

Ordinanza sui sistemi di gestione delle identità e sui servizi di elenchi della Confederazione (OIAM)

del 19 ottobre 2016 (Stato 1° gennaio 2024)

Il Consiglio federale svizzero,

visti gli articoli 26 e 84 capoverso 1 della legge del 18 dicembre 2020¹ sulla sicurezza delle informazioni (LSIn);
vista la legge federale del 17 marzo 2023² concernente l'impiego di mezzi elettronici per l'adempimento dei compiti delle autorità (LMeCA);
vista la legge del 21 marzo 1997³ sull'organizzazione del Governo e dell'Amministrazione (LOGA);
visto l'articolo 27 capoversi 5 e 6 della legge del 24 marzo 2000⁴ sul personale federale;
visto l'articolo 186 della legge federale del 3 ottobre 2008⁵ sui sistemi d'informazione militari e su altri sistemi d'informazione nel DDPS,⁶
ordina:

Sezione 1: Disposizioni generali

Art. 1 Oggetto

La presente ordinanza disciplina le competenze, il trattamento e la comunicazione di dati personali e i requisiti in materia di sicurezza delle informazioni per i sistemi di gestione delle identità (sistemi IAM⁷), i servizi di elenchi e l'archivio centralizzato delle identità della Confederazione.

RU 2016 3623

¹ RS 128

² RS 172.019

³ RS 172.010

⁴ RS 172.220.1

⁵ RS 510.91

⁶ Nuovo testo giusta il n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU 2023 738).

⁷ IAM = *Identity and Access Management*

Art. 2⁸ Campo d'applicazione

¹ Gli articoli 24 e 25 LSIn e la presente ordinanza si applicano:

- a. alle unità amministrative dell'Amministrazione federale centrale secondo l'articolo 7 dell'ordinanza del 25 novembre 1998⁹ sull'organizzazione del Governo e dell'Amministrazione (OLOGA);
- b. all'esercito.

² L'applicabilità della presente ordinanza alle unità amministrative dell'Amministrazione federale decentralizzata secondo l'articolo 2 capoverso 3 LOGA e alle organizzazioni secondo l'articolo 2 capoverso 4 LOGA si fonda sull'articolo 2 capoverso 2 lettera b e 3 dell'ordinanza dell'8 novembre 2023¹⁰ sulla sicurezza delle informazioni (OSIn).

Sezione 2: Scopo e funzione principale dei sistemi**Art. 3** Sistemi IAM

¹ Lo scopo di un sistema IAM consiste nell'amministrare in modo raggruppato i dati sull'identità e sui diritti di persone, macchine e sistemi per metterli a disposizione, su richiesta, di sistemi a valle e di altri sistemi IAM.

² I sistemi a valle sono applicazioni specifiche oppure sistemi che consentono di accedere a informazioni, strumenti informatici, locali e altre infrastrutture.

³ In quanto sistema a monte, il sistema IAM verifica l'identità e determinate caratteristiche, rilevanti ai fini dei diritti, di persone, macchine e sistemi che vogliono accedere a un sistema a valle e ne trasmette il risultato al sistema d'informazione a valle affinché possa accertare tali diritti.

Art. 4 Servizi di elenchi

Lo scopo di un servizio di elenchi consiste nel gestire informazioni sugli utenti delle infrastrutture della Confederazione al fine di identificare le persone e amministrare i dispositivi, le connessioni, i dati relativi ai contatti e simili a loro assegnati.

⁸ Nuovo testo giusta il n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU 2023 738).

⁹ RS 172.010.1

¹⁰ RS 128.1

Sezione 3: Organi responsabili

Art. 5¹¹ Sistemi IAM

¹ I seguenti organi federali sono responsabili dei sottostanti sistemi IAM dell'Amministrazione federale centrale:

