Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS)

(Codice in materia di protezione dei dati personali
art. 34 e Allegato B, regola 19, del d.lg. 30 giugno 2003, n. 196)

Premessa

La presente guida mira a facilitare l'adempimento dell'obbligo di redazione del documento programmatico sulla sicurezza (DPS) nelle organizzazioni di piccole e medie dimensioni o, comunque, non dotate al proprio interno di competenze specifiche [1].

La guida può essere di ausilio nella redazione del DPS, ma non è obbligatorio utilizzarla per adempiere all'obbligo.

La guida è strutturata in due parti: la prima contiene istruzioni per sviluppare il DPS negli aspetti descrittivi oppure nella compilazione di alcune tabelle riportate nella seconda parte.

Nella guida sono anche evidenziati altri elementi utilizzabili facoltativamente - comprese alcune tabelle-, che si ritengono utili per una più approfondita definizione del DPS.

[1] Nelle strutture di piccole dimensioni dove possono mancare specifiche competenze, si può anche chiedere consultare per alcuni profili tecnici il fornitore/installatore degli strumenti elettronici e del relativo *software*.

Parte I

Istruzioni

Per ciascuna regola dell'Allegato B al Codice sono riportati

i contenuti, le informazioni essenziali e gli ulteriori elementi da inserire nel DPS

Elenco dei trattamenti di dati personali (regola 19.1)

Contenuti

In questa sezione sono individuati i trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura (ufficio, funzione, ecc.) interna od esterna operativamente preposta, nonché degli strumenti elettronici impiegati.

Nella redazione della lista si può tener conto anche delle informazioni contenute nelle notificazioni eventualmente inviate al Garante anche in passato.

Informazioni essenziali (*v. anche* ***tab. 1.1***)

Per ciascun trattamento vanno indicate le seguenti informazioni secondo il livello di sintesi determinato dal titolare:

Descrizione sintetica: menzionare il trattamento dei dati personali attraverso l'indicazione della finalità perseguita o dell'attività svolta (es., fornitura di beni o servizi, gestione del personale, ecc.) e delle categorie di persone cui i dati si riferiscono (clienti o utenti, dipendenti e/o collaboratori, fornitori, ecc.).

Natura dei dati trattati: indicare se, tra i dati personali, sono presenti dati sensibili o giudiziari.

Struttura di riferimento: indicare la struttura (ufficio, funzione, ecc.) all'interno della quale viene effettuato il trattamento. In caso di strutture complesse, è possibile indicare la macro-struttura (direzione, dipartimento o servizio del personale), oppure gli uffici specifici all'interno della stessa (ufficio contratti, sviluppo risorse, controversie sindacali, amministrazione-contabilità.)

Altre strutture che concorrono al trattamento: nel caso in cui un trattamento, per essere completato, comporta l'attività di diverse strutture è opportuno indicare, oltre quella che cura primariamente l'attività, le altre principali strutture che concorrono al trattamento anche dall'esterno.

Descrizione degli strumenti elettronici utilizzati: va indicata la tipologia di strumenti elettronici impiegati (elaboratori o p.c. anche portatili, collegati o meno in una rete locale, geografica o Internet; sistemi informativi più complessi).

Ulteriori elementi per descrivere gli strumenti (*v. anche* ***tab. 1.2***) [*]

Identificativo del trattamento: alla descrizione del trattamento, se ritenuto utile, può essere associato un codice, facoltativo, per favorire un'identificazione univoca e più rapida di ciascun trattamento nella compilazione delle altre tabelle.

Banca dati: indicare eventualmente la banca dati (ovvero il data base *o l'archivio informatico), con le relative applicazioni, in cui sono contenuti i dati. Uno stesso trattamento può richiedere l'utilizzo di dati che risiedono in più di una banca dati. In tal caso le banche dati potranno essere elencate.*

Luogo di custodia dei supporti di memorizzazione: indicare il luogo in cui risiedono fisicamente i dati, ovvero dove si trovano (in quale sede, centrale o periferica, o presso quale fornitore di servizi, ecc.) gli elaboratori sui cui dischi sono memorizzati i dati, i luoghi di conservazione dei supporti magnetici utilizzati per le copie di sicurezza (nastri, CD, ecc.) ed ogni altro supporto rimovibile. Il punto può essere approfondito meglio in occasione di aggiornamenti.

[*] Da indicare facoltativamente.

Tipologia di dispositivi di accesso: elenco e descrizione sintetica degli strumenti utilizzati dagli incaricati per effettuare il trattamento: pc, terminale non intelligente, palmare, telefonino, ecc.

Tipologia di interconnessione: descrizione sintetica e qualitativa della rete che collega i dispositivi d'accesso ai dati utilizzati dagli incaricati: rete locale, geografica, Internet, ecc.

