Direttive
sulle esigenze minime che un sistema di gestione della protezione dei dati deve adempiere
(Direttive sulla certificazione dell'organizzazione e della procedura)

del 16 luglio 2008

L'incaricato federale della protezione dei dati e della trasparenza,

visto l'articolo 11 capoverso 2 della legge federale del 19 giugno 1992[1] sulla protezione dei dati (LPD);
visto l'articolo 4 capoverso 3 dell'ordinanza del 28 settembre 2007[2] sulle certificazioni in materia di protezione dei dati (OCPD),

emana le seguenti direttive:

1. Scopo

1 Le presenti direttive fissano le esigenze minime che un sistema di gestione della protezione dei dati (SGPD) deve adempiere per ottenere una certificazione dell'organizzazione o della procedura ai sensi dell'articolo 4 OCPD.

2 Hanno lo scopo di fornire un modello per lo stabilimento, l'attuazione, la conduzione, il monitoraggio, il riesame, l'aggiornamento e il miglioramento di un SGPD.

3 Si applicano a tutti i tipi d'organizzazione.

2. Definizioni

In aggiunta alle definizioni dei punti da 3.1 a 3.16 della norma ISO/CEI 27001:2005[3], si intende con:

a. *gestione della conformità*, le attività coordinate di un'organizzazione per rispettare le esigenze legali e regolamentari alle quali è sottomessa, in particolare quelle legate alla protezione dei dati;

b. *valutazione di non conformità*, l'insieme dei processi d'analisi di non conformità e di ponderazione di non conformità;

c. *analisi di non conformità*, l'utilizzo sistematico di informazioni per identificare le fonti di non conformità e per stimare la non conformità;

1 RS **235.1**
2 RS **235.13**
3 «Sistemi di gestione della sicurezza delle informazioni – Esigenze», ottenibile su licenza in formato cartaceo o PDF al sito www.iso.org.

d. *ponderazione di non conformità*, il processo di comparazione della non conformità stimata con i criteri di conformità prestabiliti, al fine di determinare la significatività della non conformità (natura minore o maggiore);

e. *trattamento di non conformità*, il processo di selezione e di attuazione di misure per rimediare a una non conformità[4].

3. Realizzazione

1 Un SGPD adempie le esigenze minime se si fonda su norme internazionali attualmente in uso, in particolare la norma ISO 27001, interpretata ai sensi del capoverso 2 e completata o emendata conformemente al punto 4.

2 Le esigenze della norma ISO 27001 relative al sistema di gestione della sicurezza delle informazioni (SGSI) devono essere riprese introducendo, da un lato, la nozione di protezione dei dati (PD) al posto di quella di sicurezza delle informazioni (SI) e, dall'altro, sostituendo l'allegato A della norma ISO 27001, corrispondente all'indice della norma ISO/CEI 27002:2005[5], con gli obiettivi e le misure enumerate al punto 5 delle presenti direttive.

4. Messa in opera (esigenze minime)

Il SGPD messo in funzione dall'organizzazione deve contenere almeno le esigenze minime descritte nella norma ISO 27001 e tenere conto degli aspetti di protezione dei dati seguenti:

a. in generale, la nozione di (non) conformità relativa alle esigenze di protezione dei dati completa sistematicamente quella di rischi relativi agli obiettivi di sicurezza delle informazioni. Un'analisi di conformità completa così l'analisi del rischio prevista dalla norma ISO 27001, in modo da escludere qualsiasi non conformità;

b. per quel che concerne in maniera specifica l'instaurazione del SGPD, i punti seguenti della norma ISO 27001 devono essere interpretati come segue:

4.2.1. a. il campo d'applicazione e i limiti del SGPD devono essere definiti conformemente all'articolo 4 capoverso 1 OCPD;

4.2.1. b. la politica del SGPD corrisponde alla politica di protezione dei dati di cui all'articolo 4 capoverso 2 lettera a OCPD;

4.2.1. d 1. i beni di tipo collezione di dati (art. 3 lett. g LPD) e i loro proprietari, all'occorrenza i detentori della collezione di dati (art. 3 lett. i LPD), devono essere identificati;

4 È pure possibile evitare una non conformità, ad esempio rinunciando al trattamento in questione. Non è invece possibile accettare o trasferire una non conformità.

