Ordinanza sulla protezione dei dati (OPDa)

del 31 agosto 2022 (Stato 1° aprile 2025)

Il Consiglio federale svizzero,

visti gli articoli 8 capoverso 3, 10 capoverso 4, 12 capoverso 5, 16 capoverso 3, 25 capoverso 6, 28 capoverso 3, 33, 59 capoversi 2 e 3 della legge federale del 25 settembre 2020[1] sulla protezione dei dati (LPD),

ordina:

Capitolo 1: Disposizioni generali

Sezione 1: Sicurezza dei dati

Art. 1 Principi

1 Al fine di garantire una sicurezza dei dati adeguata, il titolare del trattamento e il responsabile del trattamento definiscono la necessità di protezione dei dati personali e stabiliscono i provvedimenti tecnici e organizzativi adeguati in considerazione del rischio.

2 La necessità di protezione dei dati personali è valutata sulla base dei seguenti criteri:

a. tipo di dati trattati;

b. scopo, tipo, portata e circostanze del trattamento.

3 Il rischio per la personalità o i diritti fondamentali della persona interessata è valutato sulla base dei seguenti criteri:

a. cause del rischio;

b. pericolo sostanziale;

c. provvedimenti adottati o previsti per minimizzare il rischio;

d. probabilità e gravità di una violazione della sicurezza dei dati nonostante i provvedimenti adottati o previsti.

4 Nello stabilire i provvedimenti tecnici e organizzativi si applicano inoltre i seguenti criteri:

a. lo stato della tecnica;

b. le spese di implementazione.

RU **2022** 568

1 RS **235.1**

5 La necessità di protezione dei dati personali, il rischio e i provvedimenti tecnici e organizzativi sono verificati durante l'intera durata del trattamento. Se necessario, i provvedimenti sono aggiornati.

Art. 2 Obiettivi

Conformemente alla necessità di protezione, il titolare del trattamento e il responsabile del trattamento adottano provvedimenti tecnici e organizzativi affinché i dati trattati:

a. siano accessibili solo alle persone autorizzate (confidenzialità);
b. siano disponibili quando necessario (disponibilità);
c. non siano modificati indebitamente o inavvertitamente (integrità);
d. siano trattati in modo tracciabile (tracciabilità).

Art. 3 Provvedimenti tecnici e organizzativi

1 Per garantire la confidenzialità, il titolare del trattamento e il responsabile del trattamento adottano provvedimenti adeguati affinché:

a. le persone autorizzate abbiano accesso solo ai dati personali di cui abbisognano al fine di adempiere i loro compiti (controllo dell'accesso ai dati);
b. solo le persone autorizzate abbiano accesso ai locali e agli impianti utilizzati per il trattamento dei dati personali (controllo dell'accesso ai locali e agli impianti);
c. le persone non autorizzate non possano utilizzare i sistemi di trattamento automatizzato di dati personali con l'ausilio di impianti di trasmissione (controllo degli utenti);

2 Per garantire la disponibilità e l'integrità, il titolare del trattamento e il responsabile del trattamento adottano provvedimenti adeguati affinché:

a. le persone non autorizzate non possano leggere, copiare, modificare, spostare, cancellare o distruggere supporti di dati (controllo dei supporti di dati);
b. le persone non autorizzate non possano salvare, leggere, modificare, cancellare o distruggere dati personali nella memoria (controllo di memoria);
c. le persone non autorizzate non possano leggere, copiare, modificare, cancellare o distruggere dati personali in occasione della comunicazione degli stessi o del trasporto di supporti di dati (controllo del trasporto);
d. la disponibilità e l'accesso ai dati personali possano essere rapidamente ripristinati in caso di incidente fisico o tecnico (ripristino);
e. siano disponibili tutte le funzioni del sistema di trattamento automatizzato dei dati (disponibilità), siano segnalati eventuali malfunzionamenti (affidabilità) e i dati personali registrati non siano danneggiati da malfunzionamenti del sistema (integrità dei dati);

f. sia sempre aggiornato il livello di sicurezza dei sistemi operativi e delle applicazioni e siano colmate le lacune critiche riscontrate (sicurezza del sistema).

3 Per garantire la tracciabilità, il titolare del trattamento e il responsabile del trattamento adottano provvedimenti adeguati affinché:

a. si possa verificare quali dati personali sono stati introdotti o modificati nel sistema di trattamento automatizzato dei dati, in quale momento e da chi (controllo dell'introduzione);

b. si possa verificare a chi sono stati comunicati dati personali con l'ausilio di impianti di trasmissione (controllo di comunicazione);

c. si possano individuare rapidamente le violazioni della sicurezza dei dati (individuazione) e adottare provvedimenti per ridurre o eliminare le conseguenze (eliminazione).

