Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes (IAMV)

vom 19. Oktober 2016 (Stand am 1. Mai 2025)

Der Schweizerische Bundesrat,

gestützt auf Artikel 26 und 84 Absatz 1 des Informationssicherheitsgesetzes vom 18. Dezember 2020[1] (ISG),
auf das Bundesgesetz vom 17. März 2023[2] über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG),
auf das Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997[3] (RVOG),
auf Artikel 27 Absätze 5 und 6 des Bundespersonalgesetzes vom 24. März 2000[4] und auf Artikel 186 des Bundesgesetzes vom 3. Oktober 2008[5] über militärische und andere Informationssysteme im VBS,[6]

verordnet:

1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Gegenstand

Diese Verordnung regelt für die Identitätsverwaltungs-Systeme (IAM[7]-Systeme), die Verzeichnisdienste und den zentralen Identitätsspeicher des Bundes die Zuständigkeiten, die Bearbeitung und Bekanntgabe von Personendaten und die Anforderungen an die Informationssicherheit.

Art. 2[8] Geltungsbereich

[1] Die Artikel 24 und 25 ISG sowie diese Verordnung gelten für:

a. die Verwaltungseinheiten der zentralen Bundesverwaltung nach Artikel 7 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[9] (RVOV);

b. die Armee.

AS **2016** 3623
1 SR **128**
2 SR **172.019**
3 SR **172.010**
4 SR **172.220.1**
5 SR **510.91**
6 Fassung gemäss Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).
7 IAM = *Identity and Access Management*
8 Fassung gemäss Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).
9 SR **172.010.1**

[2] Die Geltung dieser Verordnung für die Verwaltungseinheiten der dezentralen Bundesverwaltung nach Artikel 2 Absatz 3 RVOG und Organisationen nach Artikel 2 Absatz 4 RVOG richtet sich nach Artikel 2 Absätze 2 Buchstabe b und 3 der Informationssicherheitsverordnung vom 8. November 2023[10] (ISV).

2. Abschnitt: Zweck und grundsätzliche Funktion der Systeme

Art. 3 IAM-Systeme

[1] Der Zweck eines IAM-Systems ist es, Daten über die Identität und die Berechtigungen von Personen, Maschinen und Systemen gebündelt zu verwalten, um sie nachgelagerten Systemen und anderen IAM-Systemen auf Anfrage zur Verfügung zu stellen.

[2] Die nachgelagerten Systeme sind Fachanwendungen oder vermitteln den Zugang zu Informationen, Informatikmitteln, Räumlichkeiten und anderen Infrastrukturen.

[3] Im Einsatz prüft das IAM-System als vorgelagertes System die Identität und bestimmte berechtigungsrelevante Eigenschaften von Personen, Maschinen und Systemen, die auf ein nachgelagertes System zugreifen wollen, und übermittelt das Resultat der Überprüfung an das nachgelagerte Informationssystem, damit dieses die Berechtigungen ermitteln kann.

Art. 4 Verzeichnisdienste

Der Zweck eines Verzeichnisdienstes ist es, Informationen über Benutzerinnen und Benutzer von Infrastrukturen des Bundes zu führen, um damit die Personen zu identifizieren und die ihnen zugeordneten Geräte, Anschlüsse, Kontaktangaben und dergleichen zu verwalten.

3. Abschnitt: Verantwortliche Organe

Art. 5[11] IAM-Systeme

[1] Die folgenden Bundesorgane sind für die nachstehenden IAM-Systeme der zentralen Bundesverwaltung verantwortlich:

a. der Bereich digitale Transformation und IKT-Lenkung der Bundeskanzlei (Bereich DTI) für:[12]

10 SR **128.1**
11 Fassung gemäss Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).
12 Fassung gemäss Anhang 2 Ziff. II 4 der Digitalisierungsverordnung vom 2. April 2025, in Kraft seit 1. Mai 2025 (AS **2025** 235).

