Ordinanza sulle certificazioni in materia di protezione dei dati
(OCPD)

del 31 agosto 2022

Il Consiglio federale svizzero,

visto l'articolo 13 capoverso 2 della legge federale del 25 settembre 2020[1] sulla protezione dei dati (LPD),

ordina:

Sezione 1: Organismi di certificazione

Art. 1 Requisiti

[1] Gli organismi che effettuano certificazioni in materia di protezione dei dati secondo l'articolo 13 LPD (organismi di certificazione) devono essere accreditati. L'accreditamento è retto dall'ordinanza del 17 giugno 1996[2] sull'accreditamento e sulla designazione (OAccD), per quanto la presente ordinanza non disponga altrimenti.

[2] Sono necessari due accreditamenti distinti per certificare:

a. l'organizzazione e la procedura (sistemi di gestione) relative al trattamento dei dati;

b. i prodotti, segnatamente i sistemi e i programmi di trattamento di dati e l'hardware, nonché i servizi e i processi relativi al trattamento dei dati.

[3] Gli organismi di certificazione devono disporre di un'organizzazione e di una procedura di certificazione ben definite (programma di certificazione).

[4] I requisiti minimi concernenti la qualifica del personale addetto alla certificazione sono disciplinati nell'allegato. Gli organismi di certificazione devono dimostrare di impiegare personale qualificato secondo questi criteri.

Art. 2 Procedura di accreditamento

Il Servizio d'accreditamento svizzero (SAS) consulta l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) in merito alla procedura di accreditamento e ai controlli nonché alla sospensione e alla revoca dell'accreditamento.

RS **235.13**

1 RS **235.1**

2 RS **946.512**

Art. 3 Organismi di certificazione esteri

1 Gli organismi di certificazione esteri che desiderano esercitare l'attività sul territorio svizzero devono dimostrare di possedere una qualifica equivalente a quella richiesta in Svizzera, di adempiere i requisiti di cui all'articolo 1 capoversi 3 e 4 e di conoscere sufficientemente la legislazione svizzera sulla protezione dei dati.

2 L'IFPDT riconosce un organismo di certificazione straniero dopo aver consultato il SAS.

3 Può rilasciare riconoscimenti limitati nel tempo e vincolarli a oneri.

4 Revoca il riconoscimento se non sono più adempiti condizioni od oneri.

Sezione 2: Oggetto e procedura di certificazione

Art. 4 Oggetto della certificazione

1 È possibile certificare:

a. i sistemi di gestione;

b. i prodotti, i servizi e i processi.

2 La certificazione dei sistemi di gestione può riguardare l'intero sistema, una parte dell'organizzazione o procedure specifiche.

3 La certificazione dei prodotti, dei servizi e dei processi può riguardare:

a. i prodotti destinati in prevalenza al trattamento di dati personali o generanti, al momento del loro impiego, dati personali;

b. i servizi o i processi destinati in prevalenza al trattamento di dati personali o generanti dati personali;

Art. 5 Requisiti per il programma di certificazione

1 Il programma di certificazione deve disciplinare almeno:

a. i criteri di perizia come pure i requisiti che ne conseguono per gli oggetti da certificare;

b. le modalità di svolgimento della procedura, in particolare le misure applicabili in caso di irregolarità.

2 Nell'elaborare il programma di certificazione occorre tenere conto dei seguenti punti:

a. i dati personali trattati;

b. le infrastrutture elettroniche utilizzate per il trattamento dei dati personali;

c. le misure organizzative relative al trattamento dei dati personali.

3 I criteri di perizia devono rispettare tutti i principi dell'articolo 6 LPD.

4 Il programma di certificazione deve essere conforme alle norme applicabili secondo l'allegato 2 dell'OAccD[3], nonché alle altre norme tecniche applicabili.

Art. 6 Requisiti per la certificazione dei sistemi di gestione

1 La perizia del sistema di gestione riguarda:

a. la politica di protezione dei dati;

b. la documentazione degli obiettivi, dei rischi e delle misure atte a garantire la protezione dei dati e la sicurezza dei dati;

c. i provvedimenti organizzativi e tecnici finalizzati a realizzare gli obiettivi e le misure fissate, in particolare i provvedimenti tesi a eliminare le lacune riscontrate.

