Allegato alle direttive sulle esigenze minime che un sistema di gestione della protezione dei dati deve adempiere (versione del 15.04.2014)

Indice

Codice di pratica per la gestione della protezione dei dati:

Il presente codice di pratica per la gestione della protezione dei dati (CPGPD) è suddiviso in modo logico in base ai 9 principi generali riportati nella legge federale sulla protezione dei dati (LPD; RS 235.1) e concretizzati al punto 5 delle «Direttive sulle esigenze minime che un sistema di gestione della protezione dei dati deve adempiere». Riprende in maniera non esaustiva[1] i requisiti principali della LPD e della relativa ordinanza d'esecuzione (OLPD; RS 235.11). Al fine di agevolare la lettura e la comprensione, ogni misura è strutturata in maniera analoga al «Codice di pratica per la gestione della sicurezza delle informazioni» (ISO/CEI 27002:2013[2] Code of practice for Information Security Management), che a sua volta funge da riferimento per le misure di sicurezza dei dati (principio numero 7). A differenza dell'ISO 27002 che si basa su un'analisi dei rischi, le misure del CPGPD sono formulate in maniera imperativa (deve, esige, è necessario ecc.), poiché sono il frutto di un'analisi di non conformità e derivano direttamente dalla LPD o dall'OLPD.

a. Liceità (art. 4 cpv. 1 LPD)

Obiettivo

Garantire che il *trattamento* dei dati personali sia effettuato in maniera lecita.

a.1 Motivi giustificativi (art. 13 LPD)

Misura

I privati che 'trattano' (art. 3 lett. e LPD) 'dati personali' (art. 3 lett. a LPD) hanno bisogno di motivi giustificativi, cioè del *consenso* della 'persona interessata' (art. 3 lett. b LPD), di un *interesse preponderante* privato o pubblico o di una *legge*.

Attuazione (art. 4 cpv. 5 LPD)

Il *consenso* della 'persona interessata' (art. 3 lett. b LPD) è *valido* solo se questa esprime *liberamente* la propria *volontà,* dopo *debita informazione*. In altre parole, il consenso deve essere accordato senza costrizioni dirette o indirette e in base a informazioni oggettive e pertinenti. In caso di 'dati sensibili' (art. 3 lett. c LPD) o di 'profili della personalità' (art. 3 lett. d LPD), inoltre, il consenso deve essere *esplicito*. Lo è se la 'persona interessata' ha firmato a mano o elettronicamente il documento informativo ricevuto.

All'occorrenza, la plausibilità dell'interesse preponderante privato o pubblico o l'esistenza di una base legale devono poter essere provati. Può trattarsi di una base legale federale (una legge in senso formale, un'ordinanza o altro) o cantonale. Il motivo giustificativo si applica solo ai fini indicati nella legge.

a.2 Base legale (art. 17, 19 e 20 LPD)

Misura

Gli 'organi federali' (art. 3 lett. h LPD) hanno il diritto di trattare i dati personali solo se esiste una *base legale*; il trattamento di dati sensibili e di profili della personalità deve essere sancito in una 'legge in senso formale' (art. 3 lett. j LPD).

Attuazione

---

[1] Gli opuscoli e le guide dell'IFPDT nonché le spiegazioni e le FAQ dell'UFG possono fornire chiarimenti ed informazioni utili per concretizzare gli obiettivi e le misure elencati nel presente codice di pratica.

[2] Introdotto il 15.04.2014.

