

# **Ordinanza sulle procedure di certificazione della protezione dei dati (OCPD)**

del 28 settembre 2007

---

*Il Consiglio federale svizzero,*

visto l'articolo 11 capoverso 2 della legge federale del 19 giugno 1992<sup>1</sup> sulla protezione dei dati (LPD),

*decreta:*

## **Sezione 1: Organismi di certificazione**

### **Art. 1**          Requisiti

<sup>1</sup> Gli organismi che effettuano procedure di certificazione della protezione dei dati secondo l'articolo 11 LPD (organismi di certificazione) devono essere accreditati per la loro attività. L'accREDITAMENTO degli organismi di certificazione è retto dall'ordinanza del 17 giugno 1996<sup>2</sup> sull'accREDITAMENTO e sulla designazione, per quanto la presente ordinanza non disponga altrimenti.

<sup>2</sup> Sono necessari due accREDITAMENTI distinti per certificare:

- a. l'organizzazione e le procedure della protezione dei dati;
- b. i prodotti (hardware e software o sistemi per le procedure di trattamento di dati automatizzati).

<sup>3</sup> 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 valutazione o di esame, come pure i requisiti che ne conseguono per gli enti o i prodotti da certificare (schema di valutazione e di esame); e
- b. lo svolgimento della procedura, in particolare un'adeguata strategia d'approccio in caso di irregolarità.

<sup>4</sup> I requisiti minimi del programma di controllo sono disciplinati agli articoli 4-6 e dalle norme e dai principi applicabili secondo l'allegato 2 dell'ordinanza del 17 giugno 1996 sull'accREDITAMENTO e sulla designazione.

RU **1993** 1962

<sup>1</sup> RS **235.1**

<sup>2</sup> RS **946.512**

<sup>5</sup> I requisiti minimi di qualifica del personale addetto alla certificazione sono disciplinati nell'allegato.

#### **Art. 2** Procedura di accreditamento

Il Servizio di 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

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

<sup>2</sup> Gli organismi di certificazione devono in particolare dimostrare di soddisfare i requisiti di cui all'articolo 1 capoversi 3 e 4 e di conoscere a sufficienza la legislazione svizzera in materia di protezione dei dati.

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

### **Sezione 2: Oggetto e procedura**

#### **Art. 4** Certificazione dell'organizzazione e delle procedure

<sup>1</sup> È possibile certificare:

- a. l'insieme delle procedure di trattamento dei dati di cui è responsabile un ente;
- b. singole procedure di trattamento specifiche.

<sup>2</sup> Viene valutato 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 rimediare alle irregolarità riscontrate.

<sup>3</sup> 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 impostazione, gestione, sorveglianza e ottimizzazione dei sistemi di gestione, segnatamente per quanto riguarda la sicurezza delle informazioni (standard ISO 9001:2000; ISO 27001:2005).

<sup>4</sup> La deroga all'obbligo di notifica secondo l'articolo 11a 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

<sup>1</sup> 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.

<sup>2</sup> Viene segnatamente verificato che il prodotto garantisca:

- a. le misure tecniche indispensabili allo scopo d'utilizzo del prodotto finalizzate ad assicurare la riservatezza, l'integrità, la disponibilità e l'autenticità dei dati personali trattati;
- b. la rinuncia a generare, memorizzare o altrimenti trattare dati personali, per quanto lo scopo d'utilizzo del prodotto non lo richieda;
- c. la trasparenza e la riproducibilità dei trattamenti automatizzati dei 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.

<sup>3</sup> L'Incaricato emana direttive sui criteri minimi specifici per la protezione dei dati da verificare nell'ambito della certificazione di un prodotto.

#### **Art. 6**                   Rilascio e validità della certificazione della protezione dei dati

<sup>1</sup> La certificazione è rilasciata se dalla procedura risulta che, in base ai criteri applicati dall'organismo di certificazione per la valutazione o l'esame 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 oneri o condizioni.

<sup>2</sup> 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.

<sup>3</sup> La certificazione di un prodotto è valida due anni. Un prodotto che subisce modifiche essenziali deve essere certificato di nuovo.

#### **Art. 7**                   Riconoscimento di certificazioni estere della protezione dei dati

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

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

<sup>1</sup> L'ente certificato che comunica all'Incaricato l'esito positivo della certificazione secondo l'articolo 4 per ottenere la deroga dall'obbligo di notifica della collezione di

dati secondo l'articolo 11a capoverso 5 lettera f LPD deve presentare i seguenti documenti, se ne viene fatta richiesta:

- a. rapporto di valutazione;
- b. documenti di certificazione.

