



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

Änderung vom ... Entwurf vom 24. August 2022

*Der Schweizerische Bundesrat
verordnet:*

I

Die Verordnung vom 19. Oktober 2016¹ über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes wird wie folgt geändert:

Ingress

gestützt auf Artikel 26 und 84 Absatz 1 des Informationssicherheitsgesetzes vom 18. Dezember 2020² (ISG),
auf Artikel 27 Absätze 5 und 6 des Bundespersonalgesetzes vom 24. März 2000³
und auf Artikel 186 des Bundesgesetzes vom 3. Oktober 2008⁴ über die militärischen Informationssysteme,

Art. 2 Geltungsbereich

Diese Verordnung gilt für:

- a. die Verwaltungseinheiten der zentralen Bundesverwaltung nach Artikel 7 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998⁵ (RVOV);
- b. die Verwaltungseinheiten der dezentralen Bundesverwaltung nach Artikel 7a RVOV, sofern sie Zugriff auf Informatiksysteme der zentralen Bundesverwaltung haben.

1 SR 172.010.59
2 SR 126
3 SR 172.220.1
4 SR 510.91
5 SR 172.010.1

Art. 3 Abs. 1

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 zur Verfügung zu stellen.

Art. 5 IAM-Systeme

¹ Die für IAM-Systeme verantwortlichen Bundesorgane sind:

- a. der Bereich digitale Transformation und IKT-Lenkung der Bundeskanzlei (Bereich DTI der BK) für alle als Standarddienste angebotenen oder dem Bereich DTI der BK ausdrücklich zugewiesenen IAM-Systeme;
- b. die Direktion für Ressourcen im Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) für das von der Informatik EDA betriebene IAM-System;
- c. der Bereich DTI der BK für das IAM-System der Supportprozesse einschliesslich der Cloudanbindungen;
- d. das Generalsekretariat des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport für das von der Führungsunterstützungsbasis (FUB) des VBS betriebene IAM-System;
- 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 Die Bundesorgane nach Absatz 1 sorgen dafür, dass die rechtmässige Bearbeitung der Personendaten in den IAM-Systemen, für die sie verantwortlich sind, mindestens alle vier Jahre von einer externen Stelle überprüft wird.

³ Sofern diese Verordnung auf die verpflichteten Behörden nach Artikel 2 Absatz 1 Buchstaben a und c–e ISG gemäss Artikel 84 Absatz 3 ISG anwendbar ist, legen diese selber fest, welches die in ihrem Bereich verantwortlichen Bundesorgane sind.

⁴ Die Verantwortung für das nachgelagerte System, insbesondere für den Zugang dazu, bleibt bei der zuständigen Fachstelle.

Art. 11 Abs. 2 und 3

² Es darf in diesen Systemen kein Profiling durchgeführt werden.

³ Es dürfen in diesen Systemen, sofern hierfür keine besondere rechtliche Grundlage besteht, keine besonders schützenswerten Personendaten mit Ausnahme von biometrischen Daten nach Artikel 20 Absatz 2 ISG bearbeitet werden.

Art. 13 Abs. 4

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

- a. über eine Rechtsgrundlage, welche die Bearbeitung der bereitzustellenden Daten vorsieht, und ein Bearbeitungsreglement nach Artikel 21 der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG) verfügt; und

Art. 14 Abs. 2

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

Gliederungstitel vor Art. 18

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

Art. 18 Abs. 1 und 2

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 verantwortliche Organ eines Systems oder Verzeichnisdiensts nach dieser Verordnung ein Bearbeitungsreglement nach Artikel 21 VDSG.

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 vordefinierten Minimalanforderungen bezüglich der Informationssicherheit erfüllen.