- a. il settore Trasformazione digitale e governance delle TIC della Cancelleria federale (settore TDT della CaF) per:
 1. tutti i sistemi IAM offerti come servizi standard o esplicitamente attribuiti al settore TDT della CaF inclusa la relativa messa a disposizione dei Cantoni e dei Comuni nonché delle organizzazioni e delle persone di diritto pubblico o privato conformemente all'articolo 11 capoverso 3 LMeCA,
 2. tutti i sistemi IAM dei processi di supporto legati a finanze, acquisti, immobili e logistica, compresi i collegamenti cloud;
- b. la Direzione delle risorse del Dipartimento federale degli affari esteri (DFAE) per il sistema IAM gestito dall'unità Informatica DFAE;
- c. la Segreteria generale del Dipartimento federale della difesa, della protezione della popolazione e dello sport per i sistemi IAM gestiti dall'Aggruppamento Difesa (Aggruppamento D);
- d. l'Amministrazione federale delle finanze per il sistema IAM gestito in seno all'Ufficio centrale di compensazione per il trattamento dei sistemi di assicurazioni sociali del 1° pilastro e il relativo supporto ai processi;
- e. la Segreteria generale del Dipartimento federale dell'economia, della formazione e della ricerca (DEFR) per il sistema IAM gestito presso il Centro servizi informatici DEFR (CSIeco);
- f. l'Ufficio federale delle strade per il suo sistema IAM destinato all'esercizio degli equipaggiamenti di esercizio e sicurezza delle strade nazionali.

² Provvedono affinché la liceità del trattamento dei dati personali nei sistemi IAM dei quali sono responsabili sia verificata almeno ogni quattro anni da un servizio esterno.

³ I seguenti organi federali sono responsabili dei sottostanti sistemi IAM:

- a. l'Aggruppamento D per i sistemi IAM dell'esercito;
- b. le rispettive unità amministrative per i sistemi IAM dell'Amministrazione federale decentralizzata;
- c. le rispettive organizzazioni per i sistemi IAM delle organizzazioni secondo l'articolo 2 capoverso 4 LOGA.

⁴ Le autorità assoggettate secondo l'articolo 2 capoverso 1 lettere a e c–e LSIn, alle quali la presente ordinanza si applica secondo l'articolo 84 capoverso 3 LSIn, stabiliscono quali sono gli organi federali responsabili nel loro settore.

¹¹ Nuovo testo giusta il n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU 2023 738).

⁵ La responsabilità del sistema a valle, in particolare dell'accesso ad esso, rimane al servizio tecnico cui spetta la relativa competenza.

Art. 6 Servizi di elenchi

Gli organi federali responsabili dei servizi di elenchi esterni ai sistemi IAM sono:

- a. il settore TDT della CaF¹² per i servizi standard;
- b. per gli altri elenchi, i fornitori di prestazioni informatiche che gestiscono tali sistemi, più precisamente:
 1. l'unità Informatica DFAE della Direzione delle risorse del DFAE,
 2. il Centro servizi informatici del Dipartimento federale di giustizia e
 - 3.¹³ l'Aggruppamento D,
 4. l'Ufficio federale dell'informatica e della telecomunicazione (UFIT),
 5. il CSIeco.

Art. 7 Esercizio dei diritti

Le persone interessate fanno valere i propri diritti relativi ai sistemi IAM e ai servizi di elenchi presso i seguenti servizi:

- a. diritto di lettura: presso gli organi responsabili;
- b.¹⁴ diritto di correzione e cancellazione dei dati:
 1. presso il servizio del personale della loro unità amministrativa od organizzazione oppure presso il servizio competente per l'aggiornamento dei loro dati,
 2. nel caso di cui all'articolo 9 lettera b: presso gli organi responsabili.

Sezione 4: Dati trattati, ottenimento dei dati e termine di conservazione

Art. 8 Persone registrate in sistemi IAM e in servizi di elenchi

¹ Nei sistemi IAM e nei servizi di elenchi possono essere trattati dati relativi alle seguenti persone:

- a. collaboratori dell'Amministrazione federale centrale secondo l'articolo 7 OLOGA¹⁵;

¹² Nuova espressione giusta l'all. n. 8 dell'O del 25 nov. 2020 sulla trasformazione digitale e l'informatica, in vigore dal 1° gen. 2021 (RU **2020** 5871). Di detta mod. è tenuto conto in tutto il presente testo.

¹³ Nuovo testo giusta il n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU **2023** 738).

¹⁴ Nuovo testo giusta il n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU **2023** 738).

