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

del 28 settembre 2007 (Stato 1° gennaio 2008)

*Il Consiglio federale svizzero,*

visto l'articolo 11 capoverso 2 della legge federale del 19 giugno 1992[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 11 LPD (organismi di certificazione) devono essere accreditati. L'accreditamento è retto dall'ordinanza del 17 giugno 1996[2] sull'accreditamento e sulla designazione, per quanto la presente ordinanza non disponga altrimenti.

2 Sono necessari due accreditamenti distinti per certificare:

a. l'organizzazione e le procedure della protezione dei dati;

b. i prodotti (hardware, software o sistemi per le procedure automatizzate di trattamento di dati).

3 Gli organismi di certificazione devono disporre di un'organizzazione e di una procedura di certificazione ben definite (programma di controllo). Vi sono disciplinati in particolare:

a. i criteri di perizia o di prova, come pure i requisiti che ne conseguono per gli organismi o i prodotti da certificare (schema di perizia e di prova); e

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

4 I requisiti minimi del programma di controllo sono retti dalle norme e dai principi applicabili conformemente all'allegato 2 dell'ordinanza del 17 giugno 1996 sull'accreditamento e sulla designazione e dagli articoli 4–6.

5 I requisiti minimi concernenti la qualifica del personale addetto alla certificazione sono disciplinati nell'allegato.

RU **2007** 5003

1 RS **235.1**

2 RS **946.512**

**Art. 2** Procedura di accreditamento

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

**Art. 3** Organismi di certificazione esteri

1 Previa consultazione del Servizio d'accreditamento svizzero, l'Incaricato ammette gli organismi di certificazione esteri all'esercizio dell'attività sul territorio svizzero, se gli stessi possono dimostrare di possedere una qualifica equivalente a quella richiesta in Svizzera.

2 Gli organismi di certificazione devono in particolare provare che adempiono i requisiti di cui all'articolo 1 capoversi 3 e 4 e che conoscono sufficientemente la legislazione svizzera sulla protezione dei dati.

3 L'Incaricato può rilasciare riconoscimenti limitati nel tempo o vincolarli a condizioni od oneri. Revoca il riconoscimento se non sono adempiti condizioni od oneri essenziali.

## Sezione 2: Oggetto e procedura

**Art. 4** Certificazione dell'organizzazione e della procedura

1 È possibile certificare:

a. l'insieme delle procedure di trattamento dei dati di cui un organismo è responsabile;

b. singole procedure di trattamento specifiche.

2 La perizia riguarda il sistema di gestione della protezione dei dati. Tale sistema comprende segnatamente:

a. la politica di protezione dei dati;

b. la documentazione degli obiettivi 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.

3 L'Incaricato emana direttive sui requisiti minimi che un sistema di gestione della protezione dei dati deve adempiere. Tiene conto delle norme e degli standard internazionali in materia di installazione, gestione, sorveglianza e ottimizzazione dei sistemi di gestione, segnatamente le norme ISO 9001:2000 e ISO 27001:2005.

4 La deroga all'obbligo di notifica delle collezioni di dati secondo l'articolo 11*a* capoverso 5 lettera f LPD si applica soltanto a condizione che siano state certificate tutte le procedure di trattamento dei dati cui è destinata una collezione di dati.

**Art. 5** Certificazione di prodotti

1 Possono essere certificati i prodotti destinati in prevalenza al trattamento di dati personali o generanti, al momento del loro impiego, dati personali, in particolare relativi all'utente.

2 Si esamina segnatamente se il prodotto stesso garantisce:

a. la riservatezza, l'integrità, la disponibilità e l'autenticità dei dati personali trattati, in considerazione dello scopo di impiego del prodotto;

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

c. la trasparenza e la riproducibilità dei trattamenti automatizzati di dati personali nell'ambito delle funzionalità stabilite dal fabbricante di un prodotto;

d. le misure tecniche indispensabili che permettono all'utente di rispettare altri principi o obblighi in materia di protezione dei dati.

3 L'Incaricato emana, entro il 1° gennaio 2010, direttive sui criteri specifici in materia di protezione dei dati da esaminare nell'ambito della certificazione di un prodotto.

**Art. 6** Rilascio e validità della certificazione

1 La certificazione è rilasciata se dalla procedura risulta che, in base ai criteri applicati dall'organismo di certificazione per la perizia o la prova dei prodotti, sono soddisfatti i requisiti legali in materia di protezione dei dati e gli altri requisiti derivanti dalla presente ordinanza e dalle direttive dell'Incaricato (art. 4 cpv. 3 e art. 5 cpv. 3). La certificazione può essere vincolata a condizioni od oneri.

2 La certificazione di un sistema di gestione della protezione dei dati è valida tre anni. L'organismo di certificazione verifica ogni anno, in via sommaria, se le condizioni determinanti per la certificazione continuano a essere adempite.

