Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia DFGP

Ufficio federale di giustizia UFG
Divisione principale del diritto pubblico
Divisione Progetti e metodologia legislativi

Avamprogetto di ordinanza sulle procedure di certificazione della protezione dei dati: commento

L'avamprogetto concretizza l'articolo 11 capoverso 2 della modifica del 24 marzo 2006 della legge federale sulla protezione dei dati (LPD*riv*)[1], secondo cui il Consiglio federale emana disposizioni sul riconoscimento delle procedure di certificazione e sull'introduzione di un marchio di qualità inerente alla protezione dei dati. L'avamprogetto riprende il modello di certificazione abbozzato nel messaggio concernente la revisione della LPD (FF *2003* 1885, in particolare pag. 1917 segg.). Sono sottoposti a certificazione l'organizzazione e la procedura della protezione dei dati (sistema di gestione della protezione dei dati; SGPD) nonché i prodotti (programmi e i sistemi). Il requisito fondamentale per gli organismi di certificazione consiste nell'accreditamento, che garantisce il controllo uniforme dei certificatori e permette di ridurre fortemente le necessità normative. L'ordinanza definisce inoltre alcuni requisiti minimi riguardanti gli organismi di certificazione e la procedura di certificazione.

In vista dell'introduzione del marchio di qualità inerente alla protezione dei dati sono state esaminate due opzioni:

- rinuncia a un marchio di qualità ufficiale: i privati (in particolare gli organismi di certificazione) sarebbero liberi di definire i loro marchi di qualità e di concederli in uso agli enti certificati – in genere incassando diritti di licenza. Nell'ordinanza vengono disciplinati unicamente i requisiti di certificazione comuni a tutti i marchi di qualità;
- definizione di un marchio di qualità ufficiale: nell'ordinanza verrebbe definito un marchio di qualità ufficiale a libera disposizione degli enti certificati. Tale opzione non comporta tuttavia la certificazione da parte di un ente statale. Il marchio di qualità ufficiale costituirebbe una specie di «servizio infrastrutturale» accessorio ad eventuali marchi di qualità privati.

In entrambi i casi è inoltre ipotizzabile l'istituzione di un organismo misto. Tale soluzione è però stata esclusa per mancanza di risorse.

La rinuncia a un marchio di qualità ufficiale s'imporrebbe soprattutto per un ragionamento di fondo: introducendo la certificazione della protezione dei dati, s'intende migliorare l'applicazione delle relative leggi nel settore privato. Un marchio privato rispecchierebbe in modo adeguato la parziale «privatizzazione» dei controlli. Un altro vantaggio di questa opzione consiste nella tutela dell'iniziativa privata in materia di marchi di qualità. Permetterebbe inoltre di ridurre la densità normativa dell'ordinanza. Un ipotetico svantaggio consiste nella proliferazione incontrollata di marchi di qualità inerenti alla protezione dei dati a scapito della trasparenza del mercato. Potrebbero inoltre sorgere difficoltà con i detentori di marchi che non adempiono (più) i requisiti legali.

---

[1] Testo sottoposto a referendum: FF **2006** 3291

Il marchio di qualità ufficiale permetterebbe di arginare il proliferare dei «label» e garantirebbe a tutti gli enti certificati l'accesso a un tale contrassegno – vantaggio che la prima opzione non è in grado di assicurare completamente. Un ulteriore punto a favore della seconda opzione consiste nel fatto che la certificazione costa meno poiché né gli enti certificanti né quelli certificati devono pagare diritti di licenza per il marchio di qualità. L'opzione comporta tuttavia due svantaggi rilevanti: l'ingerenza statale in un mercato finora lasciato ai privati e l'aumento della densità normativa dell'ordinanza.

Valutati i vantaggi e gli svantaggi delle due opzioni, la preferenza va alla prima. I vantaggi sono tangibili e pertanto si impongono sugli svantaggi, per i quali permane il dubbio che si manifestino davvero.