5 «Codice di pratica per la gestione della sicurezza delle informazioni», ottenibile su licenza in formato cartaceo o PDF al sito www.iso.org.

4.2.1. g. gli obiettivi e le misure di protezione dei dati propriamente dette definiti al punto 5 sono selezionati come parte integrante del processo, nella misura in cui possono adempiere queste esigenze;

4.3.1. j[6]. la documentazione del SGPD deve includere almeno la lista delle collezioni di dati non notificate (cf. punto 5, lett h, n. 2).

5. Obiettivi e misure

Al momento dell'elaborazione del SGPD, gli obiettivi e le misure[7] seguenti devono essere realizzati:

a. Liceità (art. 4 cpv. 1 LPD)
   1. Motivi giustificativi (art. 13 LPD)
   2. Fondamenti giuridici (art. 17, 19 e 20 LPD)
   3. Trattamento dei dati da parte di terzi (art. 10*a* cpv. 1 LPD)

b. Trasparenza
   1. Buona fede (art. 4 cpv. 2 LPD)
   2. Riconoscibilità (art. 4 cpv. 4 LPD)
   3. Obbligo di informare (art. 7*a* cpv. 1 LPD)

c. Proporzionalità
   1. Trattamento proporzionale (art. 4 cpv. 2 LPD)

d. Scopo (art. 4 cpv. 3 LPD)
   1. Specificazione/Modifica dello scopo (art. 3 let. i LPD)
   2. Limitazione dell'uso

e. Esattezza dei dati
   1. Esattezza dei dati (art. 5 cpv. 1 LPD)
   2. Rettifica dei dati (art. 5 cpv. 2 LPD)

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

6 Lettera aggiuntiva della norma ISO 27001.

7 Gli obiettivi e le misure enumerati sono stati ripresi direttamente dal «Codice di pratica per la gestione della protezione dei dati» (il Codice di pratica può essere consultato all'indirizzo www.edoeb.admin.ch). La tabella delle misure non è esaustiva e un'organizzazione può considerare necessario aggiungere altri obiettivi o misure. Gli obiettivi e le misure di questa tabella devono essere selezionati come parte integrante del processo d'applicazione del SGPD. Il «Codice di pratica per la gestione della protezione dei dati» fornisce raccomandazioni di messa in opera e linee direttrici riguardanti le migliori pratiche e serve da supporto alle misure proposte. Questa guida è l'equivalente della norma ISO 27002 ("Codice di pratica per la gestione della sicurezza delle informazioni»). I 9 obiettivi ritenuti sono direttamente ripresi dalla LPD e le 20 misure associate sono strutturate conformemente alla norma ISO 27002.

g. Sicurezza dei dati (art. 7 LPD)
   1. Riservatezza dei dati
   2. Integrità dei dati
   3. Disponibilità dei dati
   4. Trattamento dei dati da parte di terzi (art 10*a* cpv. 2 LPD)

h. Registrazione delle collezioni di dati (art. 11*a* cpv. 1 LPD e art. 12*b* cpv. 1 OLPD)
   1. Obbligo di notificare (art. 11*a*, cpv. 2 e 3 ; eccezioni: art. 11*a* cpv. 5 lett. f–e LPD)
   2. Inventario delle collezioni di dati non notificate (art. 12*b* cpv. 1 lett. b OLPD)

i. Diritto d'accesso e procedura
   1. Diritto d'accesso ai propri dati (art. 8 cpv. 1 LPD)
   2. Azioni e procedura (art. 15 e 25 LPD)

6. Entrata in vigore

Le presenti direttive entrano in vigore il 1° settembre 2008.

16 luglio 2008

L'Incaricato federale della protezione dei dati,

Hanspeter Thür