Persönlichkeit und der Grundrechte vorgesehen sind.

I. Zuweisung zu einer Schutzgruppe

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

Anhang 6

Muster für die erweiterte ISDS-Dokumentation nach Rz 2.8.3

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

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

b.1 Ansprechpartner / Verantwortlichkeiten

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

b.2 Beschreibung des Gesamtsystems
Beschreibung der sicherheitsrelevanten Funktionalitäten wie Zugangssteuerung (vgl. Rz 2.9), Betriebssicherheit (vgl. Rz 2.12) und Leistungen der Dritten (vgl. Rz 2.15).
Es können auch Verweise auf entsprechende Dokumentationen gemacht werden (z.B. Netzwerksicherheit- und Dokumentation vgl. 2.13.3).

Die Beschreibung sollte einem Unbeteiligte 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 5, Bst. A insbesondere:
- Erfüllung einer allfälligen Anmeldpflicht beim Datenschutzbeauftragten des Kantons oder des EDÖB
- Erstellung eines Bearbeitungsreglements
  Hilfe dazu finden Sie im Template
  https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/dokumentation/vorgaben/prozesse/p042/P042-Hi04-Bearbeitungsreglement_V2-1-d.docx.download.docx/P042-Hi04-Bearbeitungsreglement_V2-1-d.docx sowie in der Verordnung zum DSG und unter dem Link *Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes*
  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 (eventuell mit Datenschutz-Folgenabschätzung), Schutzmassnahmen, und Restrisiken

Das ISDS Konzept gibt Auskunft über die Restrisiken, die nach einer Risikoanalyse und den berücksichtigten Schutzmassnahmen verbleiben. Die Risikoanalyse berücksichtigt – sofern die Notwendigkeit einer Datenschutz-Folgenabschätzung in der ISDS-Basisdokumentation festgestellt wurde - 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
Diese enthält gemäss Gesetz (Art. 22 Abs. 3 nDSG)

- 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

Steht aufgrund der bereits erfolgten Analysen fest, dass eine umfangreiche Bearbeitung besonders schützenswerter Personendaten erfolgt, sollte in die Risikoanalyse die Folgenabschätzung integriert werden. Zu beurteilen sind die sich aus der konkreten Bearbeitung ergebenden Probleme in Bezug auf den

Persönlichkeitsschutz (privatrechtlich; Art. 28 ZGB)
Die Persönlichkeit umfasst alle physischen, psychischen, moralischen und sozialen Werte einer Person, die ihr kraft ihrer Existenz zukommen.[16] 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.

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¨

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

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 des Kantons SG

oder

https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/datenschutz/publikationen/formulare-merkblaetter/formular_dsfa.docx)

- Die Risikomatrix

Die detaillierte Risikoanalyse kann anhand einer NCSC Excel-Datei vorgenommen werden. Als Ergebnis der Risikoanalyse sind Schutzmassnahmen zu definieren und die Restrisiken zu beschreiben. 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 nDSG zu konsultieren .

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

d. Wiederherstellung des Geschäftsbetriebes/Notfall Konzept (Quelle NCSC ISDS Vorlage)

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

e. Einhaltung / Überprüfung / Abnahme der Schutzmassnahmen

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

Beschrieben wird auch die Systemabnahmeprüfung:
Neue und aktualisierte Systeme müssen während der Entwicklungsprozesse eine gründliche Überprüfung und Verifizierung erfahren, einschließlich der Vorbereitung einer detaillierten Planung der Aktivitäten, Testeingaben und erwarteten Ausgaben unter verschiedenen Bedingungen. Wie bei internen Entwicklungsvorhaben sollten derartige Prüfungen zunächst vom Entwicklungsteam durchgeführt werden. Danach sollten unabhängige Abnahmeprüfungen unternommen werden (sowohl bei internen als auch bei ausgelagerten Entwicklungsvorhaben), um sicherzustellen, dass das System wie erwartet (und nur wie erwartet) funktioniert (siehe ISO/IEC 27002:2013 Kapitel 14.1.1 und 14.1.2). 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).