- L’organo federale responsabile del trattamento dei dati deve poter essere identificato.
- Deve esistere una base legale. Per i dati sensibili o i profili della personalità deve esistere una base legale in senso formale che deve contenere gli elementi necessari, in particolare indicare l’organo responsabile, lo scopo del trattamento, le categorie di dati trattati, di destinatari o partecipanti.
- Se manca una base legale, il trattamento di dati è permesso nelle eccezioni di cui all’art. 17 cpv. 2 lett. a-c o all’art. 19 cpv. 1-2 LPD.
- La consultazione online dei dati personali è permessa solo se esplicitamente prevista. Se si tratta di dati sensibili o di profili della personalità, l'accesso online è permesso solo se una legge in senso formale lo prevede esplicitamente.
- Gli organi federali possono rendere accessibili i dati personali al pubblico per mezzo dei servizi di informazione e di comunicazione automatizzati se una base giuridica ne prevede la pubblicazione o quando gli organi stessi rendono le informazioni accessibili al pubblico ai sensi dell’art. 19 cpv. 1bis LPD.
- In caso di trattamento automatizzato nel quadro di progetti pilota, devono essere rispettate le condizioni di cui all’art. 17*a* LPD.
- È necessario che gli strumenti per opporsi alla ‘comunicazione’ (art. 3 lett. f LPD) dei dati ai sensi dell’art. 20 LPD esistano e possano essere utilizzati.

Altre informazioni (art. 22 LPD)

A determinate condizioni, gli organi federali hanno il diritto di trattare dati personali per scopi impersonali, in particolare nell'ambito di *ricerche, pianificazioni, statistiche*.

a.3 Trattamento dei dati da parte di terzi (art. 10a cpv. 1 LPD)

Misura

Il trattamento di dati può essere *affidato a terzi* purché ciò sia previsto da una *convenzione* o una *legge* e che le condizioni seguenti siano soddisfatte:

- che venga eseguito solo il trattamento al quale ha diritto il mandante stesso;
- che vincoli legali o contrattuali non impongano la segretezza.

Attuazione

- Una convenzione o la legge deve prevedere il trattamento da parte di terzi e devono essere soddisfatte le condizioni di cui all’art. 10*a* LPD.
- Il terzo non ha il permesso di svolgere trattamenti diversi da quelli che il mandante stesso ha il permesso di svolgere, cioè ogni trattamento effettuato da terzi deve essere lecito per il mandante.
- Assicurarsi formalmente che nessuna base legale o contrattuale preveda la segretezza e vieti il trattamento.
- Se necessario, deve poter essere accertata la plausibilità del motivo giustificativo.
- Le misure in A.15.1 “Sicurezza nelle relazioni con i fornitori” dell’allegato A della norma ISO/CEI 27001:2013 (“Esigenze per SMSI”) si applicano a titolo complementare[3].

Altre informazioni[4]

[3] Introdotto il 15.04.2014.

[4] Introdotto il 15.04.2014.

Cf. misura g.4 per la garanzia di sicurezza dei dati nel ambito del trattamento dei dati da parte di terzi.

b. Transparenza

Obiettivo

Garantire che i dati personali siano trattati in condizioni di lealtà e trasparenza, cioè non all'insaputa della persona interessata o per scopi diversi da quelli previsti.

b.1 Buona fede (art. 4 cpv. 2 LPD)

Misura

Garantire che i dati personali siano trattati in maniera conforme al principio della buona fede.

Attuazione

- I dati non devono essere trattati all'insaputa della persona interessata, a meno che una legge non lo preveda esplicitamente (ad esempio, in ambito poliziesco).
- I dati devono essere trattati in un contesto esente da pressioni o elementi atti a trarre in inganno.
- La persona interessata deve essere informata in maniera sufficiente e corretta sul metodo e sullo scopo del trattamento.

b.2 Riconoscibilità (art. 4 cpv. 4 LPD)

Misura

Garantire che la *raccolta* di dati personali, ed in particolare gli scopi del trattamento, siano riconoscibili per la persona interessata.

Attuazione

Le informazioni concrete a disposizione della persona interessata devono essere sufficienti a garantire il riconoscimento della raccolta di dati e gli scopi del trattamento.

b.3 Obbligo di informare (art. 7a cpv. 1 LPD)

Misura

Il 'detentore di una collezione di dati' (art. 3 lett. i LPD) è tenuto ad informare la persona interessata quando raccoglie dati sensibili o profili della personalità che la riguardano, sia se la raccolta è effettuata direttamente presso la persona interessata sia se è effettuata presso terzi.

