

**Ai gentili clienti**  
**Loro sedi**

## **DL semplificazioni: eliminato il DPS**

Gentile cliente,

con la presente intendiamo informarLa che secondo quanto previsto **dall'art. 45 del DL semplificazioni** (DL n. 5/2012), vengono **abrogate tutte le previsioni contenute nel Codice della privacy e nel Disciplinare tecnico sulle misure di sicurezza** che si riferiscono al **Documento Programmatico sulla Sicurezza** per il trattamento dei dati personali.

**Il DPS, ricordiamo, è un documento che rappresenta la politica del soggetto obbligato per quanto riguarda la privacy.** In altri termini, il documento fotografa la "privacy policy" e sulla base di un'attenta **analisi dei rischi procede a definire e programmare le misure necessarie per migliorare la sicurezza del trattamento dei dati personali.**

Il DPS, secondo le previgenti disposizioni andava redatto o aggiornato entro il 31 marzo di ciascun anno. **I soggetti obbligati alla redazione del DPS erano il titolare dei trattamenti di dati sensibili o giudiziari con strumenti elettronici, anche attraverso il responsabile, se designato.** Il DPS non andava inviato al Garante della privacy, ma doveva essere conservato presso la propria struttura ed esibito in caso di controllo.

### **Premessa**

Il DL n. 5/2012 – più noto come il DL semplificazioni – ha previsto, con l'articolo 45, **l'abrogazione di tutte le disposizioni contenute nel D.Lgs. n. 196/2003** (Codice della Privacy) **relative al documento programmatico sulla sicurezza.** In un'ottica di semplificazione degli adempimenti burocratici a carico delle imprese, infatti, **il DL semplificazioni ha previsto la totale eliminazione, a partire dal 31.03.2012, di tale onere.** Di conseguenza **vengono eliminate le ipotesi sanzionatorie previste dal Codice della Privacy relative a tale adempimento:**

- dall'articolo 162 comma 2 bis relativo alle **sanzioni amministrative in caso di irregolarità del DPS;**
- dall'articolo 169 relativo al **trattamento illecito dei dati personali.**

Evidenziamo che il DL n. 5/2012 deve essere **convertito ancora in legge**, pertanto è possibile che **il parlamento in sede di conversione del decreto approvi emendamenti modificativi delle disposizioni in commento.**

La redazione del documento programmatico sulla sicurezza, comunque, è solo **una delle misure di sicurezza**. Imprese, enti pubblici, professionisti e in genere **chi tratta i dati** (i cosiddetti titolari di trattamento) **devono rispettare le altre misure minime** (dalla password al back up), **per cui per questi obblighi rimangono applicabili anche le relative sanzioni.**

### **Il documento programmatico sulla privacy**

Il DPS, come noto, ai sensi delle previgenti disposizioni contenute all'articolo 34 del Codice della Privacy, veniva **redatto e aggiornato entro il 31 marzo di ogni anno e doveva contenere le seguenti indicazioni:**

<b>DPS – CONTENUTO PER SEZIONE DEL DOCUMENTO</b>	
<b>Elenco dei trattamenti di dati personali</b>	In questa sezione venivano individuati i <b>trattamenti effettuati dal titolare</b> , direttamente o attraverso collaborazioni esterne, con l'indicazione della <b>natura dei dati e della struttura</b> (ufficio, funzione, ecc.) interna od esterna operativamente preposta, nonché degli <b>strumenti elettronici impiegati</b> . Nella redazione della lista si poteva tener conto anche delle <b>informazioni contenute nelle notificazioni eventualmente inviate al Garante anche in passato.</b>
<b>Distribuzione dei compiti e delle responsabilità</b>	In questa sezione veniva descritta <b>sinteticamente l'organizzazione della struttura di riferimento, i compiti e le relative responsabilità, in relazione ai trattamenti effettuati.</b>
<b>Analisi dei rischi che incombono sui dati</b>	Venivano descritte in questa sezione i <b>principali eventi potenzialmente dannosi per la sicurezza dei dati</b> , e valutarne le possibili conseguenze e la gravità in relazione al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati.
<b>Misure in essere e da adottare</b>	In questa sezione andavano <b>riportate</b> , in forma sintetica, le <b>misure in essere e da adottare per contrastare i rischi individuati</b> . 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 potevano essere inserite in una sezione dedicata ai programmi per migliorare la sicurezza.
<b>Criteri e modalità di ripristino della disponibilità dei dati</b>	In questa sezione venivano <b>descritti i criteri e le procedure adottati per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati.</b>
<b>Pianificazione degli interventi formativi</b>	In questa sezione venivano riportate le <b>informazioni necessarie per individuare il quadro sintetico degli interventi formativi che si</b>

previsti	prevedeva di svolgere.
<b>Trattamenti affidati all'esterno</b>	Questa sezione del DPS prevedeva un <b>quadro sintetico delle attività affidate a terzi che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale</b> (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.
<b>Cifratura dei dati o separazione dei dati identificativi</b>	In questa sezione venivano rappresentate le modalità di <b>protezione adottate in relazione ai dati per cui è richiesta la cifratura</b> -o la separazione fra dati identificativi e dati sensibili-, nonché i <b>criteri e le modalità con cui viene assicurata la sicurezza di tali trattamenti</b> . Questo punto riguardava solo organismi sanitari e esercenti professioni sanitarie (regola 24).

