|  |  |
| --- | --- |
|  | Dopo la compilazione almeno: A USO ITERNO |

|  |
| --- |
|  |

Regolamento degli organi federali per il trattamento dei dati

< Nome del progetto / dell’oggetto da proteggere >

|  |
| --- |
|  |

|  |  |
| --- | --- |
| Classificazione | **A USO INTERNO** / CONFIDENZIALE / SEGRETO |
| Stato | **In corso di elaborazione** / in corso di verifica / approvato |
| Numero del progetto | n. |
| Capoprogetto (CP BP) | CP BP |
| Versione | Dal modello V2.1 - P042-Hi04 - Regolamento per il trattamento dei dati |
| Data |  |
| Committente | Committente |
| Elaborato da | Autore |

Controllo delle modifiche

|  |  |  |  |
| --- | --- | --- | --- |
| Versione | Data | Descrizione / Osservazioni | Nome |
| 0.1 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Distribuzione

|  |  |  |
| --- | --- | --- |
| Funzione | Nome  | Dipartimento / Ufficio |
| CPD |  |  |
| ISIU |  |  |
|  |  |  |
|  |  |  |

Indice

1 Considerazioni generali 4

1.1 Descrizione 4

1.2 Scopo del regolamento degli organi federali per il trattamento dei dati 4

1.3 Adeguamento 5

1.4 Ausili 5

1.5 Autorizzazione 6

2 Regolamento degli organi federali sul trattamento 7

2.1 Informazioni generali 7

2.1.1 Basi legali 7

2.1.2 Scopo del trattamento dei dati 8

2.1.3 Categorie di persone interessate e categorie di dati personali trattati 8

2.2 Organizzazione interna 8

2.2.1 Organo federale titolare del trattamento 8

2.2.2 Responsabile del trattamento 9

2.2.3 Utenti e accesso ai dati 9

2.2.3.1 Cerchia di utenti 9

2.2.3.2 Diritti di accesso 10

2.2.3.3 Ruoli 10

2.2.3.4 Processo relativo ai diritti di accesso 10

2.3 Procedura di trattamento e di controllo dei dati 10

2.3.1 Trattamento dei dati personali 11

2.3.1.1 Processi interni 11

2.3.1.2 Comunicazione dei dati e interfacce 11

2.3.1.3 Controllo dei dati personali registrati 12

2.3.1.4 Processi / Procedure per il trattamento dei dati 12

2.3.2 Durata di conservazione, archiviazione e cancellazione 12

2.3.2.1 Durata di conservazione 12

2.3.2.2 Archiviazione 12

2.3.2.3 Cancellazione 12

2.3.3 Diritti delle persone interessate 12

2.4 Misure atte a garantire la sicurezza dei dati 13

3 Allegato 14

3.1 Registro delle attività di trattamento 14

3.2 Valutazione d’impatto sulla protezione dei dati 15

3.3 Piano dei diritti di accesso / Matrice delle autorizzazioni 15

3.4 Elenco dei documenti 17

3.5 Abbreviazioni 18

3.6 Termini 19

# Considerazioni generali

## Descrizione

Descrizione del trattamento automatizzato del progetto TIC.

## Scopo del regolamento degli organi federali per il trattamento dei dati

Il piano SIPD è la base su cui poggia il regolamento per il trattamento dei dati, che rientra nell’ambito dei progetti TIC dell’Amministrazione federale.

L’**organo federale titolare del trattamento e il suo responsabile** (cfr. art. 6 OPDa) stabiliscono un regolamento per il trattamento automatizzato di dati se:

* trattano dati personali degni di particolare protezione;
* effettuano una profilazione;
* trattano dati personali ai sensi dell’articolo 34 capoverso 2 lettera c LPD[[1]](#footnote-1);
* concedono l’accesso a dati personali a Cantoni, autorità estere, organizzazioni internazionali o privati;
* connettono tra loro raccolte di dati; o
* gestiscono insieme ad altri organi federali un sistema d’informazione o raccolte di dati.

L’**IFPDT** è tenuto a elaborare un regolamento sul trattamento per tutti i trattamenti automatizzati (art. 40 OPDa).

