DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il **Documento Programmatico Sulla Sicurezza (DPSS o DPS)** è la fotografia del trattamento dei dati in azienda, il manuale di pianificazione della sicurezza dei dati in azienda e l'unico documento aziendale di certificazione dell'adeguamento al Codice Privacy. Inoltre, esso è uno documento di qualità perché contiene tutto quanto è relativo alla sicurezza dei dati in azienda: trattamento dei dati, distribuzione delle responsabilità, analisi dei rischi, misure adottate e pianificazione per l'anno in corso.

Chi deve compilare il DPSS

Tutti coloro che trattano dati sensibili o giudiziari con strumenti elettronici, eccetto se lo fanno esclusivamente per fini amministrativi e contabili, o se trattano esclusivamente i dati sensibili dei loro dipendenti o collaboratori (stato di salute, senza indicazione della diagnosi, o adesione ai sindacati).
L'Ufficio del Garante ha precisato che nei fini amministrativi e contabili sono inclusi i trattamenti di dati sensibili conseguenti ad obblighi di legge, purché detti trattamenti non siano l'oggetto primario dell'attività sociale.
Uno studio medico o uno studio legale devono sicuramente compilare il DPSS, ma anche le aziende che selezionano personale per conto terzi, che svolgono ricerche di mercato o sondaggi d'opinione, ecc., sono tenuti a redigerlo.
Se l'azienda non utilizza computer, non è obbligata alla tenuta del DPSS, ma dovrebbe comunque compilare un **Documento sostitutivo**. Quest'ultimo è, in pratica, un documento di qualità, utile per riassumere lo stato dell'azienda relativo alla sicurezza dei dati e la tutela della privacy. Il documento non necessita di certificazione della data di compilazione.
Il DPSS, o il Documento sostitutivo, devono essere redatti dal Titolare, da un responsabile, se esiste, o da un consulente esperto in materia di privacy, e sottoscritti dal rappresentante legale dell'azienda.
Non pensate di redigere il DPSS con applicazioni standardizzate, ad utilizzo locale (cd-rom) oppure on-line. La vostra azienda è unica, anche se presenta problematiche simili a quelle di un vostro concorrente.
Non pensate che la redazione del DPSS sia solo un problema del vostro informatico o dell'esperto in sicurezza dei posti di lavoro. Entrambi, anche se sono nel loro campo sicuramente degli ottimi professionisti, sono portati naturalmente ad evidenziare, se non a monopolizzare, gli aspetti più prossimi alle loro competenze.
Rivolgetevi a professionisti esperti in privacy aziendale che, lavorando in stretto contatto con voi per mezzo di visite ed interviste in loco, elaborino un DPSS coerente con le realtà della vostra azienda, se ne assumano le dovute responsabilità dal punto di vista civile e vi forniscano costantemente le informazioni utili per permettervi di adeguare l'azienda alla sicurezza dei dati ed alla tutela della privacy.
A proposito di responsabilità, nel DPSS è necessario indicare sempre chi lo ha redatto o aggiornato, sia esso il rappresentante legale, il responsabile od il consulente privacy.

Perché compilare il DPSS

In primo luogo, per riunire in un documento di qualità tutto quanto concerne la sicurezza dei dati personali dell'azienda: ecco perché è importante predisporre e consultare costantemente il DPSS o il Documento sostitutivo.
In secondo luogo, almeno per il DPSS, per adempiere alle norme di cui al Codice Privacy.

Quando compilare il DPSS

Il DPSS deve essere redatto, o aggiornato, tutti gli anni **entro il 31 marzo**.
La data di redazione deve essere certificata, non perché lo chiede direttamente il Codice Privacy, ma perché dovrete dichiarare, a fronte di un controllo della Guardia di Finanza, che avete redatto il DPSS nei termini previsti. Il modo più semplice è quello di far timbrare il frontespizio da un ufficio postale, dopo averlo affrancato in base al peso del documento.
Se l'azienda è di nuova costituzione, il DPSS dovrà essere compilato contestualmente all'inizio d'attività.

Cosa deve contenere il DPSS

Il DPSS, in base alle norme di cui al Codice Privacy, deve contenere quanto segue:

- L'elenco dei trattamenti dei dati personali in azienda
- La distribuzione dei compiti e delle responsabilità nel trattamento dei dati personali
- L'analisi dei rischi che incombono sui dati personali
- Le misure di sicurezza adottate e da adottare per garantire la sicurezza dei dati
- La descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento
- Il piano di formazione ed il mansionario per gli incaricati al trattamento dei dati
- I piani di verifica e di attuazione della politica della sicurezza in azienda

Come compilare il DPSS

Il DPSS non è la frettolosa compilazione di una dichiarazione più o meno uguale per tutti, ma un documento di qualità da consultare costantemente.
Pertanto occorre attribuire quanto è richiesto al punto precedente alla struttura fisica ed organizzativa dell'azienda, posizionando ed identificando i diversi elementi che la costituiscono.