Le predette informazioni possono essere completate o sostituite da schemi, tabelle, disegni di architettura del sistema informativo o da altri documenti aziendali già compilati e idonei a fornire in altro modo le informazioni medesime.

Distribuzione dei compiti e delle responsabilità (regola 19.2)

Contenuti

In questa sezione occorre descrivere sinteticamente l'organizzazione della struttura di riferimento, i compiti e le relative responsabilità, in relazione ai trattamenti effettuati. Si possono utilizzare anche mediante specifici riferimenti documenti già predisposti (provvedimenti, ordini di servizio, regolamenti interni, circolari), indicando le precise modalità per reperirli.

*Informazioni essenziali (v. anche **tab. 2**)*

Struttura: riportare le indicazioni delle strutture già menzionate nella precedente sezione.

Trattamenti effettuati dalla struttura: indicare i trattamenti di competenza di ciascuna struttura.

Compiti e responsabilità della struttura: descrivere sinteticamente i compiti e le responsabilità della struttura rispetto ai trattamenti di competenza. Ad esempio: acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.). Anche in questo caso è possibile utilizzare, nei termini predetti, altri documenti già predisposti.

Analisi dei rischi che incombono sui dati (regola 19.3)

Contenuti

Descrivere in questa sezione i principali eventi potenzialmente dannosi per la sicurezza dei dati, e valutarne le possibili conseguenze e la gravità in relazione al contesto fisico–ambientale di riferimento e agli strumenti elettronici utilizzati.

*Informazioni essenziali (v. anche **tab. 3**)*

Elenco degli eventi: individuare ed elencare gli eventi che possono generare danni e che comportano, quindi, rischi per la sicurezza dei dati personali. In particolare, si può prendere in considerazione la lista esemplificativa dei seguenti eventi:

1) comportamenti degli operatori:

- *sottrazione di credenziali di autenticazione*
- *carenza di consapevolezza, disattenzione o incuria*
- *comportamenti sleali o fraudolenti*
- *errore materiale*

2) eventi relativi agli strumenti:

- *azione di virus informatici o di programmi suscettibili di recare danno*
- *spamming o tecniche di sabotaggio*
- *malfunzionamento, indisponibilità o degrado degli strumenti*
- *accessi esterni non autorizzati*
- *intercettazione di informazioni in rete*

3) eventi relativi al contesto fisico-ambientale:

- *ingressi non autorizzati a locali/aree ad accesso ristretto*
- *sottrazione di strumenti contenenti dati*
- *eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria*
- *guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)*
- *errori umani nella gestione della sicurezza fisica*

E' possibile, per ulteriori dettagli, rinviare a documenti analoghi già redatti in tema di piani di sicurezza e gestione del rischio, come ad es.: Business Continuity Plan, Disaster Recovery Plan, *ecc. (si tenga però presente che le analisi alla base di questi altri documenti possono avere una natura ben diversa).*

Impatto sulla sicurezza: descrivere le principali conseguenze individuate per la sicurezza dei dati, in relazione a ciascun evento, e valutare la loro gravità anche in relazione alla rilevanza e alla probabilità stimata dell'evento (anche in termini sintetici: es., alta/media/bassa). In questo modo è possibile formulare un primo indicatore omogeneo per i diversi rischi da contrastare.

L'analisi dei rischi può essere condotta utilizzando metodi di complessità diversa: l'approccio qui descritto è volto solo a consentire una prima riflessione in contesti che per dimensioni ridotte o per altre analoghe ragioni, non ritengano di dover procedere ad una analisi più strutturata.

Misure in essere e da adottare (regola 19.4)

Contenuti

In questa sezione vanno riportate, in forma sintetica, le misure in essere e da adottare per contrastare i rischi individuati. Per misura si intende lo specifico intervento tecnico od organizzativo posto in essere (per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia), come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.

Le misure da adottare possono essere inserite in una sezione dedicata ai programmi per migliorare la sicurezza.

Informazioni essenziali

Misure: descrivere sinteticamente le misure adottate (seguendo anche le indicazioni contenute nelle altre regole dell'Allegato B del Codice).

Descrizione dei rischi: per ciascuna misura indicare sinteticamente i rischi che si intende contrastare (anche qui, si possono utilizzare le indicazioni fornite dall'Allegato B).

Trattamenti interessati: indicare i trattamenti interessati per ciascuna delle misure adottate.

Determinate misure possono non essere riconducibili a specifici trattamenti o banche di dati (ad esempio, con riferimento alle misure per la protezione delle aree e dei locali).

Occorre specificare se la misura è già in essere o da adottare, con eventuale indicazione, in tale ultimo caso, dei tempi previsti per la sua messa in opera.

Struttura o persone addette all'adozione: indicare la struttura o la persona responsabili o preposte all'adozione delle misure indicate.