Art. 4 Verbalizzazione

1 Se dati personali degni di particolare protezione sono trattati automaticamente su grande scala o se si esegue una profilazione a rischio elevato e i provvedimenti preventivi possono non garantire la protezione dei dati, il titolare privato del trattamento e il suo responsabile privato del trattamento verbalizzano almeno la registrazione, modificazione, lettura, comunicazione, cancellazione e distruzione dei dati. In particolare, la verbalizzazione deve avere luogo quando non è possibile stabilire a posteriori se i dati sono stati trattati ai fini per i quali sono stati raccolti o comunicati.

2 Nel caso di trattamento automatico dei dati personali l'organo federale titolare del trattamento e il suo responsabile del trattamento verbalizzano almeno la registrazione, modificazione, lettura, comunicazione, cancellazione e distruzione dei dati.

3 Nel caso di dati personali accessibili in modo generalizzato al pubblico sono verbalizzati almeno la registrazione, modificazione, cancellazione e distruzione dei dati.

4 I verbali riportano informazioni sull'identità della persona che ha effettuato il trattamento, sul tipo, la data e l'ora del trattamento nonché, all'occorrenza, sull'identità del destinatario dei dati.

5 I verbali sono conservati per almeno un anno separatamente dal sistema in cui sono trattati i dati personali. Sono accessibili esclusivamente agli organi e alle persone incaricate di verificare l'applicazione delle disposizioni in materia di protezione dei dati o di salvaguardare o ripristinare la confidenzialità, l'integrità, la disponibilità e la tracciabilità dei dati e sono utilizzati soltanto a tale fine.

Art. 5 Regolamento dei privati sul trattamento

1 Il titolare privato del trattamento e il suo responsabile privato stabiliscono un regolamento per i trattamenti automatizzati se:

a. trattano su grande scala dati personali degni di particolare protezione; o

b. eseguono una profilazione a rischio elevato.

2 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.

3 Il titolare privato del trattamento e il suo responsabile privato aggiornano periodicamente il regolamento. Se è stato designato un consulente per la protezione dei dati, il regolamento è messo a sua disposizione.

Art. 6 Regolamento degli organi federali sul trattamento

1 L'organo federale titolare del trattamento e il suo responsabile stabiliscono un regolamento per i trattamenti automatizzati se:

a. trattano dati personali degni di particolare protezione;

b. effettuano una profilazione;

c. trattano dati personali ai sensi dell'articolo 34 capoverso 2 lettera c LPD;

d. concedono l'accesso a dati personali a Cantoni, autorità estere, organizzazioni internazionali o privati;

e. connettono tra loro raccolte di dati; o

f. gestiscono insieme ad altri organi federali un sistema d'informazione o raccolte di dati.

2 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.

3 L'organo federale titolare del trattamento e il suo responsabile aggiornano periodicamente il regolamento e lo mettono a disposizione del consulente per la protezione dei dati.

Sezione 2: Trattamento da parte del responsabile del trattamento

Art. 7

1 La previa autorizzazione del titolare del trattamento, che permette al responsabile del trattamento di trasferire il trattamento dei dati a un terzo, può essere di natura specifica o generale.

2 Se l'autorizzazione è di natura generale, il responsabile del trattamento informa il titolare del trattamento su qualsiasi modifica prevista per quanto riguarda il coinvolgimento o la sostituzione di altri terzi. Il titolare del trattamento può opporsi a tale modifica.

Sezione 3: Comunicazione di dati personali all'estero

Art. 8 Valutazione dell'adeguatezza della protezione dei dati di uno Stato, un territorio, un determinato settore di uno Stato o un organismo internazionale

1 Gli Stati, i territori, determinati settori di uno Stato e gli organismi internazionali con una protezione adeguata dei dati sono elencati nell'allegato 1.

2 Per valutare se uno Stato, un territorio, un determinato settore di uno Stato o un organismo internazionale garantisce una protezione adeguata dei dati, vanno segnatamente presi in considerazione i seguenti criteri:

a. gli impegni internazionali dello Stato o dell'organismo internazionale, in particolare nel settore della protezione dei dati;

b. lo Stato di diritto e il rispetto dei diritti dell'uomo;

c. la legislazione vigente in particolare in materia di protezione dei dati, la sua attuazione e la giurisprudenza pertinente;

d. l'effettiva garanzia dei diritti delle persone interessate e della tutela giurisdizionale;

e. l'effettivo funzionamento di una o più autorità indipendenti responsabili della protezione dei dati nello Stato in questione o alle quali è assoggettato un organismo internazionale e dotate di poteri e competenze sufficienti.