Il regolamento contiene in particolare indicazioni

* sull’organizzazione interna,
* sulla procedura di trattamento e di controllo dei dati, nonché
* sui provvedimenti per garantire la sicurezza dei dati.

Contiene anche l’elenco di tutta la documentazione relativa alla pianificazione, alla realizzazione e alla gestione della raccolta di dati. Al regolamento si devono allegare il registro delle attività di trattamento (secondo art. 12 LPD), una valutazione d’impatto sulla protezione dei dati appositamente effettuata (VIPD, secondo art. 22 LPD) e un eventuale piano SIPD.

Il regolamento per il trattamento dei dati provvede alla necessaria trasparenza nell’ambito dello sviluppo e dell’adattamento dei sistemi nonché del trattamento elettronico dei dati personali in relazione a un trattamento automatizzato.

La prima versione del regolamento per il trattamento è disponibile alla fine della fase Concezione HERMES.

L’organo federale titolare del trattamento e il suo responsabile sono tenuti ad aggiornare periodicamente il regolamento e a metterlo a disposizione del consulente per la protezione dei dati.

## Adeguamento

Il regolamento per il trattamento dei dati deve essere il più possibile conciso e comprensibile, in modo che la descrizione della raccolta automatizzata di dati possa essere compresa e valutata anche da persone non esperte in materia (principio).

Il regolamento deve essere tanto più esaustivo quanto più aumenta il volume o la sensibilità dei dati personali da trattare. A meno che non siano già contenuti nel registro delle attività di trattamento, nella VIPD e nel piano SIPD, gli aspetti più importanti dal punto di vista della protezione dei dati e della sicurezza delle informazioni devono essere descritti nel regolamento per il trattamento. Per informazioni più dettagliate si rimanda ai documenti di approfondimento.

È importante non copiare il contenuto dei documenti esistenti, ma fare riferimento ad essi con informazioni precise e allegare tali documenti. Il Regolamento non deve essere un esercizio di copia e riproduzione.

Il testo in blu funge da ausilio alla compilazione del documento.

## Ausili

I seguenti documenti fungono da supporto per l’elaborazione del regolamento per il trattamento dei dati:

**Ausili:**

* [Direttive del delegato federale alla cibersicurezza sulla procedura di sicurezza e sui relativi mezzi ausiliari a livello di Confederazione, NCSC](https://intranet.ncsc.admin.ch/ncscintra/it/home/vorgaben-hilfsmittel/sicherheitsverfahren.html)
* [Strumenti di legistica, UFG](https://www.bj.admin.ch/bj/it/home/staat/legistik/hauptinstrumente.html)
* [Revisione totale della legge sulla protezione dei dati (LPD) - Elaborazione di basi legali per il trattamento dei dati da parte di organi federali: sinossi delle modifiche principali, UFG](https://www.bj.admin.ch/dam/bj/it/data/staat/gesetzgebung/datenschutzstaerkung/dsg-uebersicht-aenderungen.pdf.download.pdf/dsg-uebersicht-aenderungen-i.pdf)
* [Guida di legislazione – protezione dei dati, UFG](https://www.bj.admin.ch/dam/bj/it/data/staat/legistik/hauptinstrumente/leitfaden-datenschutz.pdf.download.pdf/leitfaden-datenschutz-i.pdf)
* Misure tecniche e organizzative (TOM) (nel centro di informazione sulla protezione dei dati dell'IFPDT)

## Autorizzazione

Le firme di autorizzazione devono essere apposte prima dell’inizio dell’attività.

Con la propria firma, il consulente per la protezione dei dati conferma di aver controllato il regolamento per il trattamento. Il consulente ha verificato in particolare che il documento sia stato compilato in ogni sua parte e che tutte le misure richieste siano documentate; ha inoltre analizzato le indicazioni in modo critico per stabilirne la coerenza e l’esattezza nel contesto del trattamento dei dati.