¹⁵ RS **172.010.1**

- b. collaboratori dell'Amministrazione federale decentralizzata secondo l'articolo 7a OLOGA;
- c. membri dell'Assemblea federale e collaboratori dei Servizi del Parlamento secondo il titolo quarto, capitolo 7 della legge del 13 dicembre 2002¹⁶ sul Parlamento;
- d. persone elette dall'Assemblea federale secondo l'articolo 168 della Costituzione federale¹⁷;
- e. collaboratori del Tribunale federale, del Tribunale amministrativo federale, del Tribunale penale federale e del Tribunale federale dei brevetti, sempre che la legislazione non preveda diversamente;
- f. collaboratori del Ministero pubblico della Confederazione secondo gli articoli 7–22 della legge del 19 marzo 2010¹⁸ sull'organizzazione delle autorità penali (LOAP);
- g. collaboratori della segreteria dell'autorità di vigilanza sul Ministero pubblico della Confederazione secondo l'articolo 27 capoverso 2 LOAP;
- h.¹⁹ militari e militi della protezione civile.

² Inoltre possono essere trattati dati di collaboratori delle seguenti imprese a condizione che essi siano regolarmente in contatto con i servizi di cui al capoverso 1:

- a. Ferrovie federali svizzere;
- b. La Posta Svizzera;
- c. RUAG;
- d. Istituto nazionale svizzero di assicurazione contro gli infortuni.

³ Nei sistemi IAM e nei servizi di elenchi possono essere inoltre trattati dati sulle seguenti persone:

- a. persone esterne che svolgono attività per i servizi di cui ai capoversi 1 o 2;
- b. persone esterne che per altri motivi hanno accesso a informazioni, strumenti informatici, locali e altre infrastrutture dell'Amministrazione federale.

Art. 9 Persone registrate nei sistemi IAM

Oltre ai dati di cui all'articolo 8, nei sistemi IAM possono essere trattati dati delle persone seguenti:

- a. collaboratori di autorità cantonali o comunali se queste persone utilizzano sistemi informatici messi a disposizione dalla Confederazione;

¹⁶ RS 171.10

¹⁷ RS 101

¹⁸ RS 173.71

¹⁹ Introdotta dal n. I dell'O del 14 nov. 2018, in vigore dal 1° gen. 2019 (RU 2018 4739).

b.²⁰ privati e rappresentanti di organizzazioni che accedono a sistemi informatici, come le applicazioni per il Governo elettronico, messi a disposizione dalla Confederazione o, per l'esecuzione del diritto cantonale, dai Cantoni e dai Comuni nonché dalle organizzazioni e dalle persone di diritto pubblico o privato.

Art. 10 Persone registrate nei servizi di elenchi

Oltre ai dati di cui all'articolo 8, nei servizi di elenchi possono essere trattati dati di collaboratori di autorità cantonali o comunali nonché di altre imprese vicine alla Confederazione diverse da quelle menzionate nell'articolo 8 capoverso 2, che utilizzano un certificato digitale della Confederazione.

Art. 11 Categorie di dati personali

¹ Nei sistemi IAM, nei servizi di elenchi e nell'archivio centralizzato delle identità di cui all'articolo 13 possono essere trattati dati personali conformemente all'allegato.

² In questi sistemi non può essere effettuata alcuna profilazione secondo l'articolo 5 lettere f e g della legge federale del 25 settembre 2020²¹ sulla protezione dei dati.²²

³ In assenza di una base legale specifica in materia, in questi sistemi non possono essere trattati dati personali degni di particolare protezione. È fatto salvo il trattamento di dati biometrici con sistemi IAM per l'identificazione delle persone in funzione dei rischi secondo gli articoli 8 e 9 lettera a (art. 20 cpv. 2 LSIn).²³

⁴ I dati riguardanti persone secondo l'articolo 8 che nell'allegato sono contrassegnati con un asterisco possono essere pubblicati in un elenco di persone accessibile a tutti coloro che vi sono riportati.

Art. 12 Ottenimento di dati personali

¹ I sistemi IAM e i servizi di elenchi possono ottenere automaticamente dati delle persone registrate nel sistema d'informazione per la gestione dei dati del personale (SIGDP) conformemente all'articolo 34 dell'ordinanza del 22 novembre 2017²⁴ sulla protezione dei dati personali del personale federale.²⁵

² Possono ottenere automaticamente dai rispettivi servizi di cui all'articolo 8 dati di persone non registrate in SIGDP²⁶, a condizione che il gruppo di persone interessato

²⁰ Nuovo testo giusta il n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU **2023** 738).