3 L'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) viene consultato al momento di ogni valutazione. Possono essere presi in considerazione i pareri di organismi internazionali o autorità estere competenti per la protezione dei dati.

4 L'adeguatezza della protezione dei dati è periodicamente oggetto di una nuova valutazione.

5 Le valutazioni vengono pubblicate.

6 Se dalla valutazione secondo il capoverso 4 o da altre informazioni si evince che non è più garantita una protezione adeguata dei dati, l'allegato 1 è modificato; tale modifica non ha alcuna ripercussione sulle comunicazioni di dati già avvenute.

Art. 9 Clausole contrattuali di protezione dei dati e garanzie specifiche

1 Le clausole contrattuali di protezione dei dati di un contratto secondo l'articolo 16 capoverso 2 lettera b LPD e le garanzie specifiche secondo l'articolo 16 capoverso 2 lettera c LPD contengono almeno i seguenti punti:

a. l'applicazione dei principi della liceità, della buona fede, della proporzionalità, della trasparenza, della finalità e dell'esattezza;

b. le categorie dei dati personali comunicati e delle persone interessate;

c. il tipo e lo scopo della comunicazione dei dati personali;

d. all'occorrenza, il nome degli Stati o degli organismi internazionali cui sono comunicati dati personali nonché i requisiti della comunicazione;

e. i requisiti della conservazione, della cancellazione e della distruzione di dati personali;

f. i destinatari o le categorie dei destinatari;

g. i provvedimenti per garantire la sicurezza dei dati;

h. l'obbligo di comunicare le violazioni della sicurezza dei dati;

i. se i destinatari sono titolari del trattamento, l'obbligo di informare le persone interessate dal trattamento;

j. i diritti della persona interessata, segnatamente:
   1. il diritto d'accesso e il diritto alla consegna o alla trasmissione dei dati,
   2. il diritto di opporsi alla comunicazione dei dati,
   3. il diritto di chiedere la rettifica, la cancellazione o la distruzione dei dati che la concernono,
   4. il diritto di chiedere tutela giurisdizionale a un'autorità indipendente.

2 Il titolare del trattamento e, nel caso di clausole contrattuali sulla protezione dei dati, il responsabile del trattamento prendono misure adeguate per garantire che il destinatario rispetti dette clausole o le garanzie specifiche.

3 Se l'IFPDT è stato informato sulle clausole contrattuali di protezione dei dati o sulle garanzie specifiche, l'obbligo di informare è considerato adempiuto per tutte le ulteriori comunicazioni che:

a. si basano sulle medesime clausole contrattuali o garanzie, sempre che le categorie dei destinatari, la finalità del trattamento o le categorie di dati rimangano sostanzialmente immutate; o

b. sono effettuate in seno alla medesima persona giuridica o società o tra imprese che appartengono allo stesso gruppo.

Art. 10 Clausole tipo di protezione dei dati

1 Se comunica dati personali all'estero mediante clausole tipo di protezione dei dati secondo l'articolo 16 capoverso 2 lettera d LPD, il titolare o il responsabile del trattamento adotta provvedimenti adeguati per garantire che il destinatario le rispetti.

2 L'IFPDT pubblica un elenco di clausole tipo di protezione dei dati che ha approvato, emanato o riconosciuto. Comunica i risultati dell'esame delle clausole tipo di protezione dei dati che gli sono state sottoposte entro 90 giorni dalla loro ricezione.

Art. 11 Norme interne dell'impresa vincolanti sulla protezione dei dati

1 Le norme interne dell'impresa vincolanti sulla protezione dei dati secondo l'articolo 16 capoverso 2 lettera e LPD valgono per tutte le imprese che appartengono allo stesso gruppo.

2 Comprendono almeno i punti menzionati nell'articolo 9 capoverso 1 e le seguenti indicazioni:

a. l'organizzazione e i dati di contatto del gruppo e delle sue imprese;

b. le misure adottate in seno al gruppo per il rispetto delle norme interne dell'impresa vincolanti sulla protezione dei dati.

3 L'IFPDT comunica i risultati dell'esame delle norme interne dell'impresa vincolanti sulla protezione dei dati che gli sono state sottoposte entro 90 giorni dalla loro ricezione.

Art. 12 Codici di condotta e certificazioni

1 I dati personali possono essere comunicati all'estero, se un codice di condotta o una certificazione garantisce una protezione adeguata dei dati.

2 Il codice di condotta deve essere previamente sottoposto all'IFPDT per approvazione.

3 Il codice di condotta o la certificazione deve essere corredato dall'impegno vincolante ed esecutorio del titolare del trattamento o del responsabile del trattamento nello Stato terzo di applicare le misure contenutevi.