2 L'IFPDT emana direttive sui requisiti minimi che un sistema di gestione deve adempiere. Tiene conto dei requisiti internazionali in materia di installazione, gestione, sorveglianza e ottimizzazione di tali sistemi di gestione e in particolare delle seguenti norme tecniche[4]:

a. UNI EN ISO 9001: Sistemi di gestione per la qualità – Requisiti;

b. UNI CEI EN ISO/IEC 27001, Tecnologie Informatiche – Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione – Requisiti;

c. UNI CEI EN ISO/IEC 27701, Tecniche di sicurezza – Estensione a ISO/IEC 27001 e ISO/IEC 27002 per la gestione delle informazioni in ambito privacy – Requisiti e linee guida.

Art. 7 Requisiti per la certificazione di prodotti, servizi e processi

1 La perizia di prodotti, servizi e processi deve permettere di verificare che siano garantiti in particolare i seguenti principi:

a. la riservatezza, l'integrità, la disponibilità e la tracciabilità dei dati personali trattati;

b. la rinuncia a trattare dati personali, per quanto lo scopo d'impiego del prodotto, del servizio o del processo non lo richieda;

c. la trasparenza del trattamento di dati personali;

d. le misure tecniche indispensabili che permettono all'utente di rispettare altri principi o obblighi in materia di protezione dei dati, segnatamente i diritti delle persone interessate.

2 L'IFPDT emana direttive sui altri criteri in materia di protezione dei dati di cui tenere conto nell'ambito della perizia.

3 RS **946.512**

4 Le norme menzionate possono essere consultate gratuitamente od ottenute a pagamento presso l'Associazione svizzera di normalizzazione (SNV), Sulzerallee 70, 8404 Winterthur; www.snv.ch.

Art. 8 Rilascio e validità della certificazione

1 L'organismo di certificazione certifica il sistema di gestione, il prodotto, il servizio o il processo se sono soddisfatti i requisiti legali in materia di protezione dei dati e gli altri requisiti derivanti dalla presente ordinanza e dalle direttive dell'IFPDT o da qualsiasi altra norma equivalente. La certificazione può essere vincolata a oneri.

2 La certificazione è valida per tre anni. L'organismo di certificazione verifica ogni anno se le condizioni determinanti per la certificazione continuano a essere adempite.

Art. 9 Riconoscimento di certificazioni estere

Dopo aver consultato il SAS, l'IFPDT riconosce le certificazioni estere purché l'adempimento dei requisiti della legislazione svizzera sia garantito.

Art. 10 Esenzione dall'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati

Il titolare privato del trattamento può rinunciare a una valutazione d'impatto sulla protezione dei dati conformemente all'articolo 22 capoverso 5 LPD soltanto se la certificazione include il trattamento per il quale dovrebbe essere effettuata la valutazione d'impatto.

Sezione 3: Sanzioni

Art. 11 Sospensione e revoca della certificazione

1 L'organismo di certificazione può sospendere o revocare una certificazione accordata, in particolare se nell'ambito della verifica constata gravi lacune. Si è in presenza di una grave lacuna in particolare se:

a. le condizioni essenziali della certificazione dei dati non sono più adempiute; o

b. una certificazione è utilizzata in modo ingannevole o abusivo.

2 Nei casi di controversia in merito alla sospensione o alla revoca, il giudizio e la procedura sono retti dalle disposizioni di diritto civile applicabili al rapporto contrattuale tra l'organismo di certificazione e il fornitore di programmi o sistemi di trattamento dei dati personali, il titolare del trattamento o il responsabile del trattamento certificati.

Art. 12 Misure di sorveglianza dell'IFPDT: procedura

1 L'IFPDT informa l'organismo di certificazione se constata gravi lacune presso un fornitore di programmi o sistemi di trattamento di dati personali, un titolare del trattamento o un responsabile del trattamento certificati.

2 L'organismo di certificazione invita senza indugio il fornitore di programmi o sistemi di trattamento di dati personali, il titolare del trattamento o il responsabile del

trattamento certificati a eliminare la lacuna riscontrata entro 30 giorni dalla ricezione della comunicazione dell'IFPDT.

3 Se la lacuna non è eliminata entro 30 giorni, l'organismo di certificazione sospende la certificazione. La certificazione va revocata se appare improbabile che venga a crearsi o venga ripristinata una situazione conforme al diritto entro un periodo di tempo ragionevole.

4 Se la lacuna non è eliminata entro il termine previsto dal capoverso 2 e l'organismo di certificazione non ha sospeso o revocato la certificazione, l'IFPDT ordina una misura ai sensi dell'articolo 51 capoverso 1 LPD. Segnatamente, può ordinare la sospensione o la revoca della certificazione. Se indirizza l'ordine all'organismo di certificazione, ne informa il SAS.