²¹ RS **235.1**

²² Nuovo testo giusta il n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU **2023** 738).

²³ Nuovo testo giusta il n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU **2023** 738).

²⁴ RS **172.220.111.4**

²⁵ Nuovo testo giusta l'all. 8 n. II 1 dell'O del 22 nov. 2017 sulla protezione dei dati personali del personale federale, in vigore dal 1° gen. 2018 (RU **2017** 7271).

²⁶ Nuova espr. giusta l'all. 8 n. II 1 dell'O del 22 nov. 2017 sulla protezione dei dati personali del personale federale, in vigore dal 1° gen. 2018 (RU **2017** 7271). Di detta mod. è tenuto conto in tutto il presente testo.

necessità di principio l'accesso a sistemi d'informazione o ad altre risorse della Confederazione.

³ Possono ottenere automaticamente dai singoli sistemi d'informazione dati di persone esterne che accedono regolarmente alle risorse della Confederazione.

⁴ Possono ottenere automaticamente dati di persone esterne dai sistemi IAM esterni collegati ai sistemi IAM della Confederazione secondo gli articoli 21–24.²⁷

Art. 13 Archivio centralizzato delle identità per la distribuzione di dati

¹ L'UFIT gestisce un archivio centralizzato delle identità per distribuire dati degli utenti ai diversi sistemi IAM e ai servizi di elenchi. In questo archivio possono essere trattati tutti i dati personali conformemente all'allegato. L'organo federale responsabile è il settore TDT della CaF.

² La SIGDP trasmette regolarmente, se disponibili, i dati conformemente all'allegato all'archivio centralizzato delle identità. Tutti i dati personali ottenuti automaticamente dalla SIGDP sono distribuiti mediante questo archivio. Fanno eccezione i dati personali di base nel sistema SAP standard ottenuti direttamente per i sistemi SAP autorizzati.

³ I dati personali secondo l'articolo 8 capoverso 1 lettera c e capoverso 3 sono messi a disposizione dei Servizi del Parlamento affinché possano essere ripresi e armonizzati.

⁴ I dati possono essere messi a disposizione automaticamente di altri sistemi d'informazione interni alla Confederazione per essere ripresi e armonizzati a condizione che il sistema interessato:

- a.²⁸ sia dotato di una base legale che prevede il trattamento dei dati da mettere a disposizione e di un regolamento per il trattamento secondo l'articolo 6 dell'ordinanza del 31 agosto 2022²⁹ sulla protezione dei dati (OPDa); e
- b. sia notificato all'Incaricato federale della protezione dei dati e della trasparenza secondo l'articolo 12 capoverso 4 della legge federale del 25 settembre 2020³⁰ sulla protezione dei dati (LPD).³¹

^{4bis} Il numero AVS è messo a disposizione a condizione che la sua utilizzazione sia annunciata all'Ufficio centrale di compensazione secondo l'articolo 134^{ter} dell'ordinanza del 31 ottobre 1947³² sull'assicurazione per la vecchiaia e per i superstiti.³³

²⁷ Introdotto dal n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU **2023** 738).

²⁸ Nuovo testo giusta il n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU **2023** 738).

²⁹ RS **235.11**

³⁰ RS **235.1**

³¹ Nuovo testo giusta l'all. 2 n. II 18 dell'O del 31 ago. 2022 sulla protezione dei dati, in vigore dal 1° set. 2023 (RU **2022** 568).

³² RS **831.101**

³³ Introdotto dal n. I dell'O del 4 mag. 2022, in vigore dal 1° giu. 2022 (RU **2022** 282).

⁵ I dati necessari per la pubblicazione nell'Annuario federale secondo l'articolo 5 dell'ordinanza del 29 ottobre 2008³⁴ sull'organizzazione della Cancelleria federale sono trasmessi regolarmente alla Cancelleria federale.

Art. 14 Termine di conservazione di dati personali

¹ Se una persona non rientra più nel campo d'applicazione della presente ordinanza, i suoi dati nei sistemi IAM e nei servizi di elenchi sono distrutti al più tardi dopo due anni.

