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

del 19 ottobre 2016 (Stato 1° gennaio 2017)

Il Consiglio federale svizzero,

vista la legge del 21 marzo 1997[1] sull'organizzazione del Governo e dell'Amministrazione (LOGA);
visti gli articoli 27 capoverso 2 lettera c e 27*a* capoverso 6 della legge del 24 marzo 2000[2] sul personale federale (LPers),

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 IAM[3]), i servizi di elenchi e l'archivio centralizzato delle identità della Confederazione.

Art. 2 Campo d'applicazione

1 La presente ordinanza si applica alle unità amministrative dell'Amministrazione federale centrale di cui all'articolo 7 dell'ordinanza del 25 novembre 1998[4] sull'organizzazione del Governo e dell'Amministrazione (OLOGA).

2 Fatte salve disposizioni di diverso tenore previste dal diritto federale in materia di organizzazione, le autorità e i servizi seguenti possono impegnarsi mediante un accordo a rispettare la presente ordinanza e le prescrizioni e direttive che ne derivano:

a. unità dell'Amministrazione federale decentralizzata di cui all'articolo 7*a* OLOGA;

b. altre autorità federali;

c. organizzazioni e persone di diritto pubblico o privato al di fuori dell'Amministrazione federale alle quali sono però attribuiti compiti dell'Amministrazione federale (art. 2 cpv. 4 LOGA);

RU **2016** 3623

1 RS **172.010**
2 RS **172.220.1**
3 IAM = *Identity and Access Management*
4 RS **172.010.1**

d. istituzioni con scopi pubblici vicine alla Confederazione, se i loro sistemi devono essere collegati a quelli dell'Amministrazione federale.

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.

Sezione 3: Organi responsabili

Art. 5 Sistemi IAM

1 Gli organi federali responsabili dei sistemi IAM sono:

a. l'Organo direzione informatica della Confederazione (ODIC) per tutti i sistemi IAM offerti come servizi standard o esplicitamente attribuiti all'ODIC;

b. la Direzione delle risorse del Dipartimento federale degli affari esteri (DFAE) per il sistema IAM gestito dall'unità Informatica DFAE;

c. lo Stato maggiore dell'esercito per il sistema IAM gestito presso la Base d'aiuto alla condotta (BAC);

d. 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).

2 Il servizio tecnico competente rimane responsabile del sistema a valle, in particolare dell'accesso ad esso.

Art. 6 Servizi di elenchi

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

a. l'ODIC 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 polizia (CSI-DFGP),
   3. la BAC,
   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. diritto di correzione e cancellazione dei dati: presso il servizio del personale della loro unità amministrativa od organizzazione oppure presso il servizio competente per l'aggiornamento dei loro dati.

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 OLOGA[5];

b. collaboratori dell'Amministrazione federale decentralizzata secondo l'articolo 7*a* OLOGA;

c. membri dell'Assemblea federale e collaboratori dei Servizi del Parlamento secondo il titolo quarto, capitolo 7 della legge del 13 dicembre 2002[6] sul Parlamento;

d. persone elette dall'Assemblea federale secondo l'articolo 168 della Costituzione federale[7];

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;

5 RS **172.010.1**
6 RS **171.10**
7 RS **101**

f. collaboratori del Ministero pubblico della Confederazione secondo gli articoli 7–22 della legge del 19 marzo 2010[8] 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.

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;

b. privati e rappresentanti di organizzazioni che accedono a sistemi informatici messi a disposizione dalla Confederazione come le applicazioni per il Governo elettronico.

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 possono essere trattati profili personali.

3 In assenza di una base legale specifica in materia, in questi sistemi non possono essere trattati dati personali degni di particolare protezione.

8 RS **173.71**

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 concernente il personale dell'Amministrazione federale (BV PLUS) secondo l'articolo 11 dell'ordinanza del 26 ottobre 2011[9] sulla protezione dei dati personali del personale federale.

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

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 l'ODIC.

2 BV PLUS trasmette regolarmente, se disponibili, i dati conformemente all'allegato all'archivio centralizzato delle identità. Tutti i dati personali ottenuti automaticamente da BV PLUS 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. sia dotato di una base legale e di un regolamento per il trattamento secondo l'articolo 21 dell'ordinanza del 14 giugno 1993[10] relativa alla legge sulla protezione dei dati (OLPD); e

b. sia notificato all'Incaricato federale della protezione dei dati e della trasparenza oppure non sottostia all'obbligo di notifica conformemente all'articolo 18 OLPD.

9 RS **172.220.111.4**
10 RS **235.11**

5 I dati necessari per la pubblicazione nell'Annuario federale secondo l'articolo 5 dell'ordinanza del 29 ottobre 2008[11] sull'organizzazione della Cancelleria federale sono trasmessi regolarmente alla Cancelleria federale.

Art. 14 Termine di conservazione di dati personali

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.

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 rilevati.

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

11 RS **172.210.10**

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

Art. 18 Requisiti in materia di sicurezza delle informazioni

1 I gestori interni ed esterni di componenti di un sistema IAM devono disporre di direttive documentate sulla sicurezza delle informazioni e sulla gestione dei rischi. In particolare, ogni organo responsabile di un sistema secondo la presente ordinanza emana un regolamento per il trattamento secondo l'articolo 21 OLPD[12].

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

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

4 L'ODIC 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.

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.

12 RS **235.11**

Sezione 7: Rete di sistemi IAM

Art. 20 Rete IAM della Confederazione

I sistemi IAM dell'Amministrazione federale possono essere collegati con i sistemi IAM dei Servizi del Parlamento o dell'esercito 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, a condizione che siano soddisfatte le condizioni e le procedure secondo gli articoli 22 e 23:

a. sistemi IAM comprendenti collaboratori cantonali e comunali secondo l'articolo 9 lettera a;

b. sistemi IAM riconosciuti dall'ODIC 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;

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 dell'ODIC.

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

4 Le richieste di modiche 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. il collegamento serve a concedere alle persone di cui agli articoli 8 o 9 l'accesso 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;

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.

2 L'ODIC 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 distrutti al più tardi dopo due anni. Essi non sono archiviati.

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 responsabile 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.

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.

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

L'ODIC 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 2013[13] sui servizi di elenchi della Confederazione è abrogata.

13 [RU **2013** 4553]

Art. 31 Entrata in vigore

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

Allegato
(art. 11 cpv. 1 e 4 nonché 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(i) attuale(i)*	x	x	x
2. Nome(i) attuale(i)*	x	x	x
3. Data di nascita		x	x
4. Sesso		x	x
5. Appellativo*	x	x	x
6. Titolo*	x	x	x
7. Iniziali*	x	x	x
8. Identificativi personali locali	x	x	x
9. Denominazione della professione*	x	x	x
10. Lingua per la corrispondenza*	x	x	x
b. Dati relativi al rapporto con il datore di lavoro/mandante			
1. Rapporto di lavoro (interno / esterno)*	x	x	
2. Unità organizzativa*	x	x	x
3. Futura attribuzione a un'unità organizzativa	x	x	
4. Categoria di personale		x	
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	
c. Dati di contatto			
1. Luogo di lavoro e indirizzo postale professionale*	x	x	x
2. Numero dell'ufficio*	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
3. Elementi dell'indirizzo professionale* come indirizzo di posta elettronica*, numeri di telefono*, numero di fax*, indirizzo VOIP*	x	x	x
4. 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, 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		x	x
8. Ultimo login		x	x
9. Tentativi di login falliti		x	x
10. Status (attivo/passivo)		x	x