*Ulteriori elementi per la descrizione analitica delle misure di sicurezza (v. anche **tab. 4.2**)*[*]

Oltre alle informazioni sopra riportate può essere opportuno compilare, per ciascuna misura, una scheda analitica contenente un maggior numero di informazioni, utili nella gestione operativa della sicurezza e, in particolare, nelle attività di verifica e controllo.

Queste schede sono a formato libero e le informazioni utili devono essere individuate in funzione della specifica misura. A puro titolo di esempio, possono essere inserite informazioni relative a:

- *la minaccia che si intende contrastare*
- *la tipologia della misura (preventiva, di contrasto, di contenimento degli effetti ecc.)*
- *le informazioni relative alla responsabilità dell'attuazione e della gestione della misura*
- *i tempi di validità delle scelte (contratti esterni, aggiornamento di prodotti, ecc.)*
- *gli ambiti cui si applica (ambiti fisici -un reparto, un edificio, ecc.– o logici - una procedura, un'applicazione, ecc.-)*

Può essere opportuno indicare chi ha compilato la scheda e la data in cui la compilazione è terminata.

[*] Da indicare facoltativamente.

Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5)

Contenuti

In questa sezione sono descritti i criteri e le procedure adottati per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati. L'importanza di queste attività deriva dall' eccezionalità delle situazioni in cui il ripristino ha luogo: è essenziale che, quando sono necessarie, le copie dei dati siano disponibili e che le procedure di reinstallazione siano efficaci. Pertanto, è opportuno descrivere sinteticamente anche i criteri e le procedure adottate per il salvataggio dei dati al fine di una corretta esecuzione del loro ripristino.

Informazioni essenziali *(v. anche* ***tab. 5.1****)*

Per quanto riguarda il ripristino, le informazioni essenziali sono:

Banca dati/Data base/Archivio: indicare la banca dati, il data base *o l'archivio interessati.*

Criteri e procedure per il salvataggio e il ripristino dei dati: descrivere sinteticamente le procedure e i criteri individuati per il salvataggio e il ripristino dei dati, con eventuale rinvio ad un'ulteriore scheda operativa o a documentazioni analoghe.

Pianificazione delle prove di ripristino: indicare i tempi previsti per effettuare i test *di efficacia delle procedure di salvataggio/ripristino dei dati adottate.*

Ulteriori elementi per specificare i criteri e le procedure per il salvataggio e il ripristino dei dati *(v. anche* ***tab. 5.2****)* [*]

Data base: identificare la banca, la base o l'archivio elettronico di dati interessati.

Criteri e procedure per il salvataggio dei dati: descrivere sinteticamente la tipologia di salvataggio e la frequenza con cui viene effettuato.

Modalità di custodia delle copie: indicare il luogo fisico in cui sono custodite le copie dei dati salvate.

Struttura o persona incaricata del salvataggio: indicare la struttura o le persone incaricate di effettuare il salvataggio e/o di controllarne l'esito.

Pianificazione degli interventi formativi previsti (regola 19.6)

Contenuti

In questa sezione sono riportate le informazioni necessarie per individuare il quadro sintetico degli interventi formativi che si prevede di svolgere.

[*] Da indicare facoltativamente.

Informazioni essenziali

Descrizione sintetica degli interventi formativi: descrivere sinteticamente gli obiettivi e le modalità dell'intervento formativo, in relazione a quanto previsto dalla regola 19.6 (ingresso in servizio o cambiamento di mansioni degli incaricati, introduzione di nuovi elaboratori, programmi o sistemi informatici, ecc) .

Classi di incarico o tipologie di incaricati interessati: individuare le classi omogenee di incarico a cui l'intervento è destinato e/o le tipologie di incaricati interessati, anche in riferimento alle strutture di appartenenza.

Tempi previsti: indicare i tempi previsti per lo svolgimento degli interventi formativi.

Trattamenti affidati all'esterno (regola 19.7)

Contenuti

Redigere un quadro sintetico delle attività affidate a terzi che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi.

Informazioni essenziali

Descrizione dell'attività "esternalizzata": indicare sinteticamente l'attività affidata all'esterno.

Trattamenti di dati interessati: indicare i trattamenti di dati, sensibili o giudiziari, effettuati nell'ambito della predetta attività.

Soggetto esterno : indicare la società, l'ente o il consulente cui è stata affidata l'attività, e il ruolo ricoperto agli effetti della disciplina sulla protezione dei dati personali (titolare o responsabile del trattamento).

