Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

FF 2023
www.fedlex.admin.ch
La versione elettronica firmata
è quella determinante

Direttive sulle esigenze minime che un sistema di gestione dati devono adempiere

(Direttive sulla certificazione dei sistemi di gestione)

del 31 agosto 2023

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

visto l'articolo 6 capoverso 2 dell'ordinanza del 31 agosto 2022[1] 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 (sistema di management, SM) deve adempiere per ottenere una certificazione dell'organizzazione o della procedura conformemente all'articolo 6 OCPD

[2] Hanno lo scopo di fornire un modello per l'istituzione, la gestione, il monitoraggio, il riesame, l'aggiornamento e il miglioramento di un SM.

[3] Si applicano a tutti i tipi d'organizzazione.

2. Definizioni

In aggiunta ai termini e alle definizioni della norma ISO/CEI 27000[2], 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;

1 RS **235.13**

2 «Information security management systems – Overview and vocabulary», ottenibile su licenza in formato cartaceo o PDF nel sito www.iso.org Le norme menzionate possono essere consultate gratuitamente o ottenute a pagamento presso l'Associazione svizzera di normalizzazione (SNV), Sulzerallee 70, 8404 Winterthur; www.snv.ch

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;

d. *ponderazione di non conformità:* il processo di comparazione die 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 SM adempie le esigenze minime se si fonda su norme internazionali attualmente in uso, in particolare la norma ISO/CEI 27001[3], interpretata ai sensi del capoverso 2 e completata o emendata conformemente al numero 4.

2 Le esigenze della norma ISO/CEI 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 supplemento l'allegato A della norma ISO/CEI 27001, corrispondente all'indice della norma ISO/CEI 27002[4] con gli obiettivi e le misure enumerate nel numero 5 delle presenti direttive.

4. Messa in opera (esigenze minime)

Il SM istituito dall'organizzazione deve contenere almeno le esigenze minime della norma ISO/CEI 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/CEI 27001, in modo da escludere qualsiasi non conformità residua.

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

4.3. il campo d'applicazione e i limiti del SM sono definiti conformemente all'articolo 4 capoverso 2 OCPD.

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

4 «Information security controls», ottenibile su licenza in formato cartaceo, ePub o PDF nel sito www.iso.org.

5.2. la politica di protezione dei dati[5] corrisponde a quella dell'articolo 6 capoverso 2 lettera a OCPD.

6.1.2. c.2. i beni di tipo collezione di dati (art. 5 lett. d e art. 12 LPD) e i loro titolare del trattamento (Proprietario del rischio) (art. 5 lett. j 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.[6] la documentazione del SM deve includere almeno il Registro delle attività di trattamento e una valutazione per stabilire se le attività di trattamento comportano rischi elevati per la personalità o i diritti fondamentali degli interessati.

5. Obiettivi e misure

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

a. liceità (art. 6 cpv. 1 LPD):
   1. motivi giustificativi (art. 31 LPD),
   2. fondamenti giuridici (art. 34 e 36 LPD),
   3. trattamento di dati personali da parte di un responsabile (art. 9 LPD in combinato disposto con art. 7 OPDa);

b. trasparenza:
   1. buona fede (art. 6 cpv. 2 LPD),
   2. riconoscibilità (art. 6 cpv. 3 LPD),
   3. obbligo di informare (art. 19 – 21 LPD in combinato disposto con art. 13 OPDa),
   4. registro delle attività di trattamento (art. 12 LPD in combinato disposto con art. 24 OPDa),
   5. valutazione d'impatto sulla protezione dei dati (art. 22 LPD in combinato disposto con art. 14 OPDa),
   6. notifica di violazioni della sicurezza dei dati (art. 24 LPD in combinato, disposto con. art. 15 OPDa);

c. proporzionalità:
   1. trattamento proporzionale (art. 6 cpv. 2 LPD),

5 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 Lettera aggiuntiva della norma ISO/CEI 27001.

7 Gli obiettivi e le misure elencati non sono esaustivi e un'organizzazione è libera di prendere in considerazione ulteriori obiettivi o misure. Gli obiettivi e le misure del presente catalogo devono essere selezionati come parte del processo di implementazione del SM.

2. protezione dei dati personali sin dalla progettazione e per impostazione predefinita (art. 7 LPD);

d. scopo (art. 6 cpv. 3 LPD);

e. esattezza dei dati (art. 6 cpv. 5 LPD);

f. Comunicazione di dati personali all'estero (art. 16 LPD in combinato disposto con art. 8 – 12 OPDa);

g. dei dati (art. 8 LPD in combinato disposto con art. 1 – 6 OPDa);

h. diritti e procedura:
   1. diritto d'accesso (art. 25 LPD in combinato disposto con art. 16 – 19 OPDa),
   2. diritto di farsi consegnare dati o di esigerne la trasmissione a terzi (art. 28 LPD in combinato disposto con art. 20 – 22 OPDa),
   3. azioni e procedura (art. 32 e 41s. OPDa).

6. Abrogazione di un altro atto normativo

Le Direttive del 19 marzo 2014[8] 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° marzo 2024.[9]

8. Entrata in vigore

Le presenti direttive entrano in vigore il 1° settembre 2023.

31 agosto 2023

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

Adrian Lobsiger

8 FF **2014** 2787
9 Le altre disposizioni transitorie saranno pubblicate dal Servizio di accreditamento svizzero (SAS).