Con la propria firma, il titolare del trattamento approva il relativo regolamento.

|  |  |
| --- | --- |
| Data / Nome / Firma **Consulente per la protezione dei dati**: | …………………………………………………...…... |
| Data / Nome / Firma **Titolare del trattamento**:  | …………………………………………………...…... |
|  |  |

È possibile apporre altre firme.

Le firme possono essere apposte anche in forma elettronica (in un file PDF).

# Regolamento degli organi federali sul trattamento

## Informazioni generali

### Basi legali

Questa sezione presenta le basi legali su cui poggia il trattamento dei dati personali nell’ambito della raccolta dei dati secondo la LPD:

**Art. 34 LPD** Basi legali

1 Gli organi federali hanno il diritto di trattare dati personali soltanto se lo prevede una base legale.

2 La base legale deve figurare in una legge in senso formale nei casi seguenti:

a. sono trattati dati personali degni di particolare protezione;

b. è effettuata una profilazione;

c. lo scopo del trattamento o il tipo di trattamento può comportare una grave ingerenza nei diritti fondamentali della persona interessata.

3 Per il trattamento di dati personali secondo il capoverso 2 lettere a e b è sufficiente una base legale figurante in una legge in senso materiale se:

a. il trattamento è indispensabile per l’adempimento di un compito stabilito in una legge in senso formale; e

b. lo scopo del trattamento non comporta rischi particolari per i diritti fondamentali della persona interessata.

4 In deroga ai capoversi 1–3, gli organi federali possono trattare dati personali se:

a. il Consiglio federale ha autorizzato il trattamento poiché non ritiene pregiudicati i diritti delle persone interessate;

b. la persona interessata ha dato, nel caso specifico, il suo consenso al trattamento oppure ha reso i suoi dati personali accessibili a chiunque e non si è opposta espressamente al trattamento; o

c. il trattamento è necessario per proteggere la vita o l’integrità fisica della persona interessata o di un terzo e non è possibile ottenere il consenso della persona interessata entro un termine ragionevole.

In virtù dell’articolo 9 capoverso 1 LPD, il trattamento di dati personali può essere affidato a un responsabile del trattamento per contratto (p. es. un contratto di esternalizzazione) o per legge se:

* questi effettua soltanto i trattamenti che il titolare del trattamento (ufficio, unità organizzativa) avrebbe il diritto di effettuare; e
* nessun obbligo legale o contrattuale di serbare il segreto lo vieta.

Il titolare del trattamento (ossia l’organo federale titolare del trattamento) deve in particolare assicurare che il responsabile del trattamento sia in grado di garantire la sicurezza dei dati (art. 9 cpv. 2 LPD).

**L’articolo 36 capoverso 5 LPD** prevede quanto segue:

Gli organi federali possono rendere accessibili a chiunque dati personali mediante servizi di informazione e comunicazione automatizzati se una base legale prevede la pubblicazione di questi dati, oppure nell’ambito dell’informazione ufficiale del pubblico in virtù del capoverso 3. Se cessa l’interesse pubblico a renderli accessibili a chiunque, i dati contenuti nel servizio di informazione e comunicazione automatizzato devono essere cancellati.

### Scopo del trattamento dei dati

(Basi legali: art. 6 cpv. 3 LPD in combinato disposto con art. 1 cpv. 2 lett. b OPDa, art. 6 cpv. 4–5, art. 7 cpv. 3, art. 12 cpv. 2 LPD)

Si devono descrivere scopo, tipo, entità e circostanze del trattamento.

Nella premessa si devono illustrare brevemente i motivi per cui si intende allestire un sistema e descrivere lo scopo (o gli scopi) nonché lo stato auspicato

### Categorie di persone interessate e categorie di dati personali trattati

(Basi legali: art. 6 cpv. 6 e 7, art. 12 cpv. 2, art. 19 LPD; art. 1 cpv. 2 lett. a, art. 13 OPDa)

In merito al contenuto dei dati trattati occorre informare su:

* tipologia di dati personali trattata (dati personali, dati personali degni di particolare protezione, profilazione a rischio elevato, altri);
* tipologia, categorie (o «gruppi») e numero di persone e dati personali trattati;
* modalità di raccolta dei dati personali.