1. Requisiti degli organismi di certificazione (art. 1)

I requisiti degli organismi di certificazione risultano in sostanza dalle guide ISO/IEC 62 e 65 (la prima divenuta norma ISO/IEC 17021, la seconda prossimamente sostituita da un'altra norma ISO), la cui applicabilità è disciplinata all'articolo 7 capoverso 1 e nell'allegato 2 dell'ordinanza sull'accreditamento e sulla designazione (OAccD; RS *946.512*). Tali norme specificano in particolare il principio di indipendenza e disciplinano la procedura di certificazione e di esame dei prodotti. Un ulteriore disciplinamento è pertanto superfluo.

Vanno per contro specificati i requisiti di qualifica dei certificatori e del personale addetto agli esami dei prodotti. A tal proposito va ricordato che non esiste una formazione standard nell'ambito della protezione dei dati e che gli esperti sono rari, per cui conviene tener conto dell'esperienza pratica. L'allegato indica i requisiti del caso.

Il capoverso 3 introduce il concetto di programma di controllo, ripreso dall'ordinanza sull'agricoltura biologica (RS *910.18*). Tale programma comprende sia lo schema di esame che indica i requisiti da adempire e i punti in essi contenuti, sia le modalità di svolgimento della procedura di controllo (compresi la sorveglianza e la verifica). Gli enti da certificare di cui alla lettera a possono essere sia organi federali sia organizzazioni private. Anche uno studio medico o legale che tratta regolarmente dati è considerato un ente ai sensi di questa disposizione e può chiedere la certificazione.

I requisiti minimi di cui al capoverso 4 derivano in primo luogo dagli standard internazionali la cui applicabilità è statuita nell'ordinanza sull'accreditamento e sulla designazione. Il rimando agli articoli 4-6 della presente ordinanza esplicita che rientrano nei requisiti minimi anche le pertinenti disposizioni del diritto in materia di protezione dei dati.

2. Coinvolgimento dell'IFPDT nella procedura di accreditamento (art. 2)

La disposizione concretizza l'articolo 11 capoversi 1 e 2 OAccD.

3. Riconoscimento di organismi di certificazione esteri (art. 3)

I requisiti e le procedure internazionali per l'accreditamento nell'ambito della protezione dei dati non sono (ancora) stati uniformati. Il riconoscimento di organismi di certificazione esteri va pertanto disciplinato in questa sede. La disposizione rispecchia l'articolo 29 dell'ordinanza sull'agricoltura biologica.

4. Certificazione di sistemi di gestione della protezione dei dati (art. 4)

4.1 Cenni generali

Il capoverso 1 opera una chiara distinzione tra i vari oggetti di audit o di certificazione.

Il capoverso 2 contiene una descrizione generale dell'oggetto valutato nell'ambito della procedura di audit. Viene definito il contenuto del SGDP, prima tra tutte la politica di protezione dei dati, un documento di base che traccia a grandi linee i principi della protezione dei dati nell'ente in questione e attesta l'impegno assunto in questo ambito; descrive l'impostazione delle misure organizzative finalizzate a garantire il rispetto delle norme legali e di eventuali altre disposizioni applicabili in materia. Tale politica fornisce gli elementi per attuare nel dettaglio le disposizioni in materia di protezione dei dati e di eventuali standard internazionali di «buona pratica» nell'ambito della protezione e della sicurezza dei dati. Sono inoltre oggetto della procedura di audit i provvedimenti adottati dal responsabile del trattamento dei dati per realizzare gli obiettivi e le misure fissate in tale ambito. L'accento è posto sull'istituzione di procedure per porre rimedio ai problemi e alle irregolarità riscontrate.

Il capoverso 4 precisa quanto enunciato all'articolo 11*a* capoverso 5 LPD*riv*, specificando che la deroga all'obbligo di notifica di una collezione di dati è ammessa unicamente se sono stati certificati tutti i trattamenti effettuati nell'ambito della sua finalità e per mezzo dei dati in essa contenuti.