² Sono fatte salve le disposizioni sulla distruzione dei dati biometrici secondo l'articolo 20 capoverso 2 LSIn.³⁵

Sezione 5: Comunicazione di dati in relazione ai sistemi IAM

Art. 15 Comunicazione di dati in caso di collegamento di un sistema d'informazione a un sistema IAM

¹ Se un sistema d'informazione in precedenza autonomo viene connesso a un sistema IAM e se a quest'ultimo viene affidata la verifica delle identità e di determinate proprietà personali rilevanti ai fini dei diritti, i relativi dati personali possono essere importati nel sistema IAM.

² Nel sistema IAM, per ogni sistema d'informazione a valle deve essere tenuto un elenco dei dati personali che possono essere comunicati al sistema d'informazione a valle in base alla presente ordinanza e alle basi legali del sistema a valle.

Art. 16 Comunicazione di dati in caso di un singolo accesso

Il sistema IAM autentica persone, macchine o sistemi che richiedono l'accesso a un sistema d'informazione a valle, verifica i dati necessari concernenti l'identità e le altre proprietà e attestazioni necessarie e trasmette al sistema a valle il risultato di tale verifica con i dati concernenti l'identità, le proprietà e le attestazioni rilevanti.

Art. 17 Comunicazione di dati personali a un gestore esterno

¹ Se un sistema d'informazione della Confederazione è gestito su mandato di quest'ultima da un gestore esterno oppure se persone di cui all'articolo 8 capoversi 1 o 3 lettera a devono accedere a sistemi d'informazione esterni, i dati personali necessari a tale fine possono essere comunicati in modo automatizzato al gestore esterno a partire da sistemi d'informazione concernenti il personale, dall'archivio centralizzato delle identità o da sistemi IAM.

² A tal fine il servizio competente del sistema d'informazione gestito esternamente o che necessita l'accesso al sistema d'informazione esterno formula una richiesta scritta,

³⁴ RS 172.210.10

³⁵ Introdotto dal n. I dell'O del 14 nov. 2018 (RU 2018 4739). Nuovo testo giusta il n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU 2023 738).

specificando le persone interessate, e la invia tramite il consulente per la protezione dei dati competente all'organo federale responsabile del sistema d'informazione che fornisce i dati richiesti.³⁶

³ Nella richiesta il servizio responsabile secondo il capoverso 2 si impegna per scritto a rispettare la legislazione federale sulla protezione dei dati, a utilizzare i dati esclusivamente per lo scopo previsto e a proteggerli conformemente allo stato della tecnica. All'organo federale responsabile del sistema d'informazione che fornisce i dati richiesti deve essere accordato un diritto di ispezione.

⁴ Le persone interessate devono essere previamente informate.

Sezione 6: Misure di protezione dei sistemi IAM e dei servizi di elenchi³⁷

Art. 18 Requisiti in materia di sicurezza delle informazioni

¹ I gestori interni ed esterni di componenti di un sistema IAM e di un servizio di elenchi devono disporre di direttive scritte sulla sicurezza delle informazioni e sulla gestione dei rischi. In particolare, ogni organo responsabile secondo la presente ordinanza di un sistema o di un servizio di elenchi emana un regolamento per il trattamento secondo l'articolo 6 OPDa^{38,39}

² I sistemi IAM e i servizi di elenchi che non sono gestiti da servizi secondo l'articolo 2 o su loro mandato, possono essere collegati a sistemi IAM o servizi di elenchi interni alla Confederazione soltanto se soddisfano i requisiti minimi in materia di sicurezza delle informazioni.⁴⁰

³ Per accedere a determinati sistemi d'informazione il servizio competente o il settore TDT della CaF possono esigere il rispetto di requisiti più severi e la presenza di determinate certificazioni.

⁴ Il settore TDT della CaF disciplina in istruzioni i requisiti in materia di sicurezza e le procedure da rispettare.

Art. 19 Trattamento dei dati nell'emissione di strumenti di identificazione elettronici

¹ Per verificare l'identità del richiedente, l'emittente di uno strumento di identificazione può esigere l'esibizione del passaporto, della carta d'identità svizzera o di un documento d'identità riconosciuto per l'ingresso in Svizzera.

³⁶ Nuovo testo giusta l'all. 2 n. II 18 dell'O del 31 ago. 2022 sulla protezione dei dati, in vigore dal 1° set. 2023 (RU 2022 568).

³⁷ Nuovo testo giusta il n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU 2023 738).

³⁸ RS 235.11

³⁹ Nuovo testo giusta il n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU 2023 738).