1. alle als Standarddienste angebotenen oder dem Bereich DTI[13] ausdrücklich zugewiesenen IAM-Systeme einschliesslich derer Zurverfügungstellung an Kantone und Gemeinden sowie Organisationen und Personen des öffentlichen oder privaten Rechts nach Artikel 11 Absatz 3 EMBAG,
2. das IAM-System der Supportprozesse Finanzen, Beschaffung, Immobilien und Logistik einschliesslich der Cloud-Anbindungen;

b. die Direktion für Ressourcen im Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) für das von der Informatik EDA betriebene IAM-System;

c. das Generalsekretariat des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport für die von der Gruppe Verteidigung (Gruppe V) betriebenen IAM-Systeme;

d. die Eidgenössische Finanzverwaltung für das in der zentralen Ausgleichsstelle betriebene IAM-System zur Versorgung der Sozialversicherungssysteme der 1. Säule und deren Prozessunterstützung;

e. das Generalsekretariat des Eidgenössischen Departements für Wirtschaft, Bildung und Forschung (WBF) für das beim Information Service Center WBF (ISCeco) betriebene IAM-System;

f. das Bundesamt für Strassen für sein IAM-System zum Betrieb der Betriebs- und Sicherheitsausrüstungen der Nationalstrassen.

[2] Sie sorgen dafür, dass die Bearbeitung der Personendaten in den IAM-Systemen, für die sie verantwortlich sind, mindestens alle vier Jahre von einer externen Stelle überprüft wird.

[3] Die folgenden Organe sind für die nachstehenden IAM-Systeme verantwortlich:

a. die Gruppe V für die IAM-Systeme der Armee;

b. die jeweiligen Verwaltungseinheiten für die IAM-Systeme der Verwaltungseinheiten der dezentralen Bundesverwaltung;

c. die jeweiligen Organisationen für die IAM-Systeme der Organisationen nach Artikel 2 Absatz 4 RVOG.

[4] Verpflichtete Behörden nach Artikel 2 Absatz 1 Buchstaben a und c–e ISG, auf die diese Verordnung gemäss Artikel 84 Absatz 3 ISG anwendbar ist, legen fest, welche die in ihrem Bereich verantwortlichen Bundesorgane sind.

[5] Die Verantwortung für das nachgelagerte System, insbesondere für den Zugang dazu, bleibt bei der Fachstelle, die für dieses zuständig ist.

Art. 6 Verzeichnisdienste

Die für Verzeichnisdienste ausserhalb von IAM-Systemen verantwortlichen Bundesorgane sind:

13 Ausdruck gemäss Anhang 2 Ziff. II 4 der Digitalisierungsverordnung vom 2. April 2025, in Kraft seit 1. Mai 2025 (AS **2025** 235). Diese Änd. wurde im ganzen Erlass berücksichtigt.

a.[14] für die vom Bereich DTI zentral bereitgestellten IKT-Mittel: der Bereich DTI;

b. für die anderen Verzeichnisse: die Informatik-Leistungserbringer, die diese Systeme betreiben, im Einzelnen:
   1. die Informatik EDA der Direktion für Ressourcen im EDA,
   2. das Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements (ISC-EJPD),
   3.[15] die Gruppe V,
   4. das Bundesamt für Informatik und Telekommunikation (BIT),
   5. das ISCeco.

Art. 7 Geltendmachung von Rechten

Die betroffenen Personen machen ihre Rechte in Bezug auf IAM-Systeme und Verzeichnisdienste bei den folgenden Stellen geltend:

a. ihr Auskunftsrecht: bei den verantwortlichen Organen;

b.[16] ihr Berichtigungs- und Vernichtungsrecht:
   1. beim Personaldienst ihrer Verwaltungseinheit oder ihrer Organisation oder bei der sonst für die Nachführung ihrer Daten zuständigen Stelle,
   2. im Falle von Artikel 9 Buchstabe b: bei den verantwortlichen Organen.

4. Abschnitt: Bearbeitete Daten, Bezug der Daten und Aufbewahrungsfrist

Art. 8 In IAM-Systemen und Verzeichnisdiensten geführte Personen

[1] In den IAM-Systemen und den Verzeichnisdiensten können Daten über die folgenden Personen bearbeitet werden:

a. Angehörige der zentralen Bundesverwaltung nach Artikel 7 RVOV[17];

b. Angehörige der dezentralen Bundesverwaltung nach Artikel 7*a* RVOV;

c. Mitglieder der Bundesversammlung und Angehörige der Parlamentsdienste nach dem 4. Titel 7. Kapitel des Parlamentsgesetzes vom 13. Dezember 2002[18];

d. von der Bundesversammlung nach Artikel 168 der Bundesverfassung[19] gewählte Personen;