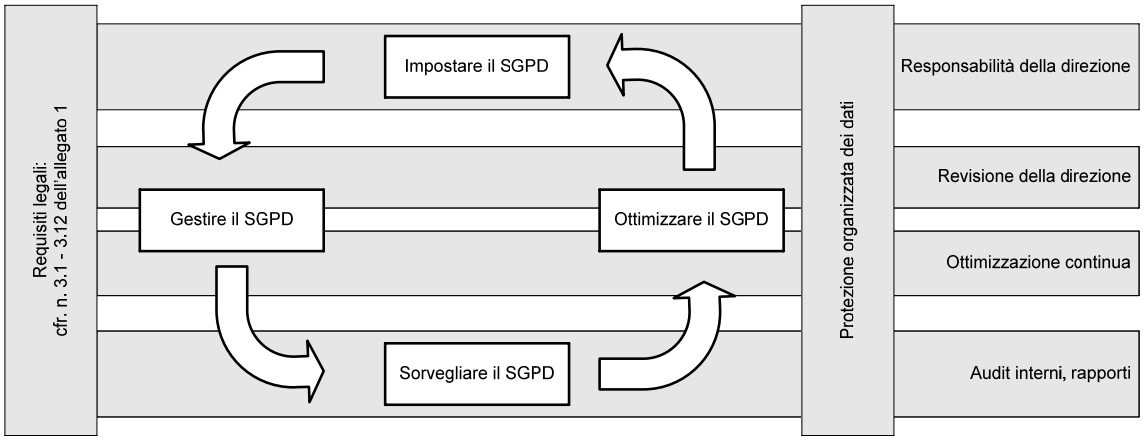
4.2 Requisiti minimi del sistema di gestione della protezione dei dati (SGPD)

4.2.1 Il SGPD come sistema organizzativo

Il capoverso 3 rinvia ai requisiti minimi che il SGPD deve adempire e cita lo standard ISO 27001 per la sicurezza informatica[2]. Evidentemente la protezione dei dati e la sicurezza informatica sono strettamente correlate; inoltre il SGPD funziona allo stesso modo dei sistemi standardizzati impiegati in altri settori. L'integrazione in un sistema esistente (ad es. in un sistema di gestione della qualità) non pone quindi particolari problemi.

Alla stregua di altri sistemi di gestione dello stesso tipo, il SGPD si basa sul modello PDCA (*Plan – Do – Check – Act* = pianificare – attuare – verificare – agire oppure impostare – gestire – sorvegliare – ottimizzare). Lo scopo è la continua ottimizzazione della protezione dei dati nell'ente in questione.

[2] SN ISO/IEC 27001:2005 (ottenibile presso l'Associazione Svizzera di Normalizzazione).



Il SGPD viene impostato e realizzato in conformità ai requisiti legali e segnatamente in funzione della finalità e della portata del trattamento di dati personali, dei mezzi utilizzati a tal fine nonché delle dimensioni e della struttura dell'ente.

Il SGPD relativo a un ente segue un approccio procedurale che ne consente lo sviluppo, la realizzazione, l'attuazione, la sorveglianza, il mantenimento e la continua ottimizzazione. Il modello PDCA va applicato a tutti i processi del SGPD descritti nell'elenco.

Il SGPD è un sistema organizzativo compatibile con altri sistemi organizzativi. Il suo assetto può essere scelto a piacimento. Altri sistemi organizzativi o altri certificati, quali ad esempio la norma ISO 27001:2005, possono fornire elementi determinanti per il SGPD. Ciò non autorizza tuttavia ad applicare la dichiarazione di certificazione al SGPD senza procedere alle verifiche del caso.

4.2.2 Contenuto

Il SGPD è impostato tenendo conto dei criteri definiti per l'applicabilità, la politica di protezione dei dati e il metodo di valutazione dei rischi alla sicurezza dei dati. Occorre identificare i requisiti derivanti dai principi di protezione dei dati (cfr. art. 4 segg. LPD) e da altri fondamenti giuridici, e valutare i rischi alla sicurezza dei dati. In base a tale identificazione/valutazione vanno definite le misure da adottare e approvare da parte della direzione.

Per attuare le misure stabilite vanno previste procedure che permettano di individuare e contrastare senza indugio le situazioni di irregolarità e di identificare e correggere le violazioni della protezione dei dati.