## Organizzazione interna

(Basi legali: art. 9, 10, 12, 13, 33 LPD; art. 7, 8, 17, 23, 25 OPDa)

### Organo federale titolare del trattamento

Riportare l’organigramma dell’organo federale responsabile del trattamento dei dati e dei relativi settori (incl. il numero di collaboratori) che lavorano con i dati. In particolare, indicare il titolare del trattamento, il responsabile delle applicazioni, il consulente per la protezione dei dati e l’ISIU.

Se un organo federale tratta dati personali congiuntamente ad altri organi federali, a organi cantonali o a privati, vanno indicate le procedure di controllo e la responsabilità in materia di protezione dei dati.

Se non figurano nel piano SIPD già allegato, occorre inoltre identificare i responsabili dell’applicazione, della rete, della banca dati, del sistema operativo ecc. che contiene i dati o nel cui ambito sono disponibili.

Indicazioni su:

Organo federale titolare del trattamento:

Utenti DataReg:

Responsabile delle applicazioni:

Consulente per la protezione dei dati:

ISIU:

Responsabile dell’applicazione:

Responsabile della rete:

Responsabile della banca dati:

Responsabile del sistema operativo:

### Responsabile del trattamento

Si devono indicare il responsabile del trattamento competente e le persone di riferimento responsabili.

Indicazioni su:

Responsabile del trattamento:

Persona di riferimento FP/Responsabile del trattamento:

### Utenti e accesso ai dati

#### Cerchia di utenti

Riportare le categorie (o «i gruppi») di tutte le unità amministrative o posizioni (organi federali, cantonali, terzi) autorizzate all’accesso. Spiegare brevemente per quali compiti legali hanno bisogno di accedere alla raccolta di dati.

Eventualmente, inserire qui un rimando alla matrice della comunicazione del piano SIPD.

Di seguito è riportato un esempio di una possibile rappresentazione.

Schizzo

Sistemi circostanti

| **Nome** | **Descrizione** | **Scopo** |
| --- | --- | --- |
| eIAM | Sistema centrale di gestione degli accessi e delle autorizzazioni dell’Amministrazione federale.  | Utilizzato per l’autenticazione degli utenti e l’autorizzazione generica (attribuzione dei ruoli). |
|  |  |  |
|  |  |  |

**eIAM / Keycloak**

eIAM è il sistema centrale di gestione degli accessi e delle autorizzazioni dell’amministrazione federale. La Cancelleria federale è responsabile del sistema e l’UFIT si occupa della sua gestione (cfr. <https://www.eiam.admin.ch/>).

#### Diritti di accesso

Elencare e descrivere brevemente il tipo e l’estensione dell’accesso degli utenti alla raccolta di dati nonché i campi dei dati. Se esiste già una matrice delle autorizzazioni (o un piano dei diritti di accesso), deve essere aggiunta al regolamento per il trattamento come allegato.

#### Ruoli

A quali ruoli sono stati assegnati diritti di accesso (ad es. collaboratore specializzato, amministratore) e quali diritti di accesso sono stati attribuiti a ogni ruolo (interrogazione, elaborazione, stampa, nessun accesso, altro)?

Di seguito è riportato un esempio di una possibile rappresentazione.

| **Nome** | **Descrizione** |
| --- | --- |
| Collaboratore specializzato |  |
| Responsabile delle applicazioni |  |
| Amministratore |  |
| … |  |

#### Processo relativo ai diritti di accesso

Qui occorre descrivere le modalità (processo e responsabilità) relative all’assegnazione e alla revoca dei diritti di accesso, fornendo le informazioni seguenti:

* Chi è responsabile dell’assegnazione e della revoca dei diritti di accesso?
* Chi controlla regolarmente i diritti di accesso assegnati e li aggiorna?
* Estensione dei diritti di accesso?
* Esiste un processo per l’assegnazione e la revoca dei diritti di accesso?
* Iter del processo?
* Il processo è gestito a livello centralizzato?