14 Fassung gemäss Anhang 2 Ziff. II 4 der Digitalisierungsverordnung vom 2. April 2025, in Kraft seit 1. Mai 2025 (AS **2025** 235).
15 Fassung gemäss Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).
16 Fassung gemäss Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).
17 SR **172.010.1**
18 SR **171.10**
19 SR **101**

e. Angehörige des Bundesgerichts, des Bundesverwaltungsgerichts, des Bundesstrafgerichts und des Bundespatentgerichts, soweit die Gesetzgebung nichts anderes vorsieht;

f. Angehörige der Bundesanwaltschaft nach den Artikeln 7–22 des Strafbehördenorganisationsgesetzes vom 19. März 2010[20] (StBOG);

g. Angehörige des Sekretariats der Aufsichtsbehörde über die Bundesanwaltschaft nach Artikel 27 Absatz 2 StBOG;

h.[21] Angehörige der Armee und des Zivilschutzes.

2 Zusätzlich können Daten bearbeitet werden von Angehörigen der folgenden Unternehmen, sofern diese Angehörigen regelmässig in Kontakt mit Stellen nach Absatz 1 stehen:

a. Schweizerische Bundesbahnen;

b. Schweizerische Post;

c. RUAG;

d. Schweizerischen Unfallversicherungsanstalt.

3 Weiter können in den IAM-Systemen und den Verzeichnisdiensten Daten über die folgenden Personen bearbeitet werden:

a. externe Personen, die für die Stellen nach Absatz 1 oder 2 tätig sind;

b. externe Personen, die aus anderen Gründen Zugang zu Informationen, Informatikmitteln, Räumlichkeiten und anderen Infrastrukturen der Bundesverwaltung haben.

Art. 9 In IAM-Systemen geführte Personen

In den IAM-Systemen können, zusätzlich zu den Daten nach Artikel 8, Daten der folgenden Personen bearbeitet werden:

a. von Angehörigen kantonaler oder kommunaler Behörden, wenn diese Personen vom Bund bereitgestellte Informationssysteme benutzen;

b.[22] von Privatpersonen und Vertreterinnen oder Vertretern von Organisationen, die auf vom Bund oder, für den Vollzug von kantonalem Recht, von Kantonen und Gemeinden sowie Organisationen und Personen des öffentlichen oder privaten Rechts bereitgestellte Informationssysteme, wie E-Government-Anwendungen, zugreifen.

Art. 10 In Verzeichnisdiensten geführte Personen

In den Verzeichnisdiensten können, zusätzlich zu den Daten nach Artikel 8, Daten von Angehörigen von kantonalen und kommunalen Behörden und von anderen als

20 SR **173.71**
21 Eingefügt durch Ziff. I der V vom 14. Nov. 2018, in Kraft seit 1. Jan. 2019 (AS **2018** 4739).
22 Fassung gemäss Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).

den in Artikel 8 Absatz 2 genannten bundesnahen Betrieben bearbeitet werden, die ein digitales Zertifikat des Bundes benutzen.

Art. 11 Kategorien von Personendaten

1 In den IAM-Systemen, den Verzeichnisdiensten und dem zentralen Identitätsspeicher nach Artikel 13 dürfen Personendaten gemäss Anhang bearbeitet werden.

2 Es darf in diesen Systemen kein Profiling nach Artikel 5 Buchstaben f und g des Datenschutzgesetzes vom 25. September 2020[23] durchgeführt werden.[24]

3 Es dürfen in diesen Systemen, sofern hierfür keine besondere rechtliche Grundlage besteht, keine besonders schützenswerten Personendaten bearbeitet werden. Davon ausgenommen ist die Bearbeitung biometrischer Daten durch IAM-Systeme zur risikogerechten Identifizierung von Personen nach den Artikeln 8 und 9 Buchstabe a (Art. 20 Abs. 2 ISG).[25]

4 Die im Anhang mit einem Stern gekennzeichneten Daten von Personen nach Artikel 8 dürfen in einem Personenverzeichnis publiziert werden, das allen darin erfassten Personen zugänglich ist.

Art. 12 Bezug von Personendaten

1 IAM-Systeme und Verzeichnisdienste können Daten der im Informationssystem Personaldatenmanagement (IPDM) geführten Personen nach Artikel 34 der Verordnung vom 22. November 2017[26] über den Schutz von Personendaten des Bundespersonals automatisch beziehen.[27]

2 Sie können Daten von nicht im IPDM[28] erfassten Personen automatisch von den jeweiligen Stellen nach Artikel 8 beziehen, sofern die entsprechende Personengruppe grundsätzlich Zugang zu Informationssystemen oder anderen Ressourcen des Bundes benötigt.