3 La certificazione di un prodotto è valida per due anni. Un prodotto che subisce modifiche essenziali deve essere nuovamente certificato.

**Art. 7** Riconoscimento di certificazioni estere

Dopo aver consultato il Servizio d'accreditamento svizzero, l'Incaricato riconosce le certificazioni estere purché l'adempimento dei requisiti della legislazione svizzera sia garantito.

**Art. 8** Comunicazione dell'esito della procedura di certificazione

1 L'organismo certificato che comunica all'Incaricato l'esito positivo della certificazione secondo l'articolo 4, per essere esonerato dall'obbligo di notifica della collezione di dati secondo l'articolo 11*a* capoverso 5 lettera f LPD, deve presentare su richiesta i seguenti documenti:

a. rapporto di valutazione;

b. documenti di certificazione.

2 Se svolgendo la propria attività di sorveglianza l'organismo di certificazione riscontra mutamenti sostanziali delle condizioni di certificazione, in particolare per quanto riguarda l'adempimento di condizioni od oneri, l'organismo certificato ne informa l'Incaricato.

3 L'Incaricato pubblica un elenco degli organismi certificati esonerati dall'obbligo di notificare le loro collezioni di dati (art. 28 cpv. 3 dell'O del 14 giu. 1993[3] relativa alla legge federale sulla protezione dei dati). Tale documento indica segnatamente la durata di validità della certificazione.

## Sezione 3: Sanzioni

**Art. 9** Sospensione e revoca della certificazione

1 L'organismo di certificazione può sospendere o revocare una certificazione accordata, segnatamente se nell'ambito della verifica (art. 6 cpv. 2) 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 l'organismo certificato.

3 Se la certificazione di cui all'articolo 8 capoverso 1 era stata comunicata all'Incaricato, l'organismo di certificazione gli comunica la sospensione o la revoca.

**Art. 10** Misure di sorveglianza dell'Incaricato: procedura

1 Se svolgendo la propria attività di sorveglianza secondo gli articoli 27 o 29 LPD constata gravi lacune presso l'organismo certificato, l'Incaricato ne informa l'organismo di certificazione.

2 L'organismo di certificazione invita senza indugio l'organismo certificato a eliminare le lacune riscontrate entro 30 giorni dalla ricezione della comunicazione dell'Incaricato.

3 Se l'organismo certificato non elimina le lacune entro tale termine, 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 l'organismo certificato non ha eliminato le lacune entro il termine previsto dal capoverso 2 e l'organismo di certificazione non ha sospeso o revocato la certificazione, l'Incaricato formula una raccomandazione secondo l'articolo 27 capoverso 4 o l'articolo 29 capoverso 3 LPD all'indirizzo dell'organismo certificato o dell'orga-

3 RS **235.11**

nismo di certificazione. Può segnatamente raccomandare all'organismo di certificazione di sospendere o revocare la certificazione. Se indirizza la raccomandazione all'organismo di certificazione, ne informa il Servizio d'accreditamento svizzero.

## Sezione 4: Entrata in vigore

### Art. 11

La presente ordinanza entra in vigore il 1° gennaio 2008.

*Allegato*
(art. 1 cpv. 5)

# Requisiti concernenti la qualifica del personale degli organismi di certificazione addetto alla certificazione

## 1 Certificazione dei sistemi di gestione della protezione dei dati

L'organismo di certificazione deve provare che il personale addetto alla certificazione dei sistemi di gestione della protezione dei dati dispone complessivamente delle seguenti qualifiche:

- conoscenza del diritto in materia di protezione dei dati: dev'essere comprovata un'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 informatica: dev'essere comprovata un'esperienza pratica di almeno due anni nel settore della sicurezza informatica oppure una formazione completa di almeno un anno, con approfondimento in sicurezza informatica, presso una scuola universitaria o una scuola universitaria professionale;
- formazione come certificatore di sistemi di gestione (secondo la norma ISO/IEC 62 [ISO/IEC 17021:2006]).

L'organismo di certificazione deve provare di 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.

## 2 Certificazione di prodotti

L'organismo di certificazione deve provare che il personale addetto alla certificazione di prodotti dispone complessivamente delle seguenti qualifiche:

- conoscenza del diritto in materia di protezione dei dati: dev'essere comprovata un'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 informatica: dev'essere comprovata un'esperienza pratica di almeno due anni nel settore della sicurezza informatica oppure una formazione completa di almeno un anno, con approfondimento in sicurezza informatica, presso una scuola universitaria o una scuola universitaria professionale;

– conoscenze specifiche in materia di prova dei prodotti (secondo la norma ISO/IEC 65).

L'organismo di certificazione deve provare di 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.