## Procedura di trattamento e di controllo dei dati

(Basi legali: art. 6–10, 12, 13, 16, 19, 21, 22, 24, 25, 28, 33, 36, 37, 41, 42 LPD; art. 1–4, 6, 9–13, 15–18, 20, 22, 26, 29, 30 OPDa)

Argomenti:

Distruzione dei dati nel momento in cui non sono più necessari allo scopo del trattamento

Misure atte alla rettifica dei dati personali

Consenso al trattamento dei dati personali

Protezione dei dati attraverso la tecnologia e preimpostazioni orientate alla protezione dei dati

Misure di sicurezza dei dati

Rapporto con il responsabile del trattamento

Coinvolgimento del consulente per la protezione dei dati

Gestione del registro delle attività di trattamento

Utilizzo di certificazioni

Condizioni per la comunicazione legale dei dati personali all’estero

Obbligo di informare sulla raccolta di dati personali

Obbligo di informare sulle decisioni individuali automatizzate

Valutazione d’impatto sulla protezione dei dati

Segnalazione di violazioni della sicurezza dei dati

Configurazione del diritto d’accesso

Diritto alla consegna o alla trasmissione dei dati

Controllo e responsabilità in caso di trattamento congiunto dei dati personali

Comunicazione dei dati personali

Opposizione alla comunicazione di dati personali da parte di un organo federale

Altre pretese e procedure nei confronti di un organo federale

Comunicazione di documenti ufficiali contenenti dati personali

### Trattamento dei dati personali

#### Processi interni

In questa sezione si devono documentare e/o rappresentare graficamente i processi interni di raccolta di dati più importanti dal punto di vista della protezione dei dati.

#### Comunicazione dei dati e interfacce

Le interfacce con altri oggetti da proteggere come sistemi, applicazioni, software ecc. devono essere rappresentate graficamente qui. È possibile inserire anche un rimando a un eventuale piano SIPD che contenga già una panoramica di questo tipo.

La descrizione delle interfacce deve contenere le seguenti informazioni relative alla trasmissione (comunicazione) di dati:

* Da chi provengono i dati personali?
* Chi riceve i dati personali?
* A che scopo vengono trasmessi i dati personali?
* Quali categorie (o «gruppi») di dati personali vengono trasmesse?
* Con quale frequenza vengono trasmessi i dati personali?
* Chi avvia la procedura di trasmissione?
* Con l’aiuto di quale strumento vengono trasmessi i dati personali?

Gli scopi per cui i dati personali vengono regolarmente comunicati si devono evincere dalla descrizione delle interfacce.

#### Controllo dei dati personali registrati

Chi controlla l’esattezza dei dati personali? Esiste un processo in tal senso? Questi dati vengono controllati e rettificati regolarmente?

#### Processi / Procedure per il trattamento dei dati

Si devono definire e descrivere i processi di rettifica, blocco, anonimizzazione, registrazione, conservazione, archiviazione e distruzione dei dati.

### Durata di conservazione, archiviazione e cancellazione

#### Durata di conservazione

Si devono chiarire le seguenti questioni:

* Per quanto tempo si possono o devono conservare i dati personali registrati o le categorie («gruppi») di dati personali?
* Luogo e responsabilità della conservazione dei dati personali?
* In quale momento vengono cancellati o devono essere consegnati all’Archivio federale?

#### Archiviazione

Si devono definire qui le modalità tecniche e organizzative (formato dei file, interfacce) per offrire all’Archivio federale di riprendere i dati personali o per la loro trasmissione all’Archivio stesso.

#### Cancellazione

In quale momento i dati personali non più necessari vengono cancellati dalla raccolta di dati? Questa formulazione deve essere stabilita d’intesa con l’ISIU e il responsabile delle applicazioni.

### Diritti delle persone interessate

Si deve stabilire in particolare a chi debba rivolgersi la persona interessata (persona di riferimento/destinatario) e la relativa procedura interna (processo).

Si devono creare gli strumenti e le procedure per l’esercizio del diritto d’accesso, del diritto alla consegna o alla trasmissione dei dati, del diritto alla rettifica, alla distruzione e al blocco nonché del diritto di aggiungere una menzione del carattere contestato. Devono sussistere ed essere attuabili appositi strumenti per il blocco della comunicazione a terzi.