L'efficacia del SGPD va sottoposta a verifica regolare, segnatamente per mezzo di audit interni a intervalli massimi di un anno. Se in tali occasioni si riscontra la necessità di intervenire, occorrerà procedere agli interventi di ottimizzazione del caso (azioni correttive e preventive).

Per il SGPD va allestita una documentazione che illustri la politica di protezione dei dati, definisca l'applicabilità del SGPD e descriva la metodologia per la valutazione dei rischi alla sicurezza dei dati (e i suoi risultati). La documentazione deve inoltre contenere un piano per garantire il rispetto dei requisiti in materia di protezione dei dati e un piano per gestire i rischi alla sicurezza dei dati. Vanno documentate anche le procedure di cui l'ente necessita per garantire l'efficacia nel pianificare, attuare e verificare la politica di protezione dei dati. I documenti vanno approvati dal servizio competente prima di essere emessi; vanno esaminati costantemente e corretti se necessario; le modifiche e lo stato di revisione corrente vanno evidenziati. I servizi competenti e gli addetti ai lavori devono disporre della versione corrente dei documenti di cui necessitano.

Vanno predisposte e gestite registrazioni (*audit log*, ecc.) che dimostrino il buon funzionamento e la conformità ai requisiti del SGPD.

Alla direzione incombono varie responsabilità: deve in particolare sviluppare la politica di protezione dei dati, definire i ruoli e le competenze in materia di protezione dei dati, decidere il livello di rischio accettabile per la sicurezza dei dati e procedere alle ottimizzazioni. Deve inoltre mettere a disposizione le risorse occorrenti per mantenere un'adeguata protezione dei dati attraverso la corretta applicazione di tutte le misure implementate e per potenziare, se necessario, l'efficacia del SGPD. La direzione provvede altresì a un'adeguata sensibilizzazione del personale e a una formazione valida in materia di protezione dei dati. Deve verificare e valutare il SGPD a intervalli massimi di un anno per assicurarne e migliorarne l'adeguatezza e l'efficacia; a tale scopo prende in considerazione tra l'altro i risultati degli audit interni del SGPD, l'esito delle misurazioni dell'efficacia e le modifiche interne ed esterne suscettibili di incidere sul SGPD. Tale revisione della direzione persegue vari obiettivi: aggiornare la valutazione dei rischi e del piano per gestire i rischi alla sicurezza dei dati, modificare le procedure a garanzia della protezione dei dati nel rispetto delle esigenze (se richiesto da eventi interni o esterni), individuare la necessità di risorse e ottimizzare i parametri per valutare l'efficacia delle misure.

5. Certificazione di prodotti (art. 5)

5.1 Cenni generali

Il capoverso 1 definisce i prodotti che possono essere certificati. Una certificazione della protezione dei dati non appare opportuna soltanto per prodotti di per sé finalizzati al trattamento dei dati, ma conviene anche per quelli il cui utilizzo genera dati personali, quali ad esempio i *browser*, i software per la gestione di *server web*, le applicazioni per la gestione di siti Internet o i sistemi logistici basati su tecnologie RFID o GPS.

Il capoverso 2 lettera a si riferisce alle misure tecniche risultanti segnatamente dall'articolo 8 OLPD. Uno standard internazionale in materia è costituito dai «*Common Criteria*» (CC 2.1/ISO 15408) e dai profili di protezione per specifiche categorie di prodotti che definiscono determinati requisiti di sicurezza. I requisiti concreti derivanti da tale disposizione dipendono dallo stato attuale della tecnica.

La lettera b formula il requisito della parsimonia e della non eccedenza dei dati, che concretizza il principio della proporzionalità stabilito dal diritto in materia di protezione dei dati (art. 4 cpv. 2 LPD).

La lettera c si riferisce alla trasparenza delle procedure di trattamento che il prodotto deve garantire. L'utente deve essere in grado di riconoscere i dati personali trattati, le modalità del trattamento e i destinatari delle trasmissioni. I requisiti dipenderanno dalla cerchia di utenti ai quali si indirizza il prodotto; saranno quindi più elevati per un prodotto destinato a un ampio pubblico, e più blandi per un prodotto utilizzato soltanto da specialisti. Vanno verificati i trattamenti automatizzati che un prodotto effettua nell'ambito delle funzionalità per le quali è stato concepito. Se si tratta di un prodotto o sistema aperto, che può essere utilizzato per finalità diverse o configurato in vari modi, occorre verificare che l'utente non possa semplicemente eludere o disattivare i meccanismi tesi a garantire la trasparenza.