Capitolo 2: Obblighi del titolare del trattamento

Art. 13 Modalità dell'obbligo di informare

Il titolare del trattamento comunica alla persona interessata le informazioni sull'ottenimento di dati personali in forma precisa, trasparente, comprensibile e facilmente accessibile.

Art. 14 Conservazione della valutazione d'impatto sulla protezione dei dati

Il titolare del trattamento conserva la valutazione d'impatto sulla protezione dei dati per almeno due anni dopo la fine del trattamento.

Art. 15 Notifica di violazioni della sicurezza dei dati

1 La notifica all'IFPDT di una violazione della sicurezza dei dati riporta le seguenti informazioni:

a. il tipo di violazione;

b. se possibile, il momento e la durata;

c. se possibile le categorie e il numero approssimativo dei dati personali interessati;

d. se possibile, le categorie e il numero approssimativo delle persone interessate;

e. le conseguenze, compresi eventuali rischi, per le persone interessate;

f. le misure adottate o previste per eliminare il difetto e ridurne le conseguenze, inclusi gli eventuali rischi;

g. i nomi e i dati di una persona di contatto.

2 Se non è in grado di comunicare contemporaneamente tutte le informazioni, il titolare del trattamento fornisce quanto prima le informazioni mancanti.

3 Se è tenuto a informare la persona interessata, il titolare del trattamento le comunica in una lingua semplice e comprensibile almeno le informazioni di cui al capoverso 1 lettere a ed e–g.

4 Il titolare del trattamento documenta le violazioni. La documentazione illustra i fatti legati agli eventi, le loro conseguenze e i provvedimenti adottati. Deve essere conservata per almeno due anni dalla notifica secondo il capoverso 1.

Capitolo 3: Diritti della persona interessata

Sezione 1: Diritto d'accesso

Art. 16 Modalità

1 Chi domanda informazioni in merito al trattamento dei propri dati personali al titolare del trattamento deve farlo per scritto. Se il titolare del trattamento è d'accordo, la domanda può anche essere presentata in forma orale.

2 Le informazioni sono fornite per scritto o nella forma in cui sono disponibili i dati. D'intesa con il titolare del trattamento, la persona interessata può consultare i suoi dati sul posto. Le informazioni possono essere fornite in forma orale se la persona interessata è d'accordo.

3 Le informazioni possono essere domandate e comunicate per via elettronica.

4 Le informazioni devono essere comunicate in una forma comprensibile per la persona interessata.

5 Il titolare del trattamento adotta misure adeguate per identificare la persona interessata. Quest'ultima ha l'obbligo di collaborare.

Art. 17 Competenza

1 Se più titolari del trattamento trattano congiuntamente dati personali, la persona interessata può esercitare il suo diritto d'accesso presso ciascuno di essi.

2 Se la domanda riguarda dati trattati da un responsabile del trattamento, quest'ultimo aiuta il titolare del trattamento a comunicare le informazioni, a meno che non risponda egli stesso alla domanda per conto del titolare del trattamento.

Art. 18 Termine

1 Le informazioni sono fornite entro 30 giorni dalla ricezione della domanda.

2 Se le informazioni non possono essere fornite entro 30 giorni, il titolare del trattamento ne informa la persona interessata e le comunica il termine entro il quale le informazioni saranno fornite.

3 Se il titolare del trattamento rifiuta, limita o differisce l'informazione, deve comunicarlo entro il suddetto termine.

Art. 19 Eccezioni alla gratuità

1 Se la comunicazione delle informazioni comporta un onere sproporzionato, il titolare del trattamento può richiedere alla persona interessata un'adeguata partecipazione alle spese.

2 La partecipazione ammonta al massimo a 300 franchi.

3 Il titolare del trattamento informa la persona interessata in merito all'entità della partecipazione prima che le siano comunicate le informazioni. Se la persona interessata non conferma la domanda entro dieci giorni, quest'ultima è considerata ritirata senza spese. Il termine di cui all'articolo 18 capoverso 1 decorre dalla fine del periodo di riflessione di dieci giorni.

Sezione 2: Diritto alla consegna o alla trasmissione dei dati

Art. 20 Portata del diritto

1 Per dati personali che la persona interessata ha comunicato al titolare del trattamento si intendono:

a. i dati che la persona ha messo a disposizione del titolare del trattamento consapevolmente e volutamente;

b. i dati che il titolare del trattamento ha rilevato sulla persona interessata e sul suo comportamento nel quadro dell'utilizzo di un servizio o di un apparecchio.

2 I dati personali che il titolare del trattamento ha prodotto in un'analisi separata dei dati personali messi a disposizione o osservati non sono considerati dati personali che la persona interessata ha comunicato al titolare del trattamento.

