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

del 19 marzo 2014

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 conformemente all'articolo 4 OCPD.

[2] Hanno lo scopo di fornire un modello per l'istituzione, 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 ai termini e alle definizioni dei numeri da 2.1 a 2.89 della norma ISO/CEI 27000:2014[3], si intende con:

a. *gestione della conformità*: le attività coordinate per gestire e controllare un'organizzazione sotto il profilo della conformità, in particolare quelle legate alla protezione dei dati;

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

c. *analisi di non conformità*: il processo volto a capire la natura di una non conformità e a stabilirne il livello, in considerazione delle conseguenze e della probabilità d'insorgenza delle stesse;

1 RS **235.1**
2 RS **235.13**
3 «Sistemi di gestione della sicurezza delle informazioni – Visione d'insieme e terminologia», ottenibile su licenza in formato cartaceo o PDF nel sito www.iso.org.

d. *ponderazione di non conformità*: il processo di comparazione dei risultati dell'analisi di non conformità con i criteri di conformità, al fine di determinare se la non conformità o la sua importanza sono accettabili;

e. *trattamento di non conformità*: il processo volto a modificare (ossia ad attenuare, eliminare, prevenire, ridurre o evitare, ma non ad accettare, condividere o trasferire) la non conformità.

3. Realizzazione

1 Un SGPD adempie le esigenze minime se si fonda su norme internazionali attualmente in uso, in particolare la norma ISO/IEC 27001:2013[4], interpretata ai sensi del capoverso 2 e completata o emendata conformemente al numero 4.

2 Le esigenze della norma ISO 27001 relative al sistema di gestione della sicurezza delle informazioni (SGSI) devono essere riprese sostituendo la nozione di sicurezza delle informazioni (SI) con quella di protezione dei dati (PD) nonché sostituendo l'allegato A della norma ISO 27001, corrispondente all'indice della norma ISO/CEI 27002:2013[5], con gli obiettivi e le misure enumerate nel numero 5 delle presenti direttive.

4. Messa in opera (esigenze minime)

Il SGPD istituito dall'organizzazione deve contenere almeno le esigenze minime della norma ISO 27001 e tenere conto degli aspetti inerenti alla protezione dei dati seguenti:

a. in generale, la nozione di conformità (o di non conformità) 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 residua;

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

   4.3. il campo d'applicazione e i limiti del SGPD sono definiti conformemente all'articolo 4 capoverso 1 OCPD;

   5.2. la politica di protezione dei dati[6] corrisponde a quella dell'articolo 4 capoverso 2 lettera a OCPD;

4 «Sistemi di gestione della sicurezza delle informazioni – Requisiti», ottenibile su licenza in formato cartaceo, ePub o PDF nel sito www.iso.org.

5 «Raccolta di prassi sui controlli per la sicurezza delle informazioni», ottenibile su licenza in formato cartaceo, ePub o PDF nel sito www.iso.org.

6 Questa politica di protezione dei dati di livello superiore viene completata con altre politiche tematiche di sicurezza dell'informazione o di protezione della sfera privata descritte nel controllo A.5.1.1.

6.1.2.c.2. i beni di tipo collezione di dati (art. 3 lett. g LPD) e i loro proprietari, in questo caso i detentori della collezione di dati (art. 3 lett. i LPD), devono essere identificati in particolare;

6.1.3.b. gli obiettivi e le misure di protezione dei dati propriamente dette definiti nel numero 5 sono selezionati come parte integrante del processo, nella misura in cui possono adempiere queste esigenze;

7.5.1.c[7]. la documentazione del SGPD deve includere almeno la lista delle collezioni di dati non notificate (cfr. n. 5 lett. h n. 2).

5. Obiettivi e misure

Al momento dell'elaborazione del SGPD, gli obiettivi e le misure[8] 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 lett. 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);

7 Lettera aggiuntiva della norma ISO 27001.

8 Gli obiettivi e le misure enumerati sono stati ripresi direttamente dal «Codice di pratica per la gestione della protezione dei dati» (il testo 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. Equivalente della norma ISO 27002, 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.
I nove 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 notifica (art. 11*a* cpv. 2 e 3 LPD; eccezioni: art. 11*a* cpv. 5 lett. e–f 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. Abrogazione di un altro atto normativo

Le Direttive del 16 luglio 2008[9] sulla certificazione dell'organizzazione e della procedura sono abrogate.

7. Disposizione transitoria

Le procedure di certificazione pendenti al momento dell'entrata in vigore di queste direttive sono rette dal diritto anteriore. Tali procedure devono essere concluse entro il 1° ottobre 2014.

8. Entrata in vigore

Le presenti direttive entrano in vigore il 1° maggio 2014.

19 marzo 2014

L'Incaricato federale
della protezione dei dati e della trasparenza:

Hanspeter Thür

9 FF **2008** 6375