Art. 20 IAM-Gesamtsystem

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

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:

- a. IAM-Systeme der Parlamentsdienste;
- b. IAM-Systeme der Armee;
- c. IAM-Systeme mit kantonalen und kommunalen Mitarbeiterinnen und Mitarbeitern nach Artikel 9 Buchstabe a;
- d. vom Bereich DTI der BK anerkannte IAM-Systeme, die für den Identitätsverbund im E-Government vorgesehen sind;

- e. ausländische IAM-Systeme oder Identitätsverbunde, deren gegenseitige Anbindung in einem Staatsvertrag vorgesehen ist; oder
- f. Attribut-Register, die Angaben zu beruflichen Funktionen gemäss Anhang Buchstabe b für den Abruf bereitstellen.

II

Der Anhang erhält die neue Fassung gemäss Beilage.

III

Diese Verordnung tritt am ... 2023 Kraft.

...

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: ...

Der Bundeskanzler: Walter Thurnherr

Anhang
(Art. 11 und 13 Abs. 1 und 2)

Datenkategorien

Vorbemerkung: Zur Bedeutung der Sterne () siehe Artikel 11 Absatz 2.*

	Verzeichnisdienste so- wie 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
2. Vornamen*	X	X
3. Geburtsdatum	X	X
4. Geschlecht	X	X
5. Anrede*	X	X
6. Titel*	X	X
7. Initialen*	X	X
8. lokale Personenidentifikatoren	X	X
9. Berufsbezeichnung*	X	X
10. Korrespondenzsprache*	X	X
11. besondere biometrische Personenmerkmale, insbesondere Irisbild, Retina, Venenscan, Fingerabdruck, Handabdruck, Gesichtsformmerkmale und Stimmprofil	X	
12. AHV-Nummer	X	X
b. Angaben zum Verhältnis zum Arbeit-/Auftraggeber		
1. Anstellungsverhältnis (intern/extern)*	X	
2. Informationen zur Organisation und zu den Planstellen*	X	X
3. künftige Zuordnung zu einer Organisationseinheit	X	
4. Personalkategorie	X	
5. Personalnummer (auch kantonale)	X	
6. Funktion*	X	
7. Stellenbezeichnung*	X	
8. Kennung des Personalinformationssystems (Quelle)	X	
9. Eintritts- und Austrittsdatum	X	
10. Ausweis- und/oder Badgenummer	X	X
c. Kontaktangaben		

	Verzeichnisdienste so- wie IAM-Systeme mit Personen nach Art. 8 und 9 Bst. a	IAM-Systeme mit Personen nach Art. 9 Bst. b
1. Arbeitsort und geschäftliche Postadresse*	X	X
2. Büronummer*	X	
3. geschäftliche Adressierungselemente* wie E-Mail-Adresse*, Telefonnummern*, Faxnummer*, VOIP-Adresse*	X	X
4. externe Adressierungselemente* (für Mitarbeiter/innen und Beauftragte*) oder private Adressierungselemente	X	X
d. Angaben zu beruflichen Funktionen		
1. Einträge aus offiziellen Berufsregistern (Arzt/Ärztin, Ur- kundsperson, Anwalt/Anwältin usw.)	X	X
2. Funktionen gemäss Handelsregister und weiteren Vertre- tungsregistern	X	X
e. technische Angaben		
1. zugeordnete Geräte, Anschlüsse, Systeme, Anwendungen usw.	X	X
2. Adressierungselemente, Kennnummern usw.	X	
3. Systemsprache der Geräte, Anschlüsse usw.	X	X
4. öffentliche Schlüssel der digitalen Zertifikate*	X	X
5. Berechtigungsgruppen	X	X
6. Namen für die Anmeldung an den IT-Systemen	X	X
7. Passwörter	X	X
8. letztes Login	X	X
9. fehlgeschlagene Login-Versuche	X	X
10. Status (aktiv/passiv)	X	X
f. Daten über die Personensicherheitsprüfung, sofern diese zu einer vorbehaltlosen Sicherheitserklärung geführt hat oder die ent- scheidende Instanz einen positiven Entscheid gefällt hat		
1. Prüfstufe	X	
2. Geltungsdauer der Sicherheitserklärung	X	