3 Sie können Daten von externen Personen mit regelmässigem Zugang zu Ressourcen des Bundes automatisch von den jeweiligen Informationssystemen beziehen.

4 Sie können Daten von externen Personen automatisch von externen IAM-Systemen beziehen, die nach den Artikeln 21–24 mit den IAM-Systemen des Bundes verbunden sind.[29]

23 SR **235.1**
24 Fassung gemäss Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).
25 Fassung gemäss Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).
26 SR **172.220.111.4**
27 Fassung gemäss Anhang 8 Ziff. II 1 der V vom 22. Nov. 2017 über den Schutz von Personendaten des Bundespersonals, in Kraft seit 1. Jan. 2018 (AS **2017** 7271).
28 Audruck gemäss Anhang 8 Ziff. II 1 der V vom 22. Nov. 2017 über den Schutz von Personendaten des Bundespersonals, in Kraft seit 1. Jan. 2018 (AS **2017** 7271).
Diese Änd. wurde im ganzen Erlass berücksichtigt.
29 Eingefügt durch Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).

Art. 13 Zentraler Identitätsspeicher als Verteiler

1 Für die Verteilung von Benutzerdaten auf die verschiedenen IAM-Systeme und Verzeichnisdienste betreibt das BIT einen zentralen Identitätsspeicher. In diesem können alle Personendaten gemäss Anhang bearbeitet werden. Verantwortliches Bundesorgan ist der Bereich DTI.

2 Das IPDM liefert die Daten gemäss Anhang soweit verfügbar regelmässig an den zentralen Identitätsspeicher. Jeder automatische Bezug von Personendaten aus dem IPDM erfolgt über diesen Verteiler. Ausgenommen ist der direkte Bezug von Personalstammdaten im SAP-Standard für die berechtigten SAP-Systeme.

3 Die Personendaten gemäss Artikel 8 Absatz 1 Buchstabe c und Absatz 3 werden den Parlamentsdiensten zur Übernahme und zum Abgleich bereitgestellt.

4 Die Daten können weiteren bundesinternen Informationssystemen automatisch zur Übernahme und zum Abgleich bereitgestellt werden, sofern das jeweilige System:

a.[30] über eine Rechtsgrundlage, welche die Bearbeitung der bereitzustellenden Daten vorsieht, und ein Bearbeitungsreglement nach Artikel 6 der Datenschutzverordnung vom 31. August 2022[31] (DSV) verfügt; und

b. beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten nach Artikel 12 Absatz 4 des Datenschutzgesetzes vom 25. September 2020[32] angemeldet wurde.[33]

4bis Die AHV-Nummer wird nur bereitgestellt, sofern ihre Verwendung der Zentralen Ausgleichsstelle nach Artikel 134ter der Verordnung vom 31. Oktober 1947[34] über die Alters- und Hinterlassenenversicherung gemeldet wird.[35]

5 Die für die Publikation des Eidgenössischen Staatskalenders nötigen Daten nach Artikel 5 der Organisationsverordnung vom 29. Oktober 2008[36] für die Bundeskanzlei werden regelmässig an die Bundeskanzlei übermittelt.

Art. 14 Aufbewahrungsfrist für Personendaten

1 Ist eine Person aus dem Geltungsbereich dieser Verordnung ausgeschieden, so werden ihre Daten in den IAM-Systemen und den Verzeichnisdiensten spätestens nach zwei Jahren vernichtet.

2 Vorbehalten bleiben die Bestimmungen über die Vernichtung von biometrischen Daten nach Artikel 20 Absatz 2 ISG.[37]

30 Fassung gemäss Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).
31 SR **235.11**
32 SR **235.1**
33 Fassung gemäss Anhang 2 Ziff. II 18 der Datenschutzverordnung vom 31. Aug. 2022, in Kraft seit 1. Sept. 2023 (AS **2022** 568).
34 SR **831.101**
35 Eingefügt durch Ziff. I der V vom 4. Mai 2022, in Kraft seit 1. Juni 2022 (AS **2022** 282).
36 SR **172.210.10**
37 Eingefügt durch Ziff. I der V vom 14. Nov. 2018 (AS **2018** 4739). Fassung gemäss Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).

5. Abschnitt: Datenbekanntgaben bei IAM-Systemen

Art. 15 Datenbekanntgabe beim Anschluss eines Informationssystems an ein IAM-System

1 Wird ein bisher autonomes Informationssystem an ein IAM-System angeschlossen und diesem die Prüfung der Identität und bestimmter berechtigungsrelevanter Eigenschaften von Personen übertragen, so dürfen die entsprechenden Personendaten ins IAM-System importiert werden.