Attuazione (art. 7*a* cpv. 2-3 LPD)

- Il 'detentore di una collezione di dati' deve comunicare alla 'persona interessata' almeno le seguenti informazioni:
  - la propria identità (detentore di una collezione di dati);
  - gli scopi del trattamento per il quale i dati sono raccolti;
  - le categorie di destinatari se è prevista la comunicazione dei dati.
- Se i dati non sono raccolti presso la persona interessata, il detentore di una collezione di dati deve informarla prima di registrarli o, in mancanza di una registrazione, prima di comunicarli a terzi.

Altre informazioni (art. 7a cpv. 4 LPD)

Il detentore di una collezione di dati è esonerato dall'obbligo di informare se la persona interessata è già stata informata; inoltre non è tenuto a informarla quando i dati non sono raccolti presso di lei se

- la registrazione o la comunicazione sono esplicitamente previsti nella legge;
- l'obbligo di informazione non può essere rispettato o se ciò esige mezzi sproporzionati.

c. Proporzionalità

Obiettivo

Garantire che il trattamento dei dati personali sia proporzionato, cioè *adeguato* allo scopo da raggiungere o al compito da svolgere, *necessario* al progetto e *ragionevole* rispetto al detrimento che rappresenta per la persona interessata.

c.1 Trattamento conforme al principio della proporzionalità (art. 4 cpv. 2 LPD)

Misura

Possono essere trattati solo dati utili ed indispensabili (*evitare o ridurre al minimo* la raccolta) allo svolgimento dei compiti o al raggiungimento dello scopo. I *dati sensibili* devono essere trattati con una cura particolare. I dati personali inutili devono essere distrutti o anonimizzati, a meno che non vi sia l'obbligo di archiviarli o conservarli.

Nel caso in cui non sia necessario conoscere l'identità della persona, i dati devono essere trattati sotto pseudonimo o in modo anonimo.

Attuazione

- I dati vengono trattati in modo *anonimo* quando vengono *eliminati* tutti gli elementi che permettono l'identificazione, in modo cioè di non consentire nessun collegamento o soltanto a prezzo di un dispendio eccessivo[5] a persone identificate o identificabili (in questa forma non sono più sottoposti alla LPD).
- La *pseudonimizzazione* di dati personali consiste nel *sostituire* l'insieme degli elementi che permettono l'identificazione con un elemento identificante neutro denominato *pseudonimo* memorizzato con gli elementi di identificazione in un'apposita tabella delle corrispondenze allegata, la quale permette a chi ne ha il diritto di rintracciare, in caso di necessità, la persona interessata (identificabilità ai sensi della LPD). Grazie a questo metodo, i dati pseudonimizzati possono essere considerati "anonimi" per chi non ha accesso alla tabella delle corrispondenze. Questo procedimento ha senso solo se quest'ultima è *custodita* in modo *esemplare*, è gestita da persone autorizzate e registrate, è memorizzata solo in forma cifrata e in linea di principio permette solo la reidentificazione individuale con la registrazione cronologica di tutte le operazioni di «depseudonimizzazione» svolte.
- Per quel che riguarda i *dati biometrici* raccolti *captando* caratteristiche fisiologiche umane come l'impronta digitale, la mano, il viso, l'iris o l'impronta genetica o caratteristiche comportamentali come la firma, la voce o la battitura, il rapporto tra la finalità del trattamento e il detrimento per le persone interessate deve restare accettabile. La valutazione deve in particolare tener conto del *carattere unico e insostituibile* dei dati biometrici nonché della loro *natura primaria* (dati grezzi) *o secondaria* (dati elaborati, modello). Si preferirà l'uso di caratteristiche biometriche che *non lasciano tracce fisiche* (ad es. il contorno della mano), il ricorso a *dati biometrici secondari* (*modelli biometrici* in genere meno intrusivi dei dati primari

[5] Introdotto il 10.03.2010.

corrispondenti) e, nel quadro di una verifica, la *decentralizzazione* dei dati biometrici (in possesso solo delle persone interessate).

d. Finalità (art. 4 cpv. 3 LPD)

Obiettivo

Garantire che i dati personali siano trattati al solo scopo indicato al momento della raccolta e riportato in una legge o stabilito in base alle circostanze.

d.1 Specificazione/modificazione della finalità (art. 3 lett. i LPD)

Misura

Il 'detentore di una collezione di dati' deve mettere a verbale lo scopo del 'trattamento' in un documento idoneo.