## La modifica al codice della privacy

Nel dettaglio, l'articolo 45 del DL n. 5/2012 prevede l'abrogazione:

- **della lettera g), dell'art. 34, comma 1 e comma 1 bis, del D.Lgs 196/2003** (Codice della Privacy);
- del suo **Allegato B, paragrafi da 19 a 19.8 e 26** (Disciplinare Tecnico in materia di misure minime di sicurezza);

Complessivamente, quindi, **viene espunto dal codice della privacy ogni riferimento al Documento programmatico sulla Sicurezza**.

LE MODIFICHE AL CODICE DELLA PRIVACY	
Testo prima delle modifiche	Testo dopo le modifiche del DL n. 5/2012
<p>1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:</p> <p>a) autenticazione informatica;</p> <p>b) adozione di procedure di gestione delle credenziali di autenticazione;</p> <p>c) utilizzazione di un sistema di autorizzazione;</p> <p>d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;</p> <p>e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;</p> <p>f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;</p>	<p>1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:</p> <p>a) autenticazione informatica;</p> <p>b) adozione di procedure di gestione delle credenziali di autenticazione;</p> <p>c) utilizzazione di un sistema di autorizzazione;</p> <p>d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;</p> <p>e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;</p> <p>f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;</p> <p>g) (lettera abrogata);</p>

<p>g) tenuta di un aggiornato <b>documento programmatico sulla sicurezza</b>;</p> <p>h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.</p>	<p>h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.</p>
<p>1-bis. Per i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori, anche se extracomunitari, compresi quelli relativi al coniuge e ai parenti, la tenuta di un aggiornato <b>documento programmatico sulla sicurezza</b> è sostituita dall'obbligo di autocertificazione, resa dal titolare del trattamento ai sensi dell'articolo 47 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, di trattare soltanto tali dati in osservanza delle misure minime di sicurezza previste dal presente codice e dal disciplinare tecnico contenuto nell'allegato B). In relazione a tali trattamenti, nonché a trattamenti comunque effettuati per correnti finalità amministrativo - contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani, il Garante, sentiti il Ministro per la semplificazione normativa e il Ministro per la pubblica amministrazione e l'innovazione, individua con proprio provvedimento, da aggiornare periodicamente, modalità semplificate di applicazione del disciplinare tecnico contenuto nel citato allegato B) in ordine all'adozione delle misure minime di cui al comma 1.</p>	<p>1-bis. (Comma abrogato)</p>

Il decreto liberalizzazioni, come detto, ha abrogato anche le disposizioni di dettaglio sul Dps inserite nell'allegato B) al codice della privacy (in particolare i paragrafi da 19 a 19.8). **“Salta”, quindi, la necessità di documentare l'elenco dei trattamenti di dati personali e la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati.** “Salta” anche l'incombente di **mettere nero su bianco l'analisi dei rischi che incombono sui dati, le misure da adottare per garantire l'integrità e la disponibilità dei dati.**

### Gli altri adempimenti

Le **altre disposizioni in materia di sicurezza del trattamento dei dati personali**, invece, **rimangono intatte**. Tra queste ricordiamo in particolare:

- la **redazione idonee Informative** (Art. 13 DLgs 196/2003): Informative Dipendenti e Collaboratori; Informative Clienti, Fornitori, Potenziali Clienti, Terzi; Informative utenti sito web; Informativa Candidati all'assunzione; Privacy Policy sito web;

- la **nomina Incaricati al trattamento dati personali** (Art. 30 DLgs 196/2003): redazione documento che individua l'ambito di trattamento dati personali consentito a ciascuna unità organizzativa; redazione lettere d'incarico per ciascun incaricato al trattamento dati personali;
- la **nomina Responsabili al trattamento dati personali e analisi trattamenti affidati in outsourcing** (Art. 29 DLgs 196/2003): redazione lettera di nomina per ciascun Responsabile al trattamento dati personali; analisi dei casi specifici di affidamento dati personali all'esterno dell'Azienda; analisi dei flussi di dati intra ed extra Unione Europea; individuazione dell'ideone rapporto da formalizzare con i soggetti esterni ai quali viene affidato il trattamento dati personali;
- il **disciplinare interno uso Internet e Posta elettronica** (Art 154 comma 1 lett. c) DLgs 196/2003, Provvedimento Garante 1° Marzo 2007): redazione Disciplinare interno obbligatorio relativo all'uso di Internet e della posta elettronica;
- le **nuove prescrizioni in tema di Amministratori di sistema** (Art 154 comma 1 lett. c) e h) DLgs 196/2003, Provvedimento Garante 27 Novembre 2008): adempimenti procedurali e redazione documentazione richiesta dal Provvedimento Generale 27 novembre 2008 – Garante privacy;
- le nuove prescrizioni in materia di videosorveglianza (Art. 154 comma 1, lett. c) DLgs 196/2003, provvedimento garante 8 Aprile 2010);
- la **gestione Privacy Policy sito web, Newsletter e Servizi interattivi**: procedure di gestione dati personali utenti sito web; procedure di attivazione e gestione servizio Newsletter; procedure di attivazione e accesso aree riservate.

*Alla luce di quanto sopra, lo studio resta a disposizione per ogni qualsivoglia chiarimento in merito alle problematiche connesse a quanto argomentato.*

Cordiali saluti