2 Im IAM-System muss für jedes nachgelagerte Informationssystem eine Liste der Personendaten geführt werden, die es diesem aufgrund dieser Verordnung und der gesetzlichen Grundlagen des nachgelagerten Systems bekanntgeben darf.

Art. 16 Datenbekanntgabe beim einzelnen Zugang

Das IAM-System authentifiziert Personen, Maschinen oder Systeme, die den Zugang zu einem nachgelagerten Informationssystem verlangen, überprüft die notwendigen Identitätsdaten und die notwendigen weiteren Eigenschaften und Bestätigungen und leitet das Ergebnis der Prüfung mit den festgelegten Identitätsdaten, Eigenschaften und Bestätigungen an das nachgelagerte System weiter.

Art. 17 Bekanntgabe von Personendaten an einen externen Betreiber

1 Wird ein Informationssystem des Bundes von einem externen Betreiber im Auftrag des Bundes betrieben oder müssen Personen nach Artikel 8 Absatz 1 oder 3 Buchstabe a auf fremde Informationssysteme zugreifen, so dürfen die dazu notwendigen Personendaten aus Personalinformationssystemen, dem zentralen Identitätsspeicher oder IAM-Systemen automatisiert dem externen Betreiber bekanntgegeben werden.

2 Dazu erstellt die Stelle, die für das extern betriebene Informationssystem zuständig ist oder den Zugang auf das fremde Informationssystem benötigt, einen schriftlichen Antrag, der den betroffenen Personenkreis nennt, und stellt diesen via die zuständige Datenschutzberaterin oder den zuständigen Datenschutzberater dem für das liefernde Informationssystem zuständigen Bundesorgan zu.[38]

3 Der Antrag enthält die schriftliche Verpflichtung der zuständigen Stelle nach Absatz 2, die Datenschutzgesetzgebung des Bundes einzuhalten, die Daten ausschliesslich für den beabsichtigten Zweck zu verwenden und diese nach dem Stand der Technik zu schützen. Dem für das liefernde Informationssystem zuständigen Bundesorgan ist ein Inspektionsrecht einzuräumen.

4 Die betroffenen Personen müssen vorgängig informiert werden.

38 Fassung gemäss Anhang 2 Ziff. II 18 der Datenschutzverordnung vom 31. Aug. 2022, in Kraft seit 1. Sept. 2023 (AS **2022** 568).

6. Abschnitt: Massnahmen zum Schutz der IAM-Systeme und Verzeichnisdienste[39]

Art. 18 Anforderungen an die Informationssicherheit

[1] Interne und externe Betreiber von Komponenten eines IAM-Systems oder Verzeichnisdiensts müssen über schriftlich festgehaltene Vorgaben für die Handhabung der Informationssicherheit und der Risiken verfügen. Insbesondere erlässt jedes nach dieser Verordnung verantwortliche Organ eines Systems oder Verzeichnisdiensts ein Bearbeitungsreglement nach Artikel 6 DSV[40].[41]

[2] IAM-Systeme und Verzeichnisdienste, die nicht von Stellen nach Artikel 2 oder in deren Auftrag geführt werden, dürfen nur mit bundesinternen IAM-Systemen oder Verzeichnisdiensten verbunden werden, wenn sie die Minimalanforderungen bezüglich der Informationssicherheit erfüllen.[42]

[3] Für den Zugang zu bestimmten Informationssystemen können von der zuständigen Stelle oder vom Bereich DTI die Einhaltung höherer Anforderungen und bestimmte Zertifizierungen verlangt werden.

[4] Der Bereich DTI regelt in Weisungen die einzuhaltenden Sicherheitsanforderungen und Verfahren.

Art. 19 Datenbearbeitung beim Ausstellen von elektronischen Identifikationsmitteln

[1] Der Aussteller eines Identifikationsmittels darf für die Prüfung der Identität von der antragstellenden Person die Vorlage eines Passes, der Schweizer Identitätskarte oder eines für die Einreise in die Schweiz anerkannten Ausweisdokuments verlangen.

[2] Er kann von der Person ein Foto oder eine Unterschrift aufnehmen oder im System bereits hinterlegte Fotos oder Unterschriften zum Abgleich mit dem Ausweisdokument verwenden.