5.2 Requisiti minimi per l'esame dei prodotti

Il capoverso 3 stabilisce che l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) emana direttive sui criteri minimi specifici per la protezione dei dati da verificare nell'ambito della certificazione di un prodotto. Contrariamente a quanto

accade per la certificazione dei sistemi di gestione della protezione dei dati, in questo ambito non vi sono standard internazionali riconosciuti che possano essere adeguati con facilità.

È tuttavia ipotizzabile che l'IFPDT basi il proprio schema di valutazione per l'esame dei prodotti sui criteri definiti a tale scopo da un organismo indipendente tedesco, il «*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*»[3]. L'elenco enumera a titolo esemplificativo i requisiti di protezione e di sicurezza dei dati nonché le domande relative alle disposizioni legali rilevanti di cui tener conto a tale proposito e propone una struttura tipo per procedere alla verifica dei requisiti. Una semplice lista di controllo non è sufficiente, poiché il profilo dei requisiti e i tipi di dati variano da un prodotto o sistema informatico all'altro e i periti sono tenuti a documentare sempre le proprie valutazioni.

Le direttive definiscono i requisiti dell'assetto tecnico, compresi in particolare i principi della non eccedenza dei dati e della trasparenza.

L'ammissibilità del trattamento desiderato va verificata in base ai pertinenti principi di protezione dei dati (art. 4 segg. LPD).

Vanno pure individuate le misure tecniche e organizzative previste dal prodotto a tutela degli interessati. Tali misure risultano in primo luogo dagli articoli 8 segg. OLPD. La valutazione deve vertere sugli schemi di attacco su cui poggiano le misure adottate o da adottare, sugli attacchi contro i quali il prodotto o il sistema è protetto, sulle misure aggiuntive supportate (o le eventuali restrizioni) e infine sui rischi residui.

Va inoltre valutata la tutela dei diritti degli interessati (ad es. comunicazione, accesso, trasparenza). Oggi i diritti degli interessati sono spesso garantiti con accorgimenti organizzativi. Per il prodotto o sistema da certificare è determinante se l'impostazione tecnica:

- permette o addirittura incoraggia l'esercizio dei diritti da parte degli interessati; e
- supporta le unità organizzative nel garantire i diritti degli interessati.

In aggiunta vanno considerati gli aspetti legati alla parsimonia dei dati (ad es. operando in forma anonima o pseudonima) e alla registrazione dell'esercizio dei diritti da parte degli interessati.

Da notare infine che uno stesso prodotto permette di trattare e trasferire tra le varie componenti diverse tipologie di dati. A titolo d'esempio citiamo i dati degli interessati (dati primari) quali i dati sanitari personali raccolti da un'assicurazione, e i dati secondari (ad es. *audit trail* riguardanti l'immissione di dati e l'accesso a banche dati, ma anche le modifiche di configurazione o l'accesso a locali sensibili quali il centro di calcolo).

6. Rilascio e validità della certificazione (art. 6)

Il capoverso 1 esplicita che i requisiti posti a un ente o a un prodotto o sistema da certificare risultano dalle disposizioni legali in materia di protezione dei dati e dagli allegati 1 e 2.

Il capoverso 2 fissa a tre anni la validità della certificazione per l'organizzazione e la procedura (SGPD). Statuisce inoltre l'obbligo di riesaminare annualmente le certificazioni rilasciate (cfr. la norma pertinente nella guida ISO/IEC 62, n. 3.6.1). L'organismo di certificazione deve istituire un meccanismo di sorveglianza.

---

[3] *Anforderungskatalog V1.2 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim ULD SH* (http://www.datenschutzzentrum.de/download/anford.pdf).

