

# Vademecum DPS

In questi giorni, si sente molto parlare di adeguamento al Codice della Privacy e sono tutti preoccupati di predisporre il temutissimo Documento Programmatico sulla Sicurezza.

Per capire bene di cosa si tratta veramente abbiamo predisposto questo vademecum....

## Cos'è il DPS?

Deve essere un Documento (scritto) che traccia un Programma (programmatico) degli interventi che si prevede di adottare nell'anno a cui si riferisce per migliorare la Sicurezza nel trattamento dei dati personali.

Il Documento Programmatico sulla Sicurezza, partendo dalle misure di sicurezza adottate nel trattamento dei dati personali (lo stato attuale del livello di sicurezza) deve analizzare i potenziali rischi ed individuare le azioni correttive per evitare o meglio per ridurre al minimo il verificarsi di qualsiasi tipo di evento dannoso o pericoloso a carico degli stessi dati personali. In definitiva il Documento Programmatico sulla Sicurezza serve a fotografare la politica aziendale in tema di sicurezza dei dati personali, e a definire, sulla base di una attenta analisi dei potenziali rischi, quali misure saranno adottate per migliorare la sicurezza nel trattamento dei dati personali.

## A cosa serve?

Predisporre questo documento permette di capire come funzionano le nostre strutture di trattamento dei dati personali (strumenti, sistemi di accesso, sistemi e programmi informatici, attrezzature, locali, ecc..), quali trattamenti vengono effettuati, quanto investiamo per difendere i dati e le nostre informazioni e soprattutto come pensiamo di tutelare noi stessi da sanzioni penali e da pretestuose richieste di risarcimento danni provenienti da chi ritiene che abbiamo in qualche modo violato la sua privacy.

## Chi è obbligato a farlo?

Si tratta di uno dei punti più controversi della normativa in quanto mentre il codice dice una cosa l'allegato al codice dice una cosa diversa.

Da una lettura delle prescrizioni contenute nell'allegato B, infatti, sembrerebbe che il Documento Programmatico sulla Sicurezza lo debbano redigere solo coloro che trattano dati sensibili e giudiziari con ausilio di strumenti elettronici.

Al contrario, secondo quanto stabilito dall'art. 34 del Dlg. N.196/2003 Il Documento Programmatico sulla Sicurezza è obbligatorio per tutti coloro che trattano che trattano dati personali (senza distinzione di tipologia) con l'impiego di elaboratori elettronici.

## Chi lo deve compilare?

Materialmente deve essere compilato dal titolare di un trattamento, anche attraverso il Responsabile (se è stato designato).

## Termini di redazione

Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza.

## Periodicità

Per quando concerne l'aggiornamento per gli anni successivi il Documento Programmatico sulla Sicurezza deve essere redatto entro il 31 marzo di ogni anno.

## Come si redige

Esiste una "Guida operativa per redigere il Documento programmatico sulla sicurezza" pubblicata dal Garante della Privacy.

Il base a quanto definito al punto 19 del Disciplinare Tecnico in Materia di Misure minime di Sicurezza (allegato B al Dlgs. 196/2003) deve contenere obbligatoriamente le seguenti parti:

### - 19.1 Elenco dei trattamenti di dati personali

Individuare 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 a I Garante anche in passato.

### - 19.2 Distribuzione dei compiti e delle responsabilità

Descrizione sintetica dell'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.

### - 19.3 Analisi dei rischi che incombono sui dati

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.

### - 19.4 Misure in essere e da adottare

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.

#### - 19.5 Criteri e modalità di ripristino della disponibilità dei dati

Descrivere i criteri e le procedure adottate 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.

#### - 19.6 Pianificazione degli interventi formativi previsti

Riportare le informazioni necessarie per individuare il quadro sintetico degli interventi formativi che si prevede di svolgere.

#### - 19.7 Trattamenti affidati all'esterno

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.

#### - 19.8 Cifratura dei dati o separazione dei dati identificativi (Questo punto riguarda solo organismi sanitari e esercenti professioni sanitarie)

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.

#### La data certa

L'obbligo che il Documento Programmatico sulla Sicurezza, sia un "atto avente data certa". non è indicato in nessuna parte della normativa.

In proposito, comunque, il Garante osserva che tale requisito si collega con la comune disciplina civilistica in materia di prove documentali e, in particolare, con quanto previsto dagli artt. 2702 - 2704 del codice civile, i quali recano un'elencazione non esaustiva degli strumenti per attribuire data certa ai documenti, consentendo di provare tale data anche in riferimento a ogni "fatto che stabilisca in modo egualmente certo l'anteriorità della formazione del documento" (art. 2704, terzo comma, cod.civile).

#### Art. 2703 Codice Civile. Sottoscrizione autenticata

Si ha per riconosciuta la sottoscrizione autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.

L'autenticazione consiste nell'attestazione da parte del pubblico ufficiale che la sottoscrizione è stata apposta in sua presenza. Il pubblico ufficiale deve previamente accertare l'identità della persona che sottoscrive.

A chi deve essere inviato

Il Documento Programmatico sulla Sicurezza non deve essere inviato a nessuno. Una copia del Documento Programmatico sulla Sicurezza deve essere custodita presso la sede per essere consultabile e deve essere esibita in caso di controlli.

Nella relazione al bilancio&hellip;

Il titolare del trattamento deve dare conto nella relazione accompagnatoria del bilancio aziendale annuale dell'avvenuta redazione/aggiornamento del Documento Programmatico sulla Sicurezza.

Cosa si rischia&hellip;

L'&rsquo;inosservanza di questo obbligo rende il trattamento illecito anche se non si determina un danno per gli interessati, viola l'obbligo per il titolare dei dati, compreso il diritto fondamentale alla protezione dei dati personali delle persone che può essere esercitato nei confronti del titolare del trattamento (artt. 1 e 7, comma 3, del Codice), ed espone a responsabilità civile per danno anche non patrimoniale qualora, davanti al giudice ordinario, non si dimostri di aver adottato tutte le misure idonee ad evitarlo (artt. 15 e 152 del Codice).

Pertanto, in aggiunta alle conseguenze appena citate, il Codice conferma l'&rsquo;impianto secondo il quale l'&rsquo;omessa adozione di alcune misure indispensabili ("minime"), costituisce anche reato (art. 169 del Codice), che prevede l'&rsquo;arresto sino a due anni o l'&rsquo;ammenda da 10 mila euro a 50 mila euro. Le sanzioni vengono elevate qualora si trattino dati giudiziari e/o sensibili.