Sezione 4: Disposizioni finali

Art. 13 Abrogazione di un altro atto normativo

L'ordinanza del 28 settembre 2007[5] sulle certificazioni in materia di protezione dei dati è abrogata.

Art. 14 Entrata in vigore

La presente ordinanza entra in vigore il 1° settembre 2023.

In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Ignazio Cassis
Il cancelliere della Confederazione, Walter Thurnherr

5 RU **2007** 5003, **2010** 949, **2016** 3447.

Allegato
(art. 1 cpv. 5)

Requisiti minimi concernenti la qualifica del personale

1 Certificazione dei sistemi di gestione

Il personale addetto alla certificazione dei sistemi di gestione dispone complessivamente delle seguenti qualifiche:

– conoscenze in materia di diritto della protezione dei dati: esperienza pratica di almeno due anni nel settore della protezione dei dati oppure una formazione completa di almeno un anno, con approfondimento nel diritto sulla protezione dei dati, presso una scuola universitaria o una scuola universitaria professionale;

– conoscenze in materia di sicurezza dell'informazione: esperienza pratica di almeno due anni nel settore della sicurezza dell'informazione oppure una formazione completa di almeno un anno, con approfondimento in sicurezza dell'informazione, presso una scuola universitaria o una scuola universitaria professionale;

– conoscenze degli sviluppi nel settore della protezione dei dati e in materia di sicurezza dell'informazione;

– formazione come certificatore di sistemi di gestione che soddisfa i requisiti determinanti a livello internazionale, così come figurano in particolare nelle norme seguenti[6]:

  - UNI CEI EN ISO/IEC 17021-1, Valutazione della conformità – Requisiti per gli organismi che forniscono audit e certificazione di sistemi di gestione – Parte 1: Requisiti,
  - UNI CEI EN ISO/IEC 17021-3, Valutazione della conformità – Requisiti per gli organismi che forniscono audit e certificazione di sistemi di gestione – Parte 3: Requisiti di competenza per le attività di audit e la certificazione di sistemi di gestione per la qualità, e
  - UNI CEI EN ISO/IEC 27006, Tecnologie informatiche – Tecniche di sicurezza – Requisiti per gli enti che forniscono servizi di audit e certificazione dei sistemi di gestione per la sicurezza delle informazioni.

L'organismo di certificazione deve disporre di personale qualificato per i singoli settori. La perizia dei sistemi di gestione della protezione dei dati da parte di un gruppo interdisciplinare è autorizzata.

6 Le norme menzionate possono essere consultate gratuitamente od ottenute a pagamento presso l'Associazione svizzera di normalizzazione (SNV), Sulzerallee 70, 8404 Winterthur; www.snv.ch.

2 Certificazione di prodotti, servizi e processi

Il personale addetto alla certificazione di prodotti, servizi o processi dispone complessivamente delle seguenti qualifiche:

– conoscenze in materia di diritto della protezione dei dati: esperienza pratica di almeno due anni nel settore della protezione dei dati oppure una formazione completa di almeno un anno, con approfondimento nel diritto sulla protezione dei dati, presso una scuola universitaria o una scuola universitaria professionale;

– conoscenze in materia di sicurezza dell'informazione: esperienza pratica di almeno due anni nel settore della sicurezza dell'informazione oppure una formazione completa di almeno un anno, con approfondimento in sicurezza dell'informazione, presso una scuola universitaria o una scuola universitaria professionale;

– conoscenze degli sviluppi nel settore della protezione dei dati e in materia di sicurezza dell'informazione;

– conoscenze specifiche in materia di certificazione di prodotti, servizi o processi che soddisfano i requisiti del programma di certificazione e le direttive emesse dall'IFPDT nonché i requisiti determinanti a livello internazionale, così come figurano in particolare nelle norme tecniche applicabili e nella norma «UNI CEI EN ISO//IEC 17065[7]: Valutazione della conformità – Requisiti per organismi che certificano prodotti, processi e servizi».

L'organismo di certificazione deve disporre di personale qualificato per i singoli settori. La perizia dei prodotti, servizi e processi da parte di un gruppo interdisciplinare è autorizzata.

7 La norma menzionata può essere consultata gratuitamente od ottenuta a pagamento presso l'Associazione svizzera di normalizzazione (SNV), Sulzerallee 70, 8404 Winterthur; www.snv.ch.