Abkürzungsverzeichnis

Abkürzung	**Benennung**	**Link**
Abs.	Absatz	
AHV	Alters- und Hinterlassenenversicherung	
AHVG	Bundesgesetz über die Alters- und Hinterlassenenversicherung, SR 831.10	https://www.admin.ch/opc/de/classified-compilation/19460217/index.html
AHVV	Verordnung über die Alters- und Hinterlassenenversicherung, SR 831.101	https://www.admin.ch/opc/de/classified-compilation/19470240/index.html
AK	Ausgleichskasse	
Art.	Artikel	
ATSG	Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts, SR 830.1	https://www.admin.ch/opc/de/classified-compilation/20002163/index.html
AV	Anwendungsverantwortlicher	
BBl	Bundesblatt	
BCM	Business Continuity Management	
BinfV	Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung, SR 172.010.58	https://www.admin.ch/opc/de/classified-compilation/20081009/index.html
BIT	Bundesamt für Informatik und Telekommunikation	
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft, SR 101	https://www.admin.ch/opc/de/classified-compilation/19995395/201801010000/101.pdf
CA	Certificate Authority, Zertifizierungsstelle	
DS	Durchführungsstellen	
DSG	Bundesgesetz über den Datenschutz, SR 235.1	https://www.admin.ch/opc/de/classified-compilation/19920153/index.html#a5
eAHV/IV	Verein der Durchführungsstellen der AHV und IV	https://www.eahv-iv.ch/de/
E-AHVG	Entwurf zur Änderung des AHVG (BBl 2020 109), gemäss Botschaft zur Änderung des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (Modernisierung der Aufsicht in der 1. Säule und Optimierung in der 2. Säule der Alters-, Hinterlassenen- und Invalidenvorsorge (BBl 2020 1)	
E-Art.	Entwurf zu Artikel	
eCH	Verein, der Standards setzt im e-Government	https://www.ech.ch/en
EDÖB	Eidgenössischer Datenschutz- und Öffenlichkeitsbeauftragter	https://www.edoeb.admin.ch/edoeb/de/home.html
EL	Ergänzungsleistungen	

Abkürzung	Benennung	Link
ELG	Bundesgesetz über Ergänzungsleistungen zur Alters-, Hinterlassenen- und Invalidenversicherung, SR 831.30	https://www.admin.ch/opc/de/classified-compilation/20051695/index.html
EO	Erwerbsersatzordnung	
EOG	Bundesgesetz über den Erwerbsersatz für Dienstleistende und bei Mutterschaft, SR 834.1	https://www.admin.ch/opc/de/classified-compilation/19520192/index.html
FamZG	Bundesgesetz über die Familienzulagen, SR 836.2	https://www.admin.ch/opc/de/classified-compilation/20042372/index.html
FamZV	Verordnung über die Familienzulagen, SR 836.21	https://www.admin.ch/opc/de/classified-compilation/20072165/index.html
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	
ISB	Informationssicherheitsbeauftragter (im Sinne dieser Empfehlung)	
ISDS	Informationssicherheit und Datenschutz	
ISG	Informationsschutzgesetz vom 20. Dezember 2020	BBl 2020 9975
ISMS	Informationssicherheits- Management-System	
ISO	International Organisazion für Standardization	
ISO 27001	ISO/EC 27001, 2013 + Cor 1:2014) betreffend Informationstechnologie – IT Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (mit normativem Anhang 1 betr. Referenzmassnahmenziele und –massnahmen, welche aus ISO/IEC 27002 abgeleitet wurden)	
ISO 27001	ISO/IEC27002: 2013 + Cor 1:2014 + Cor 2:2015, Informationstechnologie – IT-Sicherheitsverfahren – Leitfaden für Informationssicherheits-Massnahmen	
IT	Informationstechnologie	
IV	Invalidenversicherung	
IVG	Bundesgesetz über die Invalidenversicherung, SR 831.20	https://www.admin.ch/opc/de/classified-compilation/19590131/index.html
KSSD	Kreisschreiben über die Schweigepflicht und die Datenbekanntgabe in der AHV/IV/EO/EL/FamZLw/FamZ	https://sozialversicherungen.admin.ch/de/d/6435
KVV	Verordnung über die Krankenversicherung vom 27. Juni 1995, SR 832.102	https://www.admin.ch/opc/de/classified-compilation/19950219/index.html
LE	Leistungserbringer	
NCSC	Nationales Zentrum für Cybersicherheit	Sicherheitsverfahren (admin.ch)

Abkürzung	Benennung	Link
nDSG	Revision des Datenschutzgesetzes (nDSG) vom 25. September 2020 (BBl 2020 7639)	BBl 2020 7639 - Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) (admin.ch)
nVDSG	Neue Verordnung zum neuen Datenschutzgesetz	Noch nicht verabschidete Verordnungsänderung zur VDSG
QMS	Qualitätsmanagementsystem	
RM	Risikomanagementsystem	
RVOG	Regierungs- und Verwaltungsorganisationsgesetz, SR 172.10	https://www.admin.ch/opc/de/classified-compilation/19970118/index.html
Rz/Rzn	Randziffer, Randziffern	
VDSG	Verordnung zum Bundesgesetz über den Datenschutz, SR 235.11	https://www.admin.ch/opc/de/classified-compilation/19930159/index.html
VO	Verordnung	
Vorgaben NCSC[2]	Das nationale Zentrum für Cybersicherheit NCSC hat verschiedene Vorgaben erlassen.	Sicherheit (admin.ch)
VwVG	Bundesgesetz über das Verwaltungsverfahren, SR 172.021	https://www.admin.ch/opc/de/classified-compilation/19680294/index.html
WAF	Weisung über die Aktenführung in der AHV/IV/EO/EL/FamZLw/FamZ	https://sozialversicherungen.admin.ch/de/d/6921/download
ZAS	Zentrale Ausgleichsstelle	
ZertES	Bundesgesetz über die elektronische Signatur; SR 943.03	https://www.admin.ch/opc/de/classified-compilation/20131913/index.html