⁴⁰ Nuovo testo giusta il n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU 2023 738).

² Può registrare una foto o una firma del richiedente oppure può utilizzare foto o firme già memorizzate nel sistema per confrontarle con il documento d'identità.

³ I dati utilizzati per l'identificazione sono salvati insieme a quelli relativi allo strumento di identificazione. Se i requisiti in materia di sicurezza concernenti lo strumento di identificazione interessato lo esigono, può essere salvata anche una copia dei documenti d'identità utilizzati per l'identificazione.

Sezione 7: Rete di sistemi IAM

Art. 20⁴¹ Sistema globale IAM

I sistemi IAM della Confederazione possono essere collegati tra loro e con i sistemi IAM esterni di cui all'articolo 21 al fine di costituire un sistema globale.

Art. 21 Condizioni per il collegamento di sistemi IAM esterni

I seguenti sistemi esterni IAM possono essere collegati ai sistemi IAM della Confederazione per consentire l'accesso delle persone ivi registrate alle risorse della Confederazione, sempre che siano soddisfatte le condizioni e le procedure secondo gli articoli 22 e 23 e i loro gestori s'impegnino a rispettare la presente ordinanza e le direttive emanate in virtù della stessa oppure, nel caso dei Cantoni, tali sistemi garantiscano una sicurezza delle informazioni almeno equivalente:⁴²

- a.⁴³ sistemi IAM comprendenti collaboratori cantonali e comunali secondo l'articolo 9 lettera a e i sistemi IAM del Principato del Liechtenstein;
- b. sistemi IAM riconosciuti dal settore TDT della CaF previsti per la rete per le identificazioni nell'ambito del Governo elettronico;
- c. sistemi IAM esteri o reti estere per le identificazioni il cui collegamento è previsto in un trattato internazionale; oppure
- d. registri degli attributi che mettono a disposizione per l'utilizzo dati relativi alle funzioni professionali conformemente alla lettera b dell'allegato.

Art. 22 Richiesta di collegamento di sistemi IAM esterni

¹ Il servizio competente invia la richiesta di collegamento di un sistema IAM esterno a un sistema IAM della Confederazione all'organo federale responsabile secondo l'articolo 5.

² La richiesta contiene in particolare:

- a. lo scopo del collegamento;

⁴¹ Nuovo testo giusta il n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU 2023 738).

⁴² Nuovo testo giusta il n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU 2023 738).

⁴³ Nuovo testo giusta il n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU 2023 738).

- b. le basi legali e le altre regolamentazioni relative al sistema da collegare;
- c. una descrizione tecnica del sistema da collegare;
- d. i documenti che comprovano il rispetto dei requisiti in materia di sicurezza dell'informazione secondo l'articolo 18 capoverso 2 o 3;
- e. un parere favorevole del dipartimento competente;
- f. il parere a sostegno espresso da almeno un servizio responsabile di un sistema a valle al quale si intende accedere attraverso il sistema IAM da collegare.

Art. 23 Decisione in merito al collegamento di sistemi IAM esterni

¹ La decisione in merito alla richiesta di collegamento spetta all'organo federale responsabile del sistema IAM della Confederazione interessato.

² Se il sistema IAM esterno deve essere collegato, oltre al sistema IAM direttamente collegato, anche ad altri sistemi IAM della Confederazione, per l'approvazione della richiesta è necessario il consenso del settore TDT della CaF.

³ L'organo federale responsabile stipula l'accordo con il servizio richiedente, ne informa il settore TDT della CaF e conferisce il mandato per il collegamento al fornitore di prestazioni competente.

⁴ Le richieste di modifiche o disattivazioni sono trattate analogamente alle richieste di collegamento.