L’obbligo di informare sulla raccolta di dati personali a opera di organi federali deve essere considerato e regolato.

## Misure atte a garantire la sicurezza dei dati

(Basi legali: art. 7, 8, 10, 12, 13, 22, 24, 33 LPD; art. 1–4, 6, 15, 25–27 OPDa)

Qui si devono elencare le misure tecniche e organizzative che garantiscono una protezione dei dati adeguata e che non sono già contenute nel piano SIPD.

Schizzo

# Allegato

## Registro delle attività di trattamento

Il titolare del trattamento e il responsabile del trattamento tengono ciascuno un registro delle loro attività di trattamento (art. 12 LPD).

Il registro del titolare del trattamento contiene almeno:

* l’identità del titolare del trattamento;
* lo scopo del trattamento;
* una descrizione delle categorie di persone interessate e delle categorie di dati personali trattati;
* le categorie di destinatari;
* se possibile, la durata di conservazione dei dati personali o i criteri per determinare tale durata;
* se possibile, una descrizione generale dei provvedimenti tesi a garantire la sicurezza dei dati personali secondo l’articolo 8 LPD;
* nel caso in cui i dati siano comunicati all’estero, le informazioni sullo Stato destinatario e le garanzie secondo l’articolo 16 capoverso 2 LPD.

Il registro del responsabile del trattamento contiene informazioni sull’identità del responsabile e del titolare, sulle categorie dei trattamenti che vengono svolti su incarico del titolare, nonché almeno:

* se possibile, una descrizione generale dei provvedimenti tesi a garantire la sicurezza dei dati personali secondo l’articolo 8 LPD;
* nel caso in cui i dati siano comunicati all’estero, le informazioni sullo Stato destinatario e le garanzie secondo l’articolo 16 capoverso 2 LPD.

La notifica dei registri è obbligatoria per tutti gli organi federali (art. 12 cpv. 4 LPD) e, come la prima versione del regolamento per il trattamento dei dati, è fatta alla fine della fase Concezione (art. 31 cpv. 2 OPDa).

Gli organi federali sono tenuti ad aggiornare regolarmente le indicazioni succitate e a notificare i registri all’IFPDT. La notifica avviene tramite l’applicazione web «DataReg» dell’IFPDT.

Una copia della notifica del registro deve essere allegata al regolamento per il trattamento dei dati.

## Valutazione d’impatto sulla protezione dei dati

In determinate condizioni, il titolare del trattamento deve redigere una valutazione d’impatto sulla protezione dei dati (art. 22 LPD).

La VIPD deve contenere una descrizione del trattamento previsto, una valutazione dei rischi per la personalità o per i diritti fondamentali della persona interessata, nonché i provvedimenti a tutela della personalità e dei diritti fondamentali.

Se è stata effettuata una VIPD, se ne deve allegare una copia al regolamento sul trattamento.

## Piano dei diritti di accesso / Matrice delle autorizzazioni

Il piano dei diritti di accesso o la matrice delle autorizzazioni devono essere inseriti nel regolamento per il trattamento come allegati.

Segue un **esempio** semplificato di una matrice delle autorizzazioni.

|  |  |  |  |
| --- | --- | --- | --- |
| Nome campo dati | Confederazione | Cantone | Terzi |
|  | UA I | UA II | UA III | … | … | … | Uff. cant. | … | … | … | … | … | … | … |
|  |
| I. Dati di base |
| Cognome/i | I | I | T | … | … | … | I | … | … | … | … | … | … | … |
| Nome/i | I | I | T | … | … | … | I | … | … | … | … | … | … | … |
| Data di nascita |  | I | I | … | … | … | I | … | … | … | … | … | … | … |
| Nazionalità |  | I | I | … | … | … | T | … | … | … | … | … | … | … |
| … | … | … | … | … | … | … | … | … | … | … | … | … | … | … |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| II. Informazioni sul dossier |
| Titolare del dossier | T | T | T | … | … | … | I | … | … | … | … | … | … | … |
| Stato del dossier | T | T | T | … | … | … |  | … | … | … | … | … | … | … |
| Numero di riferimento | I | T | T | … | … | … | T | … | … | … | … | … | … | … |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| III. Titolo X |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Livelli di accesso**