Attuazione

- Lo scopo del trattamento deve essere descritto in un documento specifico, in modo conciso e comprensibile alle persone interessate. Il documento deve essere datato e firmato dal 'detentore della collezione'.
- Ogni successiva modifica dello scopo iniziale deve essere ricostruibile, come anche le operazioni a fine informativo (pubblicazione ufficiale, nuovi consensi ecc.) svolte nei confronti delle persone interessate.

d.2 Limiti all'uso

Misura

Garantire che il 'trattamento' di 'dati personali' non si discosti dallo scopo prefissato.

Ogni trattamento di dati che oltrepassi gli scopi fissati al momento della raccolta costituisce una **modifica indebita** e può essere denunciato e punito.

Attuazione (art. 10 OLPD)

- Il detentore della collezione *registra in un giornale* i trattamenti automatizzati di dati sensibili o di profili della personalità quando le misure preventive non bastano per garantire la protezione dei dati. In particolare la registrazione è necessaria quando senza questa misura *non sarebbe possibile verificare a posteriori che i dati sono stati trattati in maniera conforme alle finalità per cui sono stati raccolti* o comunicati. L'incaricato può raccomandare la registrazione in un giornale per altri trattamenti.
- Gli archivi storici *sono conservati per un anno* nella forma che soddisfa le esigenze della revisione. Sono accessibili solo agli organi o alle persone incaricate di verificare l'applicazione delle disposizioni di protezione dei dati e sono *utilizzati unicamente a tale scopo*.

e. Esattezza dei dati

Obiettivo

Garantire che i 'dati personali' trattati siano e restino esatti.

e.1 Esattezza dei dati (art. 5 cpv. 1 LPD)

Misura

Chi tratta i ‘dati personali’ deve accertarsi che siano corretti e prendere tutte le misure adeguate per cancellare o rettificare i dati inesatti o incompleti nel quadro degli scopi per i quali sono trattati.

Attuazione

- Al momento della raccolta di dati personali, è necessario prendere le misure opportune per *accertare l'identità* della persona interessata e convalidare la *plausibilità* delle informazioni ricevute. Impostazioni adeguate (formati prefissati ecc.) nei formulari permettono di evitare numerosi errori di battitura o di immissione.
- Il dato personale di cui non si può garantire l'esattezza con misure opportune non deve essere raccolto o dovrà essere controllato o distrutto dopo un po' di tempo. Soluzioni crittografiche possono impedire di decifrare i dati dopo la data di scadenza.
- Il detentore di una collezione di dati deve garantire l'aggiornamento dei dati raccolti.

e.2 Rettifica di dati (art. 5 cpv. 2 LPD)

Misura

Chi tratta i dati personali deve garantire la rettifica dei dati non esatti, in particolare quando lo chiede la persona interessata.

Attuazione

Quando fa valere il proprio diritto d'accesso o accede direttamente ai propri dati (in modalità lettura), la persona interessata può scoprire che alcuni dati non esatti sono stati raccolti o sono trattati dal detentore della collezione. Sulla base degli articoli 15 e 25 LPD l’interessato può chiedere di rettificarli o eliminarli e d'interromperne la trasmissione. Quando non è possibile stabilire se i dati sono esatti o meno, il richiedente può domandare che si metta in evidenza l'elemento di incertezza. È compito del detentore della collezione di dati mettere a disposizione strumenti che permettano di rettificare, eliminare o mettere in evidenza i dati, ma anche di interromperne la trasmissione se necessario.

f. Comunicazione di dati all'estero (art. 6 cpv. 1 LPD)

Obiettivo

Nessun ‘dato personale’ può essere comunicato all'estero se la personalità degli interessati può subirne grave pregiudizio, in particolare a causa della mancanza di una base legale che assicuri la protezione adeguata.

f.1 Livello di protezione adeguato (art. 6 cpv. 2 LPD)

Misura

La comunicazione di dati personali non deve rappresentare una grave minaccia per la personalità delle persone interessate. Si presuppone una minaccia di questo tipo quando i destinatari di dati non sottostanno ad una legislazione in grado di garantire una protezione adeguata.