Art. 24 Collegamento di sistemi IAM della Confederazione a sistemi IAM esterni

¹ I sistemi IAM della Confederazione possono essere collegati, in qualità di fornitori di informazioni inerenti all'identificazione e all'autenticazione, a un sistema IAM esterno o a una rete esterna per le identificazioni alle seguenti condizioni:

- a.⁴⁴ il collegamento serve a concedere alle persone di cui agli articoli 8 o 9 l'accesso:
 1. ai sistemi d'informazione gestiti da un gestore esterno su mandato della Confederazione o a sistemi d'informazione terzi ai quali devono accedere per poter eseguire i loro compiti legali, oppure
 2. ai sistemi d'informazione, come le applicazioni per il Governo elettronico, messi a disposizione per l'esecuzione del diritto cantonale dai Cantoni e dai Comuni nonché dalle organizzazioni e dalle persone di diritto pubblico o privato;
- b. tra la Confederazione e il gestore del sistema d'informazione beneficiario esiste un accordo che disciplina il rapporto sotto il profilo legale, organizzativo e tecnico;
- c. il collegamento è configurato in modo da permettere unicamente un accesso a sistemi d'informazione predefiniti.

⁴⁴ Nuovo testo giusta il n. I dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU 2023 738).

² Il settore TDT della CaF disciplina in istruzioni i requisiti da soddisfare in materia di sicurezza, d'intesa con l'organo responsabile per il corrispondente sistema IAM, e periodicamente ne verifica il rispetto.

³ È altresì possibile partecipare a una rete internazionale per le identificazioni sulla base di un trattato internazionale a condizione che sia garantito il rispetto dei requisiti in materia di sicurezza delle informazioni.

Sezione 8: Verbalizzazione, statistiche e documentazione

Art. 25 Verbalizzazione nei sistemi IAM

¹ Il sistema IAM verbalizza le autenticazioni e la comunicazione di dati concernenti l'identità solo per il tempo e nella misura necessari per consentire una gestione sicura e ordinata dei propri sistemi e dei sistemi a valle.

² I dati verbalizzati sono conservati separatamente dal sistema in cui sono trattati i dati personali e distrutti entro due anni. Essi non sono archiviati.⁴⁵

³ È fatta salva una verbalizzazione più dettagliata, una conservazione prolungata o un'archiviazione dei dati protocollati concernenti gli accessi a un determinato sistema d'informazione se lo prevede su una base legale particolare.

Art. 26 Trasmissione di dati verbalizzati da sistemi IAM

¹ I gestori di sistemi IAM della Confederazione possono trasmettere al servizio competente del sistema a valle i dati verbalizzati inerenti all'autenticazione e alla comunicazione di dati concernenti l'identità.

² A tal fine, tramite il consulente per la protezione dei dati, deve essere inviata all'organo responsabile del sistema IAM una richiesta scritta in cui vengono indicati lo scopo e la base legale. La trasmissione può essere concordata in maniera analoga anche nell'accordo di gestione stipulato tra l'organo responsabile e il gestore del sistema IAM.⁴⁶

³ In base ai principi vigenti per l'ottenimento di servizi informatici in seno alla Confederazione la trasmissione può essere soggetta a pagamento.

Art. 27 Statistiche riguardanti i sistemi IAM

Per far fronte alle esigenze del servizio competente del sistema IAM o del sistema d'informazione a valle possono essere elaborate statistiche sugli accessi. I dati personali devono essere resi anonimi.

⁴⁵ Nuovo testo giusta l'all. 2 n. II 18 dell'O del 31 ago. 2022 sulla protezione dei dati, in vigore dal 1° set. 2023 (RU 2022 568).

⁴⁶ Nuovo testo giusta l'all. 2 n. II 18 dell'O del 31 ago. 2022 sulla protezione dei dati, in vigore dal 1° set. 2023 (RU 2022 568).

Art. 28 Inventario e documentazione

¹ Ogni organo che secondo la presente ordinanza è responsabile di un sistema IAM, un servizio di elenchi o un altro sistema d'informazione tiene un inventario su:

- a. i propri sistemi IAM e i propri servizi di elenchi;
- b. i sistemi d'informazione da cui sono ottenuti automaticamente dati;
- c. i sistemi d'informazione i cui dati sono messi a disposizione automaticamente;
- d. tutti i sistemi IAM con cui è collegato il proprio sistema IAM.

² I documenti e i giustificativi importanti, in particolare le richieste secondo la presente ordinanza, devono essere conservati almeno finché sono validi.

Sezione 9: Disposizioni finali**Art. 29** Esecuzione

Il settore TDT della CaF emana le istruzioni amministrative e tecniche per realizzare e gestire i sistemi IAM della Confederazione.

Art. 30 Abrogazione di un altro atto normativo

L'ordinanza del 6 dicembre 2013⁴⁷ sui servizi di elenchi della Confederazione è abrogata.