Art. 21 Requisiti tecnici per l'attuazione

1 Per formato elettronico usuale si intendono i formati che permettono che i dati personali siano trasmessi con un onere proporzionato e riutilizzati dalla persona interessata o da un altro titolare del trattamento.

2 Il diritto alla consegna o alla trasmissione dei dati non obbliga il titolare del trattamento a adottare o conservare sistemi di trattamento dei dati tecnicamente compatibili.

3 L'onere è sproporzionato se la trasmissione di dati personali a un altro titolare del trattamento non è possibile per ragioni tecniche.

Art. 22 Termine, modalità e competenza

Gli articoli 16 capoversi 1 e 5 nonché 17–19 sono applicabili per analogia al diritto alla consegna o alla trasmissione dei dati.

Capitolo 4: Disposizioni particolari sul trattamento di dati da parte di persone private

Art. 23 Consulente per la protezione dei dati

Il titolare del trattamento:

a. mette a disposizione del consulente per la protezione dei dati le risorse necessarie;

b. concede al consulente per la protezione dei dati l'accesso a qualsiasi informazione, documento, registro delle attività di trattamento e dato personale necessario all'adempimento dei suoi compiti;

c. concede al consulente per la protezione dei dati il diritto di informare i massimi organi dirigenti o amministrativi in casi importanti.

Art. 24 Eccezione all'obbligo di tenere un registro delle attività di trattamento

Le imprese e le altre organizzazioni di diritto privato che al 1° gennaio di un anno impiegano meno di 250 collaboratori e le persone fisiche sono esentate dall'obbligo di tenere un registro delle attività di trattamento, salvo che sia adempiuta una delle seguenti condizioni:

a. sono trattati su vasta scala dati personali degni di particolare protezione;

b. viene eseguita una profilazione ad alto rischio.

Capitolo 5: Disposizioni particolari sul trattamento di dati da parte di organi federali

Sezione 1: Consulente per la protezione dei dati

Art. 25 Nomina

Ciascun organo federale nomina un consulente per la protezione dei dati. Più organi federali possono nominare congiuntamente un consulente per la protezione dei dati.

Art. 26 Requisiti e compiti

1 Il consulente per la protezione dei dati:

a. dispone delle conoscenze tecniche necessarie;

b. esercita la sua funzione in modo indipendente dall'organo federale e senza ricevere da questi istruzioni.

2 Ha i seguenti compiti:

a. contribuire all'applicazione delle norme sulla protezione dei dati, in particolare:
   1. verificando il trattamento di dati personali e raccomandando provvedimenti correttivi se si constata una violazione delle prescrizioni in materia di protezione dei dati,
   2. fornendo consulenza al titolare del trattamento nell'allestimento della valutazione d'impatto sulla protezione dei dati e verificandone l'esecuzione;

b. fungere da interlocutore per le persone interessate;

c. formare e fornire consulenza in materia di protezione dei dati ai collaboratori dell'organo federale.

Art. 27 Obblighi dell'organo federale

1 L'organo federale ha i seguenti obblighi nei confronti del consulente per la protezione dei dati:

a. gli concede l'accesso alle informazioni, ai documenti, ai registri delle attività di trattamento e ai dati personali che gli sono necessari all'adempimento dei suoi compiti;

b. provvede affinché sia informato su qualsiasi violazione della sicurezza dei dati.

2 Pubblica i dati di contatto del consulente della protezione dei dati in Internet e li comunica all'IFPDT.

Art. 28 Servizio di contatto dell'IFPDT

Il consulente per la protezione dei dati è il servizio di contatto dell'IFPDT per le questioni riguardanti il trattamento di dati personali da parte dell'organo federale in questione.

Sezione 2: Obbligo di informare

Art. 29 Obbligo di informare in occasione della comunicazione di dati personali

L'organo federale informa il destinatario sull'attualità, l'affidabilità e la completezza dei dati personali comunicati, nella misura in cui tali informazioni non risultino dai dati medesimi o dalle circostanze.

Art. 30 Obbligo di informare in occasione del trattamento automatizzato di dati personali

Se la persona interessata non è obbligata a fornire informazioni, l'organo federale titolare del trattamento che raccoglie sistematicamente dati personali la informa in merito.

Sezione 3: Notifica di progetti di trattamento automatizzato di dati personali all'IFPDT

Art. 31

1 L'organo federale titolare del trattamento notifica all'IFPDT le previste attività di trattamento automatizzato al momento dell'autorizzazione del progetto o della decisione sullo sviluppo del progetto.

2 La notifica contiene le indicazioni di cui all'articolo 12 capoverso 2 lettere a–d LPD e la probabile data di inizio delle attività di trattamento.