Attuazione (art. 6 cpv. 1 LPD)

Lo Stato destinatario deve essere nominato nell'elenco dei Paesi che dispongono di una legislazione in grado di garantire un livello di protezione dei dati adeguato rispetto al diritto svizzero (pubblicato sul sito www.lincaricato.ch).

In mancanza di una legislazione di questo tipo, deve sussistere una delle seguenti condizioni:

- **garanzie sufficienti**, in particolare contrattuali, che assicurano un livello di protezione adeguato all'estero (art. 6 cpv. 2 lett. a LPD);
- garanzia che le parti sottostanno a **regole sulla protezione dei dati** che assicurano una protezione adeguata, quando la comunicazione ha luogo all'interno della stessa persona giuridica o società oppure tra persone giuridiche o società sottostanti a una direzione unica (art. 6 cpv. 2 lett. g LPD).

In mancanza di una garanzia di tipo appena esposto, deve essere soddisfatta una delle condizioni seguenti:

- la persona interessata ha dato il suo consenso nel caso specifico (art. 6 cpv. 2 lett. b LPD);
- il trattamento è in relazione diretta con la conclusione o l'esecuzione di un contratto e i dati trattati concernono l'altro contraente (art. 6 cpv. 2 lett. c LPD);
- nel caso specifico la comunicazione è indispensabile per tutelare un interesse pubblico preponderante oppure per accertare, esercitare o far valere un diritto in giustizia (art. 6 cpv. 2 lett. d LPD);
- nel caso specifico la comunicazione è necessaria per proteggere la vita o l'incolumità fisica della persona interessata (art. 6 cpv. 2 lett. e LPD);
- la persona interessata ha reso i dati accessibili a chiunque e non si è opposta formalmente al loro trattamento (art. 6 cpv. 2 lett. f LPD);

g. Sicurezza dei dati (art. 7 LPD)

Obiettivo

Garantire che i 'dati personali' sono protetti contro ogni 'trattamento' non autorizzato con misure tecniche e organizzative appropriate.

g.1 Riservatezza dei dati

Misura

Garantire che i 'dati personali' non sono comunicati o rivelati a persone, a enti o in processi non autorizzati.

Attuazione[6] (allegato A d'ISO 27001, che rinvia integralmente all'ISO 27002)

A.6.5.1[nv]	Sicurezza dell'informazione nella gestione di progetto (=>'Privacy by Design')
A.6.2 [nv]	Apparecchi mobili e telelavoro
A.8.x	Gestione dei beni
A.9.x	Controllo degli accessi
A.10.x [nv]	Crittografia
A.11.x[7]	Sicurezza fisica e ambientale
A.12.4	Protocollazione e monitoraggio

[6] Introdotto il 15.04.2014.

[7] Introdotto il 10.03.2010.

A.13.1 Gestione della sicurezza nella rete
A.13.2 Trasferimento delle informazioni

Il controllo A.8.2 verte sulla *classificazione* delle informazioni: il livello di protezione dei dati trattati può essere valutato secondo il grado di sensibilità. La classificazione di protezione dei dati deve distinguere almeno tra il «*livello normale*» e il «*livello elevato*»: il primo per i dati personali il cui uso abusivo potrebbe causare un danno minore alla persona interessata, il secondo per i dati personali sensibili o i profili della personalità il cui uso abusivo potrebbe causare un danno più rilevante alla persona interessata o addirittura metterne in pericolo la vita. È possibile definire livelli intermedi, ma si raccomanda di non prevedere più di quattro livelli di protezione.

g.2 Integrità dei dati

Misura

Garantire l'integralità, la validità e l'attualità dei dati personali.

Attuazione[8]

A.12.2 Protezione contro software dannosi
A.14.x Acquisizione, sviluppo e manutenzione dei sistemi informativi

g.3 Disponibilita dei dati

Misura

Garantire che i 'dati personali' siano accessibili e utilizzabili dietro richiesta da enti autorizzati.