Art. 31 Entrata in vigore

La presente ordinanza entra in vigore il 1° gennaio 2017.

⁴⁷ [RU 2013 4553]

*Allegato*⁴⁸
(art. 11 e 13 cpv. 1 e 2)

Categorie di dati

Osservazione preliminare: per il significato degli asterischi () si veda l'articolo 11 capoverso 4.*

	Servizi di elenchi	Sistemi IAM con persone secondo gli art. 8 e 9 lett. a	Sistemi IAM con persone secondo l'art. 9 lett. b
a. Dati personali			
1. Cognome*	X	X	X
2. Nomi*	X	X	X
3. Data di nascita		X	X
4. Luogo di nascita			X
5. Nazionalità			X
6. Sesso		X	X
7. Appellativo*	X	X	X
8. Titolo*	X	X	X
9. Iniziali*	X	X	X
10. Identificativi personali locali	X	X	X
11. Denominazione della professione*	X	X	X
12. Lingua per la corrispondenza*	X	X	X
13. Particolari caratteristiche biometriche personali, segnatamente scansione dell'iride, retina, scansione delle vene, impronte digitali, impronta della mano, caratteristiche della forma del viso e profilo vocale		X	
14. Immagine del viso	X	X	X
15. Numero AVS	X	X	X
b. Dati relativi al rapporto con il datore di lavoro/mandante			
1. Rapporto di lavoro (interno/esterno)*	X	X	
2. Informazioni concernenti l'organizzazione e i posti in organico*	X	X	X
3. Futura attribuzione a un'unità organizzativa	X	X	
4. Categoria di personale		X	

⁴⁸ Nuovo testo giusta il n. II dell'O dell'8 nov. 2023, in vigore dal 1° gen. 2024 (RU 2023 738).

	Servizi di elenchi	Sistemi IAM con persone secondo gli art. 8 e 9 lett. a	Sistemi IAM con persone secondo l'art. 9 lett. b
5. Numero personale (anche cantonale)	X	X	
6. Funzione*	X	X	
7. Designazione del posto*	X	X	
8. Identificazione del sistema d'informazione concernente il personale (fonte)	X	X	
9. Data di entrata / data di partenza	X	X	
10. Numero del documento d'identità e/o del badge	X	X	X
c. Dati di contatto			
1. Luogo di lavoro e indirizzo postale professionale*	X	X	X
2. Indirizzo postale privato			X
3. Numero dell'ufficio*	X	X	
4. Elementi dell'indirizzo professionale* come indirizzo di posta elettronica*, numeri di telefono*, numero di fax*, indirizzo VOIP*	X	X	X
5. Elementi dell'indirizzo esterno* (per collaboratori e incaricati*) o elementi dell'indirizzo privato	X	X	X
d. Dati sulle funzioni professionali			
1. Iscrizioni registrate in albi professionali ufficiali (medico, pubblico ufficiale rogatore, avvocato ecc.)		X	X
2. Funzioni secondo il registro di commercio e altri registri di rappresentanza		X	X
e. Dati tecnici			
1. Dispositivi, collegamenti, sistemi, applicazioni ecc. attribuiti	X	X	X
2. Elementi dell'indirizzo, numeri d'identificazione ecc.	X		
3. Linguaggio di sistema dei dispositivi, dei collegamenti ecc.	X	X	X
4. Chiave pubblica dei certificati digitali*	X	X	X
5. Gruppi di autorizzazioni	X	X	X
6. Nomi per la registrazione nei sistemi IT	X	X	X
7. Password (protette crittograficamente)		X	X
8. Ultimo login		X	X
9. Tentativi di login falliti		X	X
10. Status (attivo/passivo)		X	X

	Servizi di elenchi	Sistemi IAM con persone secondo gli art. 8 e 9 lett. a	Sistemi IAM con persone secondo l'art. 9 lett. b
<p>11. Qualità dell'autenticazione</p> <p>f. Dati sui controlli di sicurezza relativi alle persone, se l'esito di quest'ultimi è una dichiarazione di sicurezza senza riserve o se l'autorità decisionale ha emanato una decisione positiva.</p> <p>1. Livello di controllo</p> <p>2. Durata di validità della dichiarazione di sicurezza</p>		<p>X</p> <p>X</p> <p>X</p>	<p>X</p>