I = Interrogazione

T = Trattamento

vuoto = nessun accesso

altro

**Unità amministrative**

UA I: ad es. servizio legale dell’UA interessata

UA II: ad es. collaboratore specializzato dell’UA interessata

UA III: ad es. amministratore dell’UA interessata

…

Uff. cant.: ad es. polizia cantonale

…

## Elenco dei documenti

Comprende l’elenco di tutte le leggi, ordinanze, istruzioni, regolamentazioni, specifiche tecniche ecc. rilevanti per la raccolta di dati in oggetto, inclusi i documenti propri del dipartimento e/o dell’ufficio.

|  |  |
| --- | --- |
| Tipo di documento | Titolo |
| Leggi | Base legale dell’oggetto da proteggere (inserita dall’autore) |
|  | [Legge federale del 25 settembre 2020 sulla protezione dei dati (LPD; RS](https://www.fedlex.admin.ch/eli/oc/2022/491/it) *[235.1](https://www.fedlex.admin.ch/eli/oc/2022/491/it)*[)](https://www.fedlex.admin.ch/eli/oc/2022/491/it) |
|  | [Legge federale del 17 dicembre 2004 sul principio di trasparenza dell'amministrazione (legge sulla trasparenza, LTras; RS](http://www.admin.ch/ch/i/sr/c152_3.html) *[152.3](http://www.admin.ch/ch/i/sr/c152_3.html)*[)](http://www.admin.ch/ch/i/sr/c152_3.html) |
|  | [Legge federale del 26 giugno 1998 sull'archiviazione (legge sull'archiviazione, LAr; RS](http://www.admin.ch/ch/i/sr/c152_1.html) *[152.1](http://www.admin.ch/ch/i/sr/c152_1.html)*[)](http://www.admin.ch/ch/i/sr/c152_1.html) |
| Ordinanze | [Ordinanza del 25 novembre 2020 sul coordinamento della trasformazione digitale e la governance delle TIC in seno all'Amministrazione federale (ordinanza sulla trasformazione digitale e l'informatica, OTDI; RS](https://www.fedlex.admin.ch/eli/cc/2020/988/it) *[172.010.58](https://www.fedlex.admin.ch/eli/cc/2020/988/it)*[)](https://www.fedlex.admin.ch/eli/cc/2020/988/it) |
|  | [Ordinanza del 31 agosto 2022 sulla protezione dei dati (OPDa; RS](https://www.fedlex.admin.ch/eli/cc/2022/568/it) *[235.11](https://www.fedlex.admin.ch/eli/cc/2022/568/it)*[)](https://www.fedlex.admin.ch/eli/cc/2022/568/it) |
|  | [Ordinanza del 4 luglio 2007 sulla protezione delle informazioni della Confederazione (ordinanza sulla protezione delle informazioni, OPrI; RS](https://www.fedlex.admin.ch/eli/cc/2007/414/it) *[510.411](https://www.fedlex.admin.ch/eli/cc/2007/414/it)*[)](https://www.fedlex.admin.ch/eli/cc/2007/414/it) |
|  | [Ordinanza del 22 novembre 2017 sulla protezione dei dati personali del personale federale (OPDPers; RS](https://www.fedlex.admin.ch/eli/cc/2017/793/it) *[172.220.111.4](https://www.fedlex.admin.ch/eli/cc/2017/793/it)*[)](https://www.fedlex.admin.ch/eli/cc/2017/793/it) |
|  | [Ordinanza del 27 maggio 2020 sulla protezione contro i ciber-rischi nell'Amministrazione federale (ordinanza sui ciber-rischi, OCiber; RS](https://www.fedlex.admin.ch/eli/cc/2020/416/it) *[120.73](https://www.fedlex.admin.ch/eli/cc/2020/416/it)*[)](https://www.fedlex.admin.ch/eli/cc/2020/416/it) |
| Strategie | [SN002 - Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) 2018–2022 - 18.4.2018](https://intranet.ncsc.admin.ch/dam/ncscintra/it/dokumente/grundlagen/ncs/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_IT.pdf.download.pdf/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_IT.pdf) |
|  |  |
| Documenti propri | Piano dei diritti di accesso |
|  | Rappresentazione del flusso di dati / Diagramma del flusso di dati |
|  | Struttura architettura IT |
|  | … |

