



$$\Delta x \Delta p_x \geq \frac{\hbar}{2}$$

www.ingamendola.com

Il Documento Programmatico sulla Sicurezza (DPS): linee guida e misure attuative

Approfondimenti tematici



$$\Delta x \Delta p_x \geq \frac{\hbar}{2}$$

www.ingamendola.com

DPS

Documento Programmatico sulla Sicurezza

- **Obbligo di redazione**
- **Profili di responsabilità**
- **Trattamento di dati ultra-sensibili**

Obbligo di redazione del DPS

- In generale obbligo di adozione delle misure minime di sicurezza - (artt. 31-36 e all. B)
- Sanzioni penali in caso di mancata adozione
- Costituiscono solo una parte degli adempimenti
- Obbligo di ridurre i rischi (distruzione, perdita, diffusione, etc)
 - Adozione di misure idonee

Adozione delle misure minime

- Proroga dei termini (31 marzo 2006)
 - *Adozione delle misure minime di sicurezza di cui agli articoli da 33 a 35 e all'allegato B) che non erano previste dal decreto del Presidente della Repubblica 28 luglio 1999, n. 318 – (art.180, comma 1)*
- Proroga dei termini (30 giugno 2006)
 - *Per il titolare che dispone di strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione delle misure minime di cui all'articolo 34 (trattamento con strumenti elettronici) e delle corrispondenti modalità tecniche di cui all'allegato B) – (art.180, commi 2 e 3)*

(Legge 23 febbraio 2006, n. 51 – G.U. n. 49 del 28/02/06)

DPR n. 318, 28 luglio 1999

Regolamento recante norme per l'individuazione delle misure di sicurezza minime per il trattamento dei dati personali a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675

- Obbligo di redazione del DPS
 - per i titolari del trattamento dei dati di cui agli articoli 22 (*dati sensibili*) e 24 (*dati relativi ai provvedimenti di cui all'articolo 686 del codice di procedura penale*) della legge 675/96, effettuato mediante gli elaboratori indicati nell'articolo 3, comma 1, lettera b) del medesimo decreto, e cioè solo tramite elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico

D.Lgs. 196, 30 giugno 2003

Codice in materia di protezione dei dati personali

- Obbligo di redazione del DPS

- *il trattamento dei dati personali effettuato con strumenti elettronici è consentito solo se, tra le misure minime di sicurezza, si tiene aggiornato un documento programmatico sulla sicurezza (art. 34)*
- *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 (reg. 19, all. B)*

D.Lgs. 196, 30 giugno 2003

Codice in materia di protezione dei dati personali

- **Obbligo di redazione del DPS**

- art. 34: *DPS per coloro che trattano tutti i tipi di dati personali purché con strumenti elettronici*
- reg. 19, all. B: *solo i titolari di dati sensibili o giudiziari, a prescindere dalle modalità di trattamento (e dunque anche in assenza di strumenti elettronici)*

D.Lgs. 196, 30 giugno 2003

Codice in materia di protezione dei dati personali

- **Obbligo di redazione del DPS**
 - Garante Privacy: *la misura minima del DPS deve essere ora adottata dal titolare di un trattamento di dati sensibili o giudiziari effettuato con strumenti elettronici, attraverso l'organo, ufficio o persona fisica a ciò legittimata in base all'ordinamento aziendale o della pubblica amministrazione interessata (art. 34, comma 1, lett. g; reg. 19, all. B) – (Parere a Confindustria, 22 marzo 2004)*

D.Lgs. 196, 30 giugno 2003

Codice in materia di protezione dei dati personali

- II DPS

- non è solo un adempimento normativo
- è soprattutto un valido **strumento di autoanalisi**
- contestualizza l'analisi, la valutazione e la gestione del rischio
- apporta un **vantaggio competitivo**
- è il punto di partenza di un Sistema di Gestione per la Sicurezza delle Informazioni
- solleva solo da responsabilità penali

Profili di responsabilità

- Illeciti penali: omissione di adozione delle misure minime di sicurezza (art. 169)
 - *arresto sino a due anni o ammenda da 10.000 euro a 50.000 euro*
 - *"ravvedimento operoso" di chi adempie puntualmente alle prescrizioni impartite dal Garante una volta accertato il reato ed effettua un pagamento in sede amministrativa, ottenendo così l'estinzione del reato*

Profili di responsabilità

- Illeciti civili: danni cagionati per effetto del trattamento (art. 15)
 - *Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile*
 - art. 2050 del codice civile (*Responsabilità per l'esercizio di attività pericolose*): *chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno*

Profili di responsabilità

- Illeciti civili: **inversione dell'onere della prova**
 - *Il titolare del trattamento dovrà dimostrare di avere adottato tutte le misure idonee ad evitare il danno*
 - *Responsabilità **aggravata** o **oggettiva**?*

Profili di responsabilità

- Illeciti civili: **inversione dell'onere della prova**
 - responsabilità aggravata: *si riconduce la determinazione della responsabilità all'ordinaria diligenza ed alla comune prudenza del titolare del trattamento nella scelta e nell'adozione delle misure di sicurezza idonee*
 - responsabilità oggettiva: *l'imputabilità della responsabilità al titolare del trattamento verrà meno solo qualora l'evento dannoso si configuri come fortuito, ovvero imponderabile, ovvero senza alcun nesso eziologico con il trattamento stesso*

Profili di responsabilità

- Responsabilità: art. 23 della Direttiva Comunitaria 95/46/CE
 - *Gli Stati membri dispongono che chiunque subisca un danno cagionato da un trattamento illecito o da qualsiasi altro atto incompatibile con le disposizioni nazionali di attuazione della presente direttiva abbia il diritto di ottenere il risarcimento del pregiudizio subito dal responsabile del trattamento*
 - *Il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità se prova che l'evento dannoso non gli è imputabile*

Trattamento di dati ultra-sensibili

- **D.Lgs. 196/03**, Capo II – Regole ulteriori per i Soggetti Pubblici
 - *I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di **cifratura** o mediante l'utilizzazione di **codici identificativi** o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità (art. 22, comma 6)*
 - *Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, tra l'altro, 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 (art. 34, comma 1, lett. g)*

Trattamento di dati ultra-sensibili

- **Allegato B** – Disciplinare tecnico in materia di misure minime di sicurezza (artt. da 33 a 36 del codice)
 - *Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato (reg. 24)*

Trattamento di dati ultra-sensibili

- **Garante Privacy**

- *nel DPS occorre individuare i criteri da adottare per **cifrare** o per **separare i dati** idonei a rivelare lo stato di salute e la vita sessuale trattati da organismi sanitari ed esercenti le professioni sanitarie (regg. 19.8 e 24, all. B)*
- La **cifratura**, o la **disgiunzione**, riguardano solo organismi sanitari e esercenti professioni sanitarie



$$\Delta x \Delta p_x \geq \frac{\hbar}{2}$$

www.ingamendola.com

Grazie!

info@ingamendola.com

www.ingamendola.com