3 L'IFPDT inserisce tale notifica nel registro delle attività di trattamento.

4 L'organo federale responsabile del trattamento aggiorna la notifica con il passaggio all'esercizio produttivo o alla sospensione del progetto.

Sezione 4: Sistemi pilota

Art. 32 Carattere imprescindibile del sistema pilota

Un sistema pilota è imprescindibile se è adempiuta una delle seguenti condizioni:

a. l'adempimento di un compito richiede innovazioni tecniche di cui devono dapprima essere valutati gli effetti;

b. l'adempimento di un compito richiede importanti misure organizzative o tecniche la cui efficacia deve dapprima essere esaminata, in particolare in caso di collaborazione tra organi della Confederazione e dei Cantoni;

c. l'adempimento di un compito richiede che i dati personali siano accessibili mediante procedura di richiamo.

Art. 33 Procedura di autorizzazione del sistema pilota

1 Prima di consultare le unità amministrative interessate, l'organo federale competente per il sistema pilota illustra come s'intende garantire il rispetto delle condizioni di cui all'articolo 35 LPD e invita l'IFPDT a presentare un parere.

2 L'IFPDT presenta un parere sul rispetto delle condizioni di autorizzazione di cui all'articolo 35 LPD. A tal fine, l'organo federale gli mette a disposizione tutti i documenti necessari, in particolare:

a. una descrizione generale del sistema pilota;

b. un rapporto attestante che l'adempimento dei compiti legali necessita un trattamento secondo l'articolo 34 capoverso 2 LPD e che una fase sperimentale prima dell'entrata in vigore della legge formale è imprescindibile;

c. una descrizione dell'organizzazione interna e delle procedure di trattamento e di controllo dei dati;

d. una descrizione dei provvedimenti di sicurezza e di protezione dei dati;

e. un progetto di ordinanza che disciplini le modalità di trattamento o le grandi linee di tale atto normativo;

f. la pianificazione delle diverse fasi del sistema pilota.

3 L'IFPDT può esigere altri documenti e procedere a verifiche complementari.

4 L'organo federale informa l'IFPDT di ogni modifica importante che concerne il rispetto delle condizioni di cui all'articolo 35 LPD. Se necessario, l'IFPDT presenta nuovamente un parere.

5 Il parere dell'IFPDT è allegato alla proposta al Consiglio federale.

6 Il trattamento automatizzato dei dati è disciplinato in un'ordinanza.

Art. 34 Rapporto di valutazione

1 L'organo federale competente sottopone per parere all'IFPDT il progetto di rapporto di valutazione destinato al Consiglio federale.

2 Sottopone il rapporto di valutazione al Consiglio federale accompagnato dal parere dell'IFPDT.

Sezione 5: Trattamento di dati per scopi impersonali

Art. 35

Se dati personali sono trattati per scopi impersonali, in particolare per la ricerca, la pianificazione e la statistica, e nel contempo per un altro scopo, le eccezioni di cui all'articolo 39 capoverso 2 LPD sono applicabili soltanto al trattamento per scopi impersonali.

Capitolo 6: Incaricato federale della protezione dei dati e della trasparenza

Art. 36 Sede e segretariato permanente

1 La sede dell'IFPDT è a Berna.

2 Ai rapporti di lavoro degli impiegati del segretariato permanente dell'IFPDT si applica la legislazione sul personale federale. Gli impiegati sono assicurati nell'ambito

della Cassa di previdenza della Confederazione presso la Cassa pensioni della Confederazione.

Art. 37 Canale di comunicazione

1 L'IFPDT comunica con il Consiglio federale per il tramite del cancelliere della Confederazione. Questi trasmette al Consiglio federale proposte, pareri e rapporti senza modificarli.

2 L'IFPDT presenta rapporti all'attenzione dell'Assemblea federale tramite i servizi del Parlamento.

Art. 38 Comunicazione di decisioni, direttive e progetti

1 Nell'ambito della protezione dei dati i dipartimenti e la Cancelleria federale comunicano all'IFPDT le loro decisioni in forma anonimizzata nonché le loro direttive.

2 Gli organi federali presentano all'IFPDT tutti i progetti di atti normativi che riguardano il trattamento di dati personali, la protezione dei dati e l'accesso ai documenti ufficiali.

Art. 39 Trattamento di dati personali

L'IFPT può trattare dati personali compresi i dati particolarmente degni di protezione, in particolare per:

a. esercitare le sue attività di vigilanza;
b. esercitare le sue attività di consulenza;
c. collaborare con autorità federali, cantonali ed estere;
d. adempiere compiti nel quadro delle disposizioni penali secondo la LPD;
e. eseguire procedure di mediazione ed emanare raccomandazioni secondo la legge del 17 dicembre 2004[2] sulla trasparenza (LTras);
f. eseguire valutazioni secondo la LTras;
g. eseguire procedure per l'accesso a documenti ufficiali secondo la LTras;
h. informare la vigilanza parlamentare;
i. informare il pubblico;
j. esercitare le sue attività di formazione.