[3] Die zur Identifikation verwendeten Daten werden zusammen mit den Daten zum Identifikationsmittel gespeichert. Wenn es die Sicherheitsanforderungen für das betreffende Identifikationsmittel verlangen, kann auch ein Bild der für die Identifikation verwendeten Ausweisdokumente gespeichert werden.

7. Abschnitt: Verbund von IAM-Systemen

Art. 20[43] IAM-Gesamtsystem

Die IAM-Systeme des Bundes können untereinander und mit den externen IAM-Systemen nach Artikel 21 zu einem Gesamtsystem verbunden werden.

39 Fassung gemäss Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).
40 SR **235.11**
41 Fassung gemäss Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).
42 Fassung gemäss Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).
43 Fassung gemäss Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).

Art. 21 Anschluss externer IAM-Systeme: Voraussetzungen

Die nachstehenden externen IAM-Systeme können für den Zugang der in ihnen geführten Personen zu den Ressourcen des Bundes an die IAM-Systeme des Bundes angeschlossen werden, sofern sie die Bedingungen und Verfahren nach den Artikeln 22 und 23 einhalten und ihre Betreiber sich verpflichten, diese Verordnung und die gestützt darauf erlassenen Vorgaben einzuhalten oder im Falle der Kantone diese eine mindestens gleichwertige Informationssicherheit gewährleisten:[44]

a.[45] IAM-Systeme mit kantonalen und kommunalen Mitarbeiterinnen und Mitarbeitern nach Artikel 9 Buchstabe a sowie IAM-Systeme des Fürstentums Liechtenstein;

b. vom Bereich DTI anerkannte IAM-Systeme, die für den Identitätsverbund im E-Government vorgesehen sind;

c. ausländische IAM-Systeme oder Identitätsverbunde, deren gegenseitige Anbindung in einem Staatsvertrag vorgesehen ist; oder

d. Attribut-Register, die Angaben zu beruflichen Funktionen gemäss Anhang Buchstabe b für den Abruf bereitstellen.

Art. 22 Anschluss externer IAM-Systeme: Antrag

1 Die zuständige Stelle richtet den Antrag auf Anschluss eines externen IAM-Systems an ein IAM-System des Bundes an das nach Artikel 5 verantwortliche Bundesorgan.

2 Der Antrag enthält insbesondere:

a. den Zweck des Anschlusses;

b. die Rechtsgrundlagen und die weiteren Regelungen für das anzuschliessende System;

c. eine technische Beschreibung des anzuschliessenden Systems;

d. die Belege für die Einhaltung der Anforderungen an die Informationssicherheit nach Artikel 18 Absatz 2 oder 3;

e. eine zustimmende Stellungnahme des zuständigen Departements;

f. die unterstützende Stellungnahme mindestens einer Stelle, die für ein nachgelagertes System verantwortlich ist, auf das mittels des anzuschliessenden IAM-Systems zugegriffen werden soll.

Art. 23 Anschluss externer IAM-Systeme: Entscheid

1 Das für ein IAM-System des Bundes verantwortliche Bundesorgan ist für den Entscheid über den Antrag zuständig.

2 Soll das externe IAM-System über das direkt angeschlossene IAM-System hinaus auch mit anderen IAM-Systemen des Bundes verbunden sein, so ist für die Gutheissung des Antrags das Einverständnis des Bereichs DTI erforderlich.

44 Fassung gemäss Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).
45 Fassung gemäss Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).

3 Das verantwortliche Bundesorgan schliesst mit der antragstellenden Stelle die Vereinbarung ab, informiert der Bereich DTI und gibt dem zuständigen Leistungserbringer den Auftrag für den Anschluss.

4 Anträge auf Änderungen oder Abschaltungen werden wie Anschlussanträge behandelt.

Art. 24 Anschluss von IAM-Systemen des Bundes an externe IAM-Systeme

1 IAM-Systeme des Bundes können als Lieferant von Identitäts- und Authentifizierungsinformationen an ein externes IAM-System oder einen externen Identitätsverbund angeschlossen werden, wenn die folgenden Voraussetzungen erfüllt sind:

a.[46] Der Anschluss dient dazu, Personen nach Artikel 8 oder 9 den Zugang:

1. zu im Auftrag des Bundes von Externen betriebenen Informationssystemen oder zu fremden Informationssystemen zu gewähren, auf die sie zur Erfüllung ihrer gesetzlichen Aufgaben zugreifen müssen; oder
2. zu für den Vollzug von kantonalem Recht von Kantonen und Gemeinden sowie Organisationen und Personen des öffentlichen oder privaten Rechts bereitgestellten Informationssystemen, wie E-Government-Anwendungen, zu gewähren.

b. Es besteht eine Vereinbarung zwischen dem Bund und dem Betreiber des empfangenden Informationssystems, welche die Beziehung in rechtlicher, organisatorischer und technischer Hinsicht regelt.

c. Die Verbindung ist so konfiguriert, dass sie einzig für den Zugang zu bestimmten, vordefinierten Informationssystemen verwendet werden kann.