Attuazione[9]

A.12.3 Back-up (delle informazioni)
A.17.x Aspetti della sicurezza dell'informazione nella gestione della continuità operativa
A.18.1.3 Protezione delle registrazioni dell'organizzazione

g.4 Trattamento di dati da parte di terzi (art. 10a cpv. 2 LPD)

Misura

Il mandante deve accertarsi in particolare che il *terzo garantisca la sicurezza dei dati*.

Attuazione

La qualità delle istruzioni fornite al mandatario con il mandato al fine di garantire la sicurezza dei dati deve corrispondere alle esigenze auspicate (cfr. le misure riportate).

Le misure in A.15.2 "Gestione della prestazione di servizi" dell'allegato A d'ISO 27001 si applicano a titolo complementare[10].

Altre informazioni[11]

[8] Introdotto il 15.04.2014.

[9] Introdotto il 15.04.2014.

[10] Introdotto il 15.04.2014.

Cf. misura a.3 per le esigenze legali nel ambito del trattamento dei dati da parte di terzi.

h. Registro delle collezioni di dati (art. 11*a* cpv. 1 LPD e art. 12*b* cpv. 1 OLPD)

Obiettivo

Garantire la trasparenza sull'esistenza delle schede di dati personali al fine di agevolare l'esercizio dei diritti da parte delle persone interessate. A tale scopo l'IFPDT cura un *registro delle schede accessibili online*, che tutti possono consultare. Inoltre questo registro permette all'IFPDT una panoramica di tutte le schede nazionali esistenti e create da poco, facilitando l'attività di controllo.

h.1 Obbligo di dichiarare (art. 11a cpv. 2 e 3 LPD; deroghe art. 11a cpv. 5 lett. e-f LPD)

Misura

Gli organi federali sono tenuti a notificare le loro 'collezioni di dati' (art. 3 lett. g LPD) all'IFPDT, mentre i privati sono tenuti a farlo solo se trattano ad intervalli regolari dati sensibili o profili della personalità oppure se comunicano con regolarità dati personali a terzi.

Le collezioni di dati possono non essere dichiarate quando la *certificazione è stata ottenuta* per l'insieme delle procedure di trattamento che riguardano i dati della collezione da notificare ed il risultato dell'audit è stato comunicato all'IFPDT o ancora quando è stato designato un *responsabile della protezione dei dati che lavora in maniera autonoma*.

Attuazione

L'IFPDT mette a disposizione degli organi federali e dei privati la nuova applicazione WebDatareg che permette di dichiarare e aggiornare online le collezioni in questione. WebDatareg permette inoltre al pubblico di accedere online alle informazioni del *registro delle collezioni notificate* e di rivolgersi alla persona che può fornire informazioni o presso la quale far valere il diritto d'accesso.

h.2 Inventario delle collezioni di dati non notificate (art. 12b cpv. 1 lett. b OLPD)

Misura

Il detentore della collezione di dati esonerato dall'obbligo di notifica deve prendere le misure necessarie per comunicare su richiesta all'incaricato o alle persone interessate le informazioni che riguardano le collezioni che non devono essere notificate.

Attuazione

È necessario prendere le misure necessarie per comunicare su richiesta all'incaricato o alle persone interessate le informazioni che riguardano le collezioni che non devono essere notificate e mantenere aggiornate le collezioni. A tale scopo è necessario allestire e gestire un *inventario delle collezioni non notificate* che contenga le informazioni seguenti:

a. il nome e l'indirizzo del detentore della collezione di dati;

b. il nome e la denominazione completa della collezione di dati;

---

[11] Introdotto il 15.04.2014.

c. la persona presso la quale può essere esercitato il diritto di accesso;
d. lo scopo della collezione di dati;
e. le categorie di dati personali trattati;
f. le categorie di destinatari dei dati;
g. le categorie di partecipanti alla collezione di dati, cioè i terzi che hanno il diritto di trattare e modificare i dati nella collezione.