Lo stesso principio vale anche per la certificazione dei prodotti (cpv. 3): una volta certificati, vanno verificati a intervalli di due anni; se hanno subito modifiche atte a influire sul trattamento dei dati personali, la certificazione va ripetuta senza indugio (guida ISO/IEC 65, n. 13). Nel caso di modifiche di lieve entità è sufficiente una verifica sommaria.

Una volta scaduta la validità, è necessario ripercorrere l'intera procedura per riottenere la certificazione.

7. Riconoscimento di certificazioni estere della protezione dei dati (art. 7)

Pare opportuno prevedere un meccanismo che permetta di riconoscere le certificazioni estere della protezione dei dati. In tal modo, anche gli enti certificati all'estero potrebbero chiedere una deroga all'obbligo di notifica delle loro collezioni di dati. È ad esempio il caso di un'impresa che si sottopone alla certificazione in Germania, ma le cui sedi in Svizzera sono egualmente toccate dalla procedura di certificazione. L'IFPDT deve valutare se i criteri di certificazione corrispondono, sul piano materiale, ai requisiti della legislazione svizzera.

8. Comunicazione dell'esito della procedura di certificazione all'IFPDT (art. 8)

La disposizione cita l'articolo 11*a* capoverso 5 lettera f LPD*riv* ed elenca i documenti da inoltrare all'IFPDT per adempire ai requisiti richiesti. Le informazioni da inserire nel rapporto di valutazione e nei documenti di certificazione sono definite nella guida ISO/IEC 62, n. 3.4 e 3.5. Nei documenti di certificazione figurano l'organismo che ha effettuato la certificazione, il fondamento giuridico della certificazione, i processi o servizi certificati, come pure la validità e la scadenza della certificazione. Il rapporto di valutazione contiene inoltre informazioni particolareggiate sulla conformità del SGPD e i requisiti di certificazione; vanno in particolare specificate le non conformità. Vi possono essere riportati anche dati comparativi di *audit* precedenti, e vanno segnalate eventuali divergenze sorte tra l'organismo di certificazione e l'ente certificato.

A tale proposito va rilevato che se gli accertamenti lo richiedono, l'IFPDT può, nell'ambito della sua attività di sorveglianza secondo gli articoli 27 e 28 LPD, consultare altri documenti relativi alla certificazione, ad es. il rapporto di valutazione.

Dal rimando all'articolo 4 si evince che la deroga all'obbligo di notificare una collezione di dati è ammessa unicamente se ad essere certificato è il SGPD. Non basta infatti che il responsabile del trattamento o il detentore della collezione di dati impieghino prodotti certificati, perché ciò non è sufficiente a garantire il pieno rispetto della normativa in materia di protezione dei dati. La presente disposizione esplicita il contenuto dell'articolo 11*a* capoverso 5 lettera f LPD*riv* in relazione all'articolo 11 capoverso 1 LPD*riv*.

9. Sospensione e revoca della certificazione (art. 9)

L'organismo di certificazione può sospendere o revocare la certificazione della protezione dei dati se, nel corso delle verifiche periodiche o in occasione della ricertificazione, emergono gravi irregolarità. Una grave irregolarità è data in particolare quando vengono infranti requisiti essenziali per la certificazione dei dati. Sarebbe ad esempio il caso se si dovesse constatare a più riprese che non sono adempiti i requisiti della documentazione (cfr. n. 4.2.2) o che non vengono effettuate le valutazioni da parte della direzione (cfr. n. 4.2.2). Costituisce un'altra grave irregolarità l'uso abusivo di una certificazione, ad esempio quando sono stati certificati soltanto singoli trattamen-

ti di dati (art. 4 cpv. 1 lett. b), ma viene comunque utilizzato un marchio di qualità indicante una certificazione completa.

Tale sanzione è altresì prevista nella guida ISO/IEC 62, determinante per l'accreditamento (in futuro ISO/IEC 17021[4]; n. 3.7.3, nota 6). Si tratta quindi di una norma dichiarativa che per motivi di chiarezza andrebbe sancita nell'ordinanza. La sospensione e la revoca non vanno pertanto disciplinate nei particolari in questa sede. Da notare inoltre che la presente disposizione *non* delega ai certificatori la competenza di emanare decisioni. Il capoverso 2 specifica infine che nei casi di controversia sia la procedura sia il giudizio materiale si basano sulle pertinenti disposizioni del diritto contrattuale.