2 Der Bereich DTI regelt in Weisungen die einzuhaltenden Sicherheitsanforderungen in Absprache mit dem für das entsprechende IAM-System verantwortlichen Organ und überprüft die Einhaltung periodisch.

3 Ebenfalls möglich ist die Teilnahme an einem internationalen Identitätsverbund auf der Basis eines Staatsvertrags, sofern gewährleistet ist, dass die Anforderungen an die Informationssicherheit eingehalten werden.

8. Abschnitt: Protokollierung, Statistiken und Dokumentation

Art. 25 Protokollierung bei IAM-Systemen

1 Das IAM-System protokolliert Authentifizierungen und die Bekanntgabe von Identitätsdaten nur in dem Umfang und nur so lange, wie es für einen sicheren und geordneten Betrieb der eigenen und der nachgelagerten Systeme erforderlich ist.

46 Fassung gemäss Ziff. I der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).

2 Protokolldaten werden getrennt vom System, in welchem die Personendaten bearbeitet werden, aufbewahrt und spätestens nach zwei Jahren vernichtet. Es werden keine Protokolldaten archiviert.[47]

3 Vorbehalten bleibt eine umfangreichere Protokollierung, eine längere Aufbewahrung oder eine Archivierung der Protokolldaten für die Zugriffe auf ein bestimmtes Informationssystem auf der Basis einer besonderen rechtlichen Grundlage.

Art. 26 Weitergabe von Protokolldaten von IAM-Systemen

1 Die Betreiber von IAM-Systemen des Bundes dürfen Protokolldaten über Authentifizierungen und über die Bekanntgabe von Identitätsdaten der für das jeweilige nachgelagerte System zuständigen Stelle bekanntgeben.

2 Dazu ist ein schriftlicher Antrag mit Angabe des Zwecks und der rechtlichen Grundlage via die zuständige Datenschutzberaterin oder den zuständigen Datenschutzberater an das für das IAM-System verantwortliche Organ zu richten. Die Lieferung kann mit den gleichen Angaben auch in der Betriebsvereinbarung zwischen dem verantwortlichen Organ und dem Betreiber des IAM-Systems vereinbart werden.[48]

3 Die Lieferung kann nach den für den bundesinternen Bezug von Informatikdienstleistungen geltenden Grundsätzen kostenpflichtig sein.

Art. 27 Statistiken bei IAM-Systemen

Für die Bedürfnisse der für das IAM-System oder für das nachgelagerte Informationssystem zuständigen Stelle dürfen Zugangsstatistiken erstellt werden. Personendaten sind zu anonymisieren.

Art. 28 Inventar und Dokumentation

1 Jedes Organ, das für ein IAM-System, für einen Verzeichnisdienst oder für ein anderes Informationssystem nach dieser Verordnung verantwortlich ist, führt ein Inventar über:

a. seine IAM-Systeme und Verzeichnisdienste;

b. die Informationssysteme, aus denen automatisch Daten bezogen werden;

c. die Informationssysteme, denen Daten automatisch zur Verfügung gestellt werden;

d. alle IAM-Systeme, mit denen sein IAM-System verbunden ist.

2 Wichtige Dokumente und Belege, insbesondere die Anträge nach dieser Verordnung, müssen mindestens so lange aufbewahrt werden, wie sie gelten.

47 Fassung gemäss Anhang 2 Ziff. II 18 der Datenschutzverordnung vom 31. Aug. 2022, in Kraft seit 1. Sept. 2023 (AS **2022** 568).

48 Fassung gemäss Anhang 2 Ziff. II 18 der Datenschutzverordnung vom 31. Aug. 2022, in Kraft seit 1. Sept. 2023 (AS **2022** 568).

9. Abschnitt: Schlussbestimmungen

Art. 29 Vollzug

Der Bereich DTI erlässt die administrativen und technischen Weisungen zum Aufbau und zum Betrieb der IAM-Systeme des Bundes.