Art. 40 Autocontrollo

L'IFPDT elabora un regolamento sul trattamento per tutti i trattamenti automatizzati; l'articolo 6 capoverso 1 non è applicabile.

2 RS **152.3**

Art. 41[3] Cooperazione con l'Ufficio federale della cibersicurezza

[1] ...[4]

[2] L'IFPDT invita l'Ufficio federale della cibersicurezza a prendere posizione prima di ordinare a un organo federale di adottare i provvedimenti di cui all'articolo 8 LPD.

Art. 42 Registro delle attività di trattamento degli organi federali

[1] Il registro delle attività di trattamento degli organi federali contiene le indicazioni degli organi federali di cui agli articoli 12 capoversi 2 LPD e 31 capoverso 2 della presente ordinanza.

[2] È pubblicato su Internet. Non sono pubblicate le iscrizioni nel registro sulle previste attività di trattamento automatizzate secondo l'articolo 31.

Art. 43 Codice di condotta

Se gli è presentato un codice di condotta, l'IFPDT comunica nel suo parere se tale codice soddisfa le condizioni dell'articolo 22 capoverso 5 lettere a e b LPD.

Art. 44 Emolumenti

[1] Gli emolumenti fatturati dall'IFPDT sono calcolati in funzione del tempo impiegato.

[2] La tariffa oraria va da 150 a 250 franchi, a seconda della funzione della persona competente.

[3] In caso di prestazioni di portata straordinaria oppure di difficoltà o urgenza particolari possono essere riscossi supplementi fino al 50 per cento dell'emolumento di cui al capoverso 2.

[4] Se la persona soggetta a emolumento può utilizzare la prestazione dell'IFPDT a scopi commerciali, possono essere riscossi supplementi fino al 100 per cento dell'emolumento di cui al capoverso 2.

[5] Per il resto si applica l'ordinanza generale dell'8 settembre 2004[5] sugli emolumenti.

Capitolo 7: Disposizioni finali

Art. 45 Abrogazione e modifica di altri atti normativi

L'abrogazione e la modifica di altri atti normativi sono disciplinati nell'allegato 2.

3 Nuovo testo giusta la cifra II n. 7 dell'O del 22 nov. 2023, in vigore dal 1° gen. 2024 (RU **2023** 746).
4 Abrogato dall'all. n. 2 dell'O del 7 mar. 2025 sulla cibersicurezza, con effetto dal 1° apr. 2025 (RU **2025** 169).
5 RS **172.041.1**

Art. 46 Disposizioni transitorie

[1] Ai trattamenti di dati che non rientrano nel campo d'applicazione della direttiva (UE) 2016/680[6], l'articolo 4 capoverso 2 si applica entro tre anni dall'entrata in vigore della presente ordinanza o al più tardi alla fine del ciclo di vita del sistema. Fino ad allora tali trattamenti sottostanno all'articolo 4 capoverso 1.

[2] L'articolo 8 capoverso 5 non si applica alle valutazioni eseguite prima dell'entrata in vigore della presente ordinanza.

[3] L'articolo 31 non si applica alle previste attività di trattamento automatizzato per le quali all'entrata in vigore della presente ordinanza è già stato autorizzato il progetto o è già stata presa la decisione sullo sviluppo del progetto.

Art. 47 Entrata in vigore

La presente ordinanza entra in vigore il 1° settembre 2023

6 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio GU L 119/89 del 4.5.2016, pag. 89.

Allegato 1[7]
(art. 8 cpv. 1)

Stati, territori, determinati settori di uno Stato e organismi internazionali in cui è garantita una protezione adeguata dei dati

1	Germania*	
2	Andorra***	
3	Argentina***	
4	Austria*	
5	Belgio*	
6	Bulgaria***	
7	Canada***	Un adeguato livello di protezione dei dati è garantito se si applica la legge federale canadese «Loi sur la protection des renseignements personnels et les documents électroniques», del 13 aprile 2000[8] nella sfera privata o una legge sostanzialmente simile di una provincia canadese. La legge federale si applica ai dati personali raccolti, trattati o comunicati nell'ambito di attività commerciali, a prescindere dal fatto che si tratti di organizzazioni quali associazioni, società di persone, singole persone o organizzazioni sindacali oppure di imprese disciplinate dal diritto federale quali installazioni, opere, imprese o attività imprenditoriali che ricadono sotto la competenza legislativa del Parlamento canadese. Le province Québec, British Columbia e Alberta hanno emanato una legge sostanzialmente simile alla legge federale; le province Ontario, New Brunswick, Terranova, Labrador e Nuova Scozia hanno emanato una legge sostanzialmente simile alla legge federale nell'ambito dei dati sanitari. In tutte le province canadesi la legge federale si applica ai dati personali ottenuti, trattati o comunicati alle imprese disciplinate dal diritto federale, compresi i dati sugli impiegati di queste imprese. La legge federale si applica anche ai dati personali trasmessi in un'altra provincia o in un altro Paese nell'ambito di attività commerciali.
8	Cipro***	