Descrizione dei criteri: perché sia garantito un adeguato trattamento dei dati è necessario che la società a cui viene affidato il trattamento rilasci specifiche dichiarazioni o documenti, oppure assuma alcuni impegni anche su base contrattuale, con particolare riferimento, ad esempio, a:

1. *trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto;*
2. *adempimento degli obblighi previsti dal Codice per la protezione dei dati personali;*
3. *rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrazione delle procedure già in essere;*
4. *impegno a relazionare periodicamente sulle misure di sicurezza adottate –anche mediante eventuali questionari e liste di controllo- e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze.*

Cifratura dei dati o separazione dei dati identificativi (regola 19.8)

Contenuti

In questa sezione vanno rappresentate le modalità di protezione adottate in relazione ai dati per cui è richiesta la cifratura -o la separazione fra dati identificativi e dati sensibili-, nonché i criteri e le modalità con cui viene assicurata la sicurezza di tali trattamenti. Questo punto riguarda solo organismi sanitari e esercenti professioni sanitarie (regola 24).

Informazioni essenziali

Trattamenti di dati: descrivere i trattamenti (le banche o le basi di) dati oggetto della protezione

Protezione scelta: riportare la tipologia di protezione adottata, scelta fra quelle indicate dal Codice o in base a considerazioni specifiche del titolare.

Tecnica adottata: descrivere sinteticamente, in termini tecnici ed eventualmente organizzativi, la misura adottata. Ad esempio, in caso di utilizzo di cifratura, le modalità di conservazione delle chiavi e le procedure di utilizzo.

Parte II
Tabelle

Per ciascuna regola sono riportate, di seguito, una o più tabelle.

Le istruzioni per la compilazione dei campi che le compongono è contenuta nella Parte I.

Per ciascuna tabella può essere indicata facoltativamente anche la data di compilazione, che può rivelarsi utile qualora la tabella sia compilata in data significativamente diversa (antecedente) rispetto alla redazione finale del DPS.

Tabella 1.1 – Elenco dei trattamenti: informazioni essenziali

Descrizione sintetica del trattamento		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	S	G			

Tabella 1.2 – Elenco dei trattamenti: ulteriori elementi per descrivere gli strumenti [2]

Identificativo del trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione

[2] Da compilare facoltativamente, collegandola alla tabella precedente, ad esempio attraverso l'identificativo.

Tabella 2 – Competenze e responsabilità delle strutture preposte ai trattamenti

Struttura	Trattamenti effettuati dalla struttura	Descrizione dei compiti e delle responsabilità della struttura

Tabella 3 - Analisi dei rischi

Rischi		Si/No	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
Comportamenti degli operatori	sottrazione di credenziali di autenticazione		
	carenza di consapevolezza, disattenzione o incuria		
	comportamenti sleali o fraudolenti		
	errore materiale		
	altro evento		

Eventi relativi agli strumenti	azione di *virus* informatici o di programmi suscettibili di recare danno		
	spamming o tecniche di sabotaggio		
	malfunzionamento, indisponibilità o degrado degli strumenti		
	accessi esterni non autorizzati		
	intercettazione di informazioni in rete		
	altro evento		
Eventi relativi al contesto	accessi non autorizzati a locali/reparti ad accesso ristretto		
	sottrazione di strumenti contenenti dati		
	eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria		
	guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)		
	errori umani nella gestione della sicurezza fisica		
	altro evento		

Tab. 4.1 – Le misure di sicurezza adottate o da adottare

Misure	Descrizione dei rischi contrastati	Trattamenti interessati	Misura già in essere	Misura da adottare (*)	Struttura o persone addette all'adozione

(*) Indicare eventualmente i tempi previsti per l'adozione delle misure

Tab. 4.2 - Scheda descrittiva delle misure adottate [3]

Scheda n.		Compilata da		Data di compilazione	
Misura					
Descrizione sintetica					
Elementi descrittivi					
Data aggiornamento					

[3] Da compilare facoltativamente.

Tab. 5.1 - Criteri e procedure per il ripristino della disponibilità dei dati

Ripristino		
Banca /data base/archivio di dati	Criteri e procedure per il salvataggio e il ripristino dei dati	Pianificazione delle prove di ripristino

Tab. 5.2 - Criteri e procedure per il salvataggio dei dati [4]

Salvataggio			
Banca dati	Criteri e procedure per il salvataggio	Luogo di custodia delle copie	Struttura o persona incaricata del salvataggio

[4] Da compilare facoltativamente.

Tab. 6 - Pianificazione degli interventi formativi previsti

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessati	Tempi previsti

Tab. 7 - Trattamenti affidati all'esterno

Descrizione sintetica dell'attività esternalizzata	Trattamenti di dati interessati	Soggetto esterno	Descrizione dei criteri e degli impegni assunti per l'adozione delle misure

Tab. 8 - Cifratura dei dati o separazione dei dati identificativi *(solo per organismi sanitari ed esercenti professioni sanitarie)*

Trattamenti di dati	Protezione scelta (Cifratura/Separazione)	Tecnica adottata	
		Descrizione	Informazioni utili