Art. 30 Aufhebung eines anderen Erlasses

Die Verordnung vom 6. Dezember 2013[49] über die vom BIT betriebenen Verzeichnisdienste des Bundes wird aufgehoben.

Art. 31 Inkrafttreten

Diese Verordnung tritt am 1. Januar 2017 in Kraft.

49 [AS **2013** 4553]

Anhang[50]
(Art. 11 sowie 13 Abs. 1 und 2)

Datenkategorien

Vorbemerkung: Zur Bedeutung der Sterne (*) siehe Artikel 11 Absatz 4.

	Verzeichnisdienste	IAM-Systeme mit Personen nach Art. 8 und 9 Bst. a	IAM-Systeme mit Personen nach Art. 9 Bst. b
a. Angaben zur Person			
1. Name*	x	x	x
2. Vornamen*	x	x	x
3. Geburtsdatum		x	x
4. Geburtsort			x
5. Nationalität			x
6. Geschlecht		x	x
7. Anrede*	x	x	x
8. Titel*	x	x	x
9. Initialen*	x	x	x
10. lokale Personenidentifikatoren	x	x	x
11. Berufsbezeichnung*	x	x	x
12. Korrespondenzsprache*	x	x	x
13. besondere biometrische Personenmerkmale, insbesondere Irisbild, Retina, Venenscan, Fingerabdruck, Handabdruck, Gesichtsformmerkmale und Stimmprofil		x	
14. Gesichtsbild	x	x	x
15. AHV-Nummer	x	x	x
b. Angaben zum Verhältnis zum Arbeit-/Auftraggeber			
1. Anstellungsverhältnis (intern/extern)*	x	x	
2. Informationen zur Organisation und zu den Planstellen*	x	x	x
3. künftige Zuordnung zu einer Organisationseinheit	x	x	
4. Personalkategorie		x	

[50] Fassung gemäss Ziff. II der V vom 8. Nov. 2023, in Kraft seit 1. Jan. 2024 (AS **2023** 738).

	Verzeichnisdienste	IAM-Systeme mit Personen nach Art. 8 und 9 Bst. a	IAM-Systeme mit Personen nach Art. 9 Bst. b
5. Personalnummer (auch kantonale)	x	x	
6. Funktion*	x	x	
7. Stellenbezeichnung*	x	x	
8. Kennung des Personalinformationssystems (Quelle)	x	x	
9. Eintritts- und Austrittsdatum	x	x	
10. Ausweis- und/oder Badgenummer	x	x	x
c. Kontaktangaben			
1. Arbeitsort und geschäftliche Postadresse*	x	x	x
2. private Postadresse			x
3. Büronummer*	x	x	
4. geschäftliche Adressierungselemente* wie E-Mail-Adresse*, Telefonnummern*, Faxnummer*, VOIP-Adresse*	x	x	x
5. externe Adressierungselemente* (für Mitarbeiter/innen und Beauftragte*) oder private Adressierungselemente	x	x	x
d. Angaben zu beruflichen Funktionen			
1. Einträge aus offiziellen Berufsregistern (Arzt/Ärztin, Urkundsperson, Anwalt/Anwältin usw.)		x	x
2. Funktionen gemäss Handelsregister und weiteren Vertretungsregistern		x	x
e. technische Angaben			
1. zugeordnete Geräte, Anschlüsse, Systeme, Anwendungen usw.	x	x	x
2. Adressierungselemente, Kennnummern usw.	x		
3. Systemsprache der Geräte, Anschlüsse usw.	x	x	x
4. öffentliche Schlüssel der digitalen Zertifikate*	x	x	x
5. Berechtigungsgruppen	x	x	x
6. Namen für die Anmeldung an den IT-Systemen	x	x	x
7. Passwörter (kryptographisch gesichert)		x	x
8. letztes Login		x	x
9. fehlgeschlagene Login-Versuche		x	x
10. Status (aktiv/passiv)		x	x

	Verzeichnisdienste	IAM-Systeme mit Personen nach Art. 8 und 9 Bst. a	IAM-Systeme mit Personen nach Art. 9 Bst. b
11. Authentisierungsqualität		x	x
f. Daten über die Personensicherheitsprüfung, sofern diese zu einer vorbehaltlosen Sicherheitserklärung geführt hat oder die entscheidende Instanz einen positiven Entscheid gefällt hat.			
1. Prüfstufe		x	
2. Geltungsdauer der Sicherheitserklärung		x	