[7] Aggiornato dalla cifra I dell'O del 14 ago. 2024, in vigore dal 15 set. 2024 (RU **2024** 435).

[8] Il testo della legge federale canadese è reperibile al seguente indirizzo: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html

9	Croazia***
10	Danimarca*
11	Spagna*
12	Estonia*
13	Finlandia*
14	Francia*
15	Gibilterra***
16	Grecia*
17	Guernsey***
18	Ungheria*
19	Isola di Man***
20	Isole Färöer***
21	Irlanda***
22	Islanda*
23	Israele***
24	Italia*
25	Jersey***
26	Lettonia*
27	Liechtenstein*
28	Lituania*
29	Lussemburgo*
30	Malta*
31	Principato di Monaco***
32	Norvegia*
33	Nuova Zelanda***
34	Paesi Bassi*
35	Polonia*
36	Portogallo*
37	Cechia*
38	Romania***
39	Regno Unito**
40	Slovacchia*
41	Slovenia*

42	Svezia*	
43	Uruguay***	
44	Stati Uniti***	Per i dati personali trattati dalle organizzazioni certificate secondo i principi del quadro per la protezione dei dati tra la Svizzera e gli Stati Uniti[9] è garantito un adeguato livello di protezione in virtù delle garanzie previste dal decreto presidenziale 14086 del 7 ottobre 2022[10], dal regolamento del procuratore generale degli Stati Uniti del 7 ottobre 2022[11] sul Tribunale del riesame in materia di protezione dei dati, dalla direttiva 126 della comunità dell'intelligence (procedure di attuazione del meccanismo di ricorso in materia di intelligence secondo il decreto presidenziale 14086) emanata il 6 dicembre 2022[12] dalla direzione dell'intelligence nazionale, nonché in virtù della designazione della Svizzera il 7 giugno 2024[13] come Stato che beneficia del meccanismo di ricorso a due livelli, compreso l'accesso al Tribunale del riesame in materia di protezione dei dati.

* La valutazione dell'adeguatezza della protezione dei dati include la comunicazione di dati personali secondo la direttiva (UE) 2016/680[14].

** La valutazione dell'adeguatezza della protezione dei dati include la comunicazione di dati personali in base a una decisione di esecuzione della Commissione europea che constata l'adeguatezza della protezione dei dati secondo la direttiva (UE) 2016/680.

*** La valutazione dell'adeguatezza della protezione dei dati non include la comunicazione di dati personali nel quadro della cooperazione prevista dalla direttiva (UE) 2016/680.

9 I principi sono reperibili al seguente indirizzo: www.dataprivacyframework.gov/s/framework-text?tabset-c1491=3.

10 Il decreto presidenziale 14086 è reperibile al seguente indirizzo: www.state.gov/executive-order-14086-policy-and-procedures/.

11 Il regolamento è reperibile al seguente indirizzo: www.federalregister.gov/documents/2022/10/14/2022-22234/data-protection-review-court.

12 La direttiva è reperibile al seguente indirizzo: www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf.

13 La designazione è reperibile al seguente indirizzo: www.justice.gov/opcl/media/1355326/dl?inline.

14 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio GU L 119/89 del 4.5.2016, pag. 89.

Allegato 2[15]
(art. 45)

Abrogazione e modifica di altri atti normativi

I

L'ordinanza del 14 giugno 1993[16] relativa alla legge federale sulla protezione dei dati (OLPD) è abrogata.

II

Gli atti normativi qui appresso sono modificati come segue:

...[17]

15 Aggiornato dall'all. 6 cifra II 1 dell'O del 23 set. 2022 concernente gli esami genetici sull'essere umano, in vigore dal 1° set. 2023 (RU **2022** 585).
16 [RU **1993** 1962; **2000** 1227 all. cifra II n. 7; **2006** 2331 all. 2 n. 3, 4705 cifra II n. 24, **2007** 4993, **2008** 189, **2010** 3399; **2012** 5521]
17 Le mod. possono essere consultate alla RU **2022** 568.