10. Procedura applicabile alle misure di sorveglianza dell'IFPDT (art. 10)

La certificazione della protezione dei dati riguarda in primo luogo i rapporti giuridici tra privati, per principio retti dal diritto privato. Ciò riflette il concetto di autoregolazione: la certificazione si affida ai meccanismi del mercato per ottimizzare l'attuazione del diritto in materia di protezione dei dati.

L'IFPDT non potrà quindi intervenire direttamente in questo rapporto giuridico di diritto privato, ma se riscontra gravi irregolarità mentre svolge i suoi compiti di sorveglianza, deve avere la facoltà di imporre il rispetto delle disposizioni legali. L'articolo 10 descrive la procedura da seguire in questi casi. L'IFPDT non è comunque autorizzato a sospendere o revocare la certificazione.

Se rileva un inadempimento delle condizioni essenziali per la certificazione della protezione dei dati oppure l'utilizzo ingannevole o abusivo della certificazione, l'IFPDT dovrà dapprima rivolgersi all'organismo di certificazione competente, informandolo delle irregolarità riscontrate (cpv. 1). Compete quindi all'organismo di certificazione di intervenire presso l'ente certificato e di provvedere a che vengano adottate le misure necessarie. Se l'ente certificato non pone rimedio alla situazione entro 30 giorni, l'organismo di certificazione sospende la certificazione. La certificazione va revocata se, scaduto anche questo termine, appare improbabile che venga a crearsi o venga ripristinata in tempo utile una situazione conforme alla legge (cpv. 3). Per tempo utile si intende un periodo massimo di tre mesi.

Se i problemi persistano nonostante l'intervento dell'organismo di certificazione e se questo non procede alla sospensione o alla revoca, l'IFPDT deve formulare una raccomandazione secondo l'articolo 27 capoverso 4 o l'articolo 29 capoverso 3 LPD. Può rivolgere la raccomandazione all'ente certificato oppure all'organismo di certificazione, in funzione della loro responsabilità nelle irregolarità. Se indirizza la raccomandazione all'organismo di certificazione, deve informarne il Servizio di accreditamento svizzero in qualità di autorità di sorveglianza. Se la raccomandazione è respinta o non le è dato seguito, l'IFPDT può adire le vie legali[5] deferendo la pratica per decisione al Tribunale amministrativo federale e ricorrendo, se del caso, al Tribunale federale.

Se le irregolarità sono particolarmente gravi (ad es. l'organismo di certificazione è stato indotto con l'inganno a concedere una certificazione o vengono utilizzati certificati falsi), andrebbe accertato se nel caso specifico sussiste una fattispecie penale (truffa, inganno, ecc.).

---

[4] Non è ancora nota la data dell'entrata in vigore.

[5] Nel diritto vigente, il ricorso in giudizio è possibile unicamente per il settore privato (art. 29 cpv. 4 LPD); il testo riveduto prevede tale possibilità anche nell'ambito della sorveglianza sugli organi federali (nuovo art. 27 cpv. 6 LPD).

Va infine rilevato che i concorrenti e i clienti interessati, come pure determinate organizzazioni, in particolare quelle per la protezione dei consumatori, potrebbero proporre azione secondo gli articoli 9 e 10 della legge contro la concorrenza sleale (RS *241*) se vengono utilizzati certificati o marchi di qualità senza che siano adempiti i requisiti legali.

11. Requisiti minimi di qualifica del personale degli organismi di certificazione (Allegato 1)

L'allegato definisce le qualifiche minime di cui deve disporre il personale di un organismo di certificazione che intende certificare la protezione dei dati. Dal momento che sono rari gli specialisti che adempiono a tutti i requisiti, è esplicitamente ammesso affidare gli audit e l'esame dei prodotti a una squadra interdisciplinare i cui membri presentano, insieme, i requisiti richiesti.