## Abbreviazioni

|  |  |
| --- | --- |
| Abbreviazione | Significato |
| art. | articolo |
| BP | beneficiario di prestazioni |
| CP | Capoprogetto |
| CPD | Consulenti per la protezione dei dati |
| cpv. | capoverso |
| FP | fornitore di prestazione |
| IFPDT | Incaricato federale della protezione dei dati e della trasparenza |
| ISIU | Incaricato della sicurezza informatica a livello di unità amministrativa |
| lett. | lettera |
| LPD | Legge federale sulla protezione dei dati (RS *235.1*) |
| NCSC | Centro nazionale per la cibersicurezza |
| OPDa | Ordinanza sulla protezione dei dati (RS *235.11*) |
| Piano SIPD | Piano per la sicurezza delle informazioni e la protezione dei dati |
| RS | Raccolta sistematica del diritto federale |
| TIC | Tecnologie dell’informazione e della comunicazione |
| UA | Unità amministrativa |
| UFG | Ufficio federale di giustizia |
| … | … |

## Termini

|  |  |
| --- | --- |
| Termine | Significato |
| Trattamento | Qualsiasi operazione relativa a dati personali, indipendentemente dai mezzi e dalle procedure impiegati, segnatamente la raccolta, la registrazione, la conservazione, l’utilizzazione, la modificazione, la comunicazione, l’archiviazione, la cancellazione o la distruzione di dati (cfr. art. 5 lett. d LPD). |
| Comunicazione | La trasmissione di dati personali o il fatto di renderli accessibili (cfr. art. 5 lett. e LPD). |
| Dati personali degni di particolare protezione | Dati concernenti le opinioni o attività religiose, filosofiche, politiche o sindacali; dati concernenti la salute, la sfera intima o l’appartenenza a una razza o a un’etnia; dati genetici; dati concernenti le misure d’assistenza sociale; dati concernenti perseguimenti e sanzioni amministrativi e penali; dati biometrici che identificano in modo univoco una persona fisica (art. 5 lett. c LPD). |
| Violazione della sicurezza dei dati | Violazione della sicurezza in seguito alla quale, in modo accidentale o illecito, dati personali vengono persi, cancellati, distrutti, modificati oppure divulgati o resi accessibili a persone non autorizzate (art. 5 lett. h LPD). |
| Titolare del trattamento | Il privato o l’organo federale che, singolarmente o insieme ad altri, determina lo scopo e i mezzi del trattamento (art. 5 lett. j LPD). |
| Responsabile del trattamento | Il privato o l’organo federale che tratta dati personali per conto del titolare del trattamento (art. 5 lett. k LPD). |
| Dati personali, persona interessata | Tutte le informazioni concernenti una persona fisica identificata o identificabile (art. 5 lett. a e b LPD). |
| Profilazione | Trattamento automatizzato di dati personali consistente nell’utilizzazione degli stessi per valutare determinati aspetti personali di una persona fisica, in particolare per analizzare o prevedere aspetti concernenti il rendimento professionale, la situazione economica, la salute, le preferenze, gli interessi, l’affidabilità, il comportamento, i luoghi di permanenza e gli spostamenti di tale persona (art. 5 lett. f LPD). |
| Profilazione a rischio elevato | Profilazione che comporta un rischio elevato per la personalità o i diritti fondamentali della persona interessata poiché comporta un collegamento tra dati che permette di valutare aspetti essenziali della personalità di una persona fisica (art. 5 lett. g LPD). |
| … | … |

1. **Art. 34** Basi legali:
2 La base legale deve figurare in una legge in senso formale nei casi seguenti:
c. lo scopo del trattamento o il tipo di trattamento **può comportare una grave ingerenza nei diritti fondamentali** della persona interessata. [↑](#footnote-ref-1)