<sup>2</sup> L'ente certificato informa l'Incaricato se l'organismo di certificazione, svolgendo la propria attività di sorveglianza, riscontra mutamenti sostanziali delle condizioni di certificazione, in particolare per quanto riguarda l'adempimento di oneri o condizioni.

<sup>3</sup> L'Incaricato pubblica un elenco degli enti certificati esonerati dall'obbligo di notificare la collezione di dati. Tale documento indica la validità della certificazione.

### **Sezione 3: Sanzioni**

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

<sup>1</sup> L'organismo di certificazione può sospendere o revocare una certificazione accordata, segnatamente se nell'ambito della verifica (art. 6 cpv. 2) emergono gravi irregolarità. Costituiscono gravi irregolarità in particolare:

- a. l'inadempienza di requisiti essenziali per la certificazione dei dati; oppure
- b. l'uso ingannevole o abusivo di una certificazione.

<sup>2</sup> 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'ente certificato.

<sup>3</sup> 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

<sup>1</sup> Se l'Incaricato, svolgendo la propria attività di sorveglianza secondo gli articoli 27 o 29 LPD, riscontra gravi irregolarità presso l'ente certificato, ne informa l'organismo di certificazione.

<sup>2</sup> L'organismo di certificazione provvede senza indugio a far adottare, entro 30 giorni dalla comunicazione dell'Incaricato, le misure necessarie all'adempimento delle condizioni di certificazione o alla garanzia di un utilizzo corretto della certificazione.

<sup>3</sup> Se l'ente certificato non rimedia alle irregolarità entro tale scadenza, l'organismo di certificazione sospende la certificazione. La certificazione va revocata se appare improbabile che in tempo utile venga a crearsi o venga ripristinata una situazione conforme alla legge.

<sup>4</sup> Se, scaduto il termine di cui al capoverso 2, l'ente certificato non ha posto rimedio alle irregolarità 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'ente certificato o dell'organismo 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 di accreditamento svizzero.

#### **Sezione 4: Disposizioni finali**

##### **Art. 11**           Entrata in vigore

<sup>1</sup> Fatto salvo il capoverso 2, la presente ordinanza entra in vigore il 1° gennaio 2007.

<sup>2</sup> Il Dipartimento federale di giustizia e polizia determina la data dell'entrata in vigore degli articoli 1 capoverso 2 lettera b, 5 e 6 capoverso 3 nonché del numero 2 dell'allegato.

*Allegato*

(Art. 1 cpv. 5)

## **Requisiti di qualifica del personale degli organismi di certificazione addetto alla certificazione**

### **1 Certificazione di sistemi di gestione della protezione dei dati (SGPD)**

L'organismo di certificazione deve dimostrare che il personale addetto alla certificazione dei SGPD disponga delle qualifiche seguenti:

- conoscenza del diritto in materia di protezione dei dati: dev'essere comprovata un'esperienza pratica di almeno due anni in tale ambito oppure il conseguimento di una formazione pertinente di almeno un anno presso un'università o una scuola universitaria professionale;
- competenze in materia di sicurezza informatica: dev'essere comprovata un'esperienza pratica di almeno due anni in tale ambito oppure il conseguimento di una formazione pertinente di almeno un anno presso un'università o una scuola universitaria professionale;
- formazione come certificatore di sistemi di gestione (secondo la guida ISO/IEC 62 [ISO/IEC 17021:...]).

L'organismo di certificazione può dimostrare di disporre di personale qualificato per i singoli settori. L'audit può essere affidato a una squadra interdisciplinare.

### **2 Certificazione di prodotti**

L'organismo di certificazione deve dimostrare che il personale addetto alla certificazione di prodotti disponga delle qualifiche seguenti:

- conoscenza del diritto in materia di protezione dei dati: dev'essere comprovata un'esperienza pratica di almeno due anni in tale ambito oppure il conseguimento di una formazione pertinente di almeno un anno presso un'università o una scuola universitaria professionale;
- competenze in materia di sicurezza informatica: dev'essere comprovata un'esperienza pratica di almeno due anni in tale ambito oppure il conseguimento di una formazione pertinente di almeno un anno presso un'università o una scuola universitaria professionale;
- conoscenze specifiche in materia di esame dei prodotti (secondo la guida ISO/IEC 65).

L'organismo di certificazione può dimostrare di disporre di personale qualificato per i singoli settori. L'esame può essere affidato a una squadra interdisciplinare.