La prima parte del DPSS deve contenere la descrizione della **Struttura della Sede Operativa**.
Si evidenziano i **Luoghi fisici** in cui sono effettuati i trattamenti dei dati personali, con particolare attenzione alle situazioni rilevanti dal punto di vista della sicurezza dei dati. Ad esempio, la destinazione d'uso (ufficio, magazzino, ecc.), la dislocazione fisica (piano di elevazione, locali che la costituiscono, ecc.), accompagnata possibilmente da una pianta, gli accessi esterni ed interni (porte, finestre, ecc.), le relative protezioni (serrature, infissi, impianti d'allarme e antincendio, ecc.), il loro contenuto in strumenti elettronici (computer, server, ecc.) e contenitori (armadi, scaffalature, ecc.) e la possibilità di accesso del pubblico.
Quindi si elencano gli **Utenti**, interni ed esterni, responsabili e addetti al trattamento, le relative mansioni ed autorizzazioni di accesso ai dati personali.
Si prosegue con la descrizione dell'**Hardware**, cioè degli strumenti elettronici (computer, server, gruppi di continuità, ecc.) e del **Software** di sistema installato (BIOS, sistema operativo, antivirus, ecc.) e delle rispettive caratteristiche rilevanti per la sicurezza dei dati.

La seconda parte del DPSS deve contenere l'elenco dei **Dati trattati nella Sede Operativa**, distinti in Base Dati elettroniche (i dati archiviati nei computer) ed Archivi Cartacei (i dati cartacei contenuti negli armadi), ed il loro trattamento, completo di tipologia dei dati (personali, sensibili o giudiziari), descrizione, luogo fisico, hardware, software, utente e modalità di salvataggio periodico.

La terza parte del DPSS deve contenere l'**Analisi dei Rischi** che incombono sui dati personali.
Si inizia dai rischi generali, che coinvolgono tutta la struttura, ed in particolare si evidenziano i **rischi ambientali**. Si prosegue analizzando i **rischi specifici** , relativi ai luoghi fisici, l'hardware, il software ed i dati personali.

La quarta parte del DPSS deve contenere l'elenco delle **Misure di Sicurezza**, adottate e da adottare, distinte per tipologia di utilizzo: luoghi fisici, utenti, hardware, software o dati personali.
Tra le misure di sicurezza deve essere richiamata la procedura per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento (**Disaster Recovery**), che può essere descritta ampiamente nel **Mansionario Privacy**.

La quinta parte del DPSS deve contenere i piani relativi alla **Politica della Sicurezza** dell'azienda.
Il **Piano di adeguamento** indica le misure di sicurezza che saranno adottate entro l'anno in corso.
Il **Piano di verifica** contiene l'elenco delle procedure messe in atto nell'anno in corso per verificare sia la situazione corrente che lo stato di avanzamento di quanto previsto dal piano di adeguamento.
Il **Piano di formazione** indica quali procedure di formazione degli incaricati al trattamento dei dati saranno adottate nell'anno in corso.

L'ultima parte del DPSS deve contenere l'elenco delle **Variazioni rispetto al precedente DPSS** ed almeno i seguenti **Allegati**: le lettere d'incarico, di nomina o d'affido ed il Mansionario Privacy.

Potete utilizzare procedure di compilazione del DPSS differenti, lo stesso Garante ne propone una, ma quella che avete appena letto ci pare la più adatta per le piccole e medie imprese e gli studi professionali e la più pratica per la consultazione.
Se esistono ulteriori Sedi Operative, poiché il DPSS è dovuto per ogni intestatario di Partita IVA, dovrete compilare un unico documento, diversificando ogni parte o l'intero documento, conservando l'originale presso la Sede Legale e fornendone una copia ad ogni Sede Operativa.

Cosa fare del DPSS

Il DPSS non deve essere inviato a nessuno.
Deve invece essere conservato con i documenti aziendali presso la Sede Legale ed esibito alla Guardia di Finanza per eventuali controlli presso di voi.
Sole le copie possono essere portate fuori dall'azienda da personale autorizzato.
Ma, soprattutto, il DPSS deve essere regolarmente consultato dal responsabile e da tutti gli incaricati al trattamento dei dati. Questo è il suo scopo primario!!!