Altre informazioni (art. 28 cpv. 3 OLPD)

L'IFPDT cura un *elenco dei detentori di collezioni di dati* esonerati dall'obbligo di notifica conformemente all'art. 11*a* cpv. 5 lett. e (nomina di un responsabile indipendente della protezione dei dati) e lett. f (marchio di qualità in virtù di una procedura di certificazione) LPD. L'elenco è consultabile online per informare il pubblico che le collezioni di questi detentori in linea di massima non sono contemplate nel relativo registro dell'IFPDT.

i. Diritto d'accesso e di procedura

Obiettivo

Il detentore di una collezione di dati è tenuto a rispondere a tutti coloro che chiedono se dati che li riguardano sono trattati. In caso di trattamento illecito, la persona interessata può chiedere che i dati vengano corretti, eliminati o bloccati (divieto di comunicazione a terzi).

i.1 Diritto d'accesso ai propri dati (art. 8 cpv. 1 LPD)

Misura

Il detentore di una collezione di dati deve rispondere a chiunque chieda se dati che lo riguardano sono trattati nella collezione.

Attuazione (art. 8 cpv. 2 e 3 art. 9 e 10 LPD)

Il detentore di una collezione di dati deve organizzarla in modo da permettere di esercitare il diritto d'accesso. Deve inoltre mettere a disposizione strumenti di ricerca che permettano di ritrovare tutti i dati trattati che riguardano la persona che fa valere il proprio diritto d'accesso. Il detentore della collezione deve infine essere in grado di presentare le informazioni alla persona interessata.

Il detentore di una collezione deve comunicare tutti i dati contenuti nella collezione che riguardano il richiedente, lo scopo ed eventualmente i fondamenti giuridici del trattamento, le categorie dei dati personali trattati, dei partecipanti alla collezione e dei destinatari dei dati. Può comunicare alla persona interessata i *dati sulla sua salute* per il tramite di un medico da essa designato.

Al fine di accertare che il diritto di accesso sia eseguibile e riproducibile, le applicazioni informatiche devono comprendere (nel menu) una **routine predefinita** che fornisca in modo chiaro tutti i dati relativi alla persona identificata.

Il detentore della collezione di dati deve allestire processi che gli permettono di garantire i diritti delle persone interessate. Il diritto di accesso può essere *rifiutato, limitato o differito* solo nei casi previsti dalla legge. Il detentore della collezione di dati deve indicare il motivo per cui rifiuta di fornire, limita o aggiorna le informazioni.

Se l'accesso viene aggiornato, il detentore della collezione deve allestire un sistema di richiamo. Inoltre deve essere garantita la tracciabilità, in particolare in caso di rifiuto o di limitazioni dell'accesso.

Altre informazioni (art. 10 LPD)

Il detentore di una collezione di dati usata esclusivamente per la diffusione nella parte redazionale di un mezzo di comunicazione sociale con carattere periodico può rifiutare, limitare o differire l'informazione in determinate circostanze.

i.2 Azioni e procedura (art. 15 e 25 LPD)

Misura

Nel quadro della regolamentazione di azioni e procedure, la persona interessata può chiedere al giudice civile (trattamento da parte di privati) o al Tribunale amministrativo federale (trattamento da parte di un organo federale) che i dati vengano *rettificati*, *distrutti* o *bloccati* (divieto di comunicare a terzi). Se non può essere dimostrata né l'esattezza né l'inesattezza dei dati, l'attore può chiedere che si aggiunga ai dati la *menzione che ne rilevi il carattere contestato*.

Attuazione (art. 15/25 cpv. 4 LPD)

È necessario prevedere strumenti e processi per esercitare il diritto di rettifica, di eliminazione, di blocco o di menzione. Inoltre sono necessari strumenti applicabili che permettono di opporsi alla comunicazione dei dati conformemente all'art. 20 LPD (trattamento di dati personali da parte di organi federali).

Altre informazioni

L'introduzione nella legge dell'obbligo di informare (art. 7*a* LPD) ha rafforzato il diritto di chiedere il divieto di trattare i dati.