

SPECIALE PRIVACY PER LE AZIENDE

INDICE

<i>Introduzione</i>	Pag. 3
2. Soggetti che effettuano il trattamento dei dati personali	Pag. 5
4. Regole generali per il trattamento dei dati personali	Pag. 7
4.1 <i>Modalità del trattamento e requisiti dei dati</i>	Pag. 7
4.2 <i>Informativa</i>	Pag. 7
4.3 <i>Consenso</i>	Pag. 8
5. Le misure di sicurezza	
5.1 Le misure di sicurezza “idonee”	Pag. 10
5.2 Le misure di sicurezza “minime”	Pag. 10
5.2.1 <i>Dati trattati senza l’ausilio di strumenti informatici</i>	Pag. 11
5.2.2 <i>Dati trattati con l’ausilio di strumenti informatici</i>	Pag. 11
6. Il Documento Programmatico sulla sicurezza (DPS)	Pag. 13
7. Schema riassuntivo dei soggetti obbligati e degli adempimenti	Pag. 14

Introduzione

Dal 1° gennaio 2004 è entrato in vigore il Codice della Privacy. Si tratta di un Testo Unico sulle disposizioni in materia di protezione dei dati personali, che è stato adottato con il d.lgs. 30 giugno 2003, n. 196, pubblicato in Gazzetta Ufficiale il 29 luglio 2003.

Tale decreto è stato emanato ai sensi della legge di delega 24 marzo 2001, n. 127, la quale, all'art. 1, ha previsto che "Il Governo emana un testo unico delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e delle disposizioni connesse coordinandovi le norme vigenti ed apportando alle medesime le integrazioni e modificazioni necessarie al predetto coordinamento o per assicurarne la migliore attuazione."

Il testo unico riordina tutta la normativa in tema di trattamento dei dati personali riunendo in un unico contesto la L. 675/1996 e gli altri decreti legislativi¹, regolamenti e codici deontologici che si sono succeduti in questi ultimi anni, apportando numerose integrazioni e modificazioni che tengono conto della "giurisprudenza" del Garante per la protezione dei dati personali e della direttiva Ue 2000/58 sulla riservatezza nelle comunicazioni elettroniche.

Nell'opera di sistematizzazione dell'intera disciplina, il Legislatore si è ispirato ai principi di semplificazione ed efficacia, riducendo del 30% circa (come rileva la relazione di accompagnamento al codice) il numero di disposizioni vigenti in materia.

In particolare, l'opera di semplificazione ha investito principalmente l'adempimento delle notificazioni, dell'informativa e del consenso con un conseguente snellimento degli adempimenti necessari.

Il codice, costituito da 186 articoli, si compone di tre parti che contengono rispettivamente:

- disposizioni generali (artt. 1-45), riguardanti le regole "sostanziali" della disciplina del trattamento dei dati personali, applicabili a tutti i trattamenti, salvo eventuali regole specifiche (II parte);

¹ D.Lgs. n. 123 del 9 maggio 1997, D.Lgs. n. 255 del 28 luglio 1997, D.Lgs. n. 135 dell'8 maggio 1998, D.Lgs. n. 171 del 13 maggio 1998, D.Lgs. n. 389 del 6 novembre 1998, D.Lgs. n. 51 del 26 febbraio 1999, D.Lgs. n. 135 dell'11 maggio 1999, D.Lgs. 281 del 30 luglio 1999, D.Lgs. n. 282 del 30 luglio 1999, D.Lgs. n. 467 del 28 dicembre 2001.

- disposizioni particolari (artt. 46-140) per specifici trattamenti, ad integrazione od eccezione alle disposizioni generali (I parte);
- disposizioni (artt. 141-186) relative alle azioni di tutela dell'interessato ed al sistema sanzionatorio cui si aggiungono le norme di modifica, finali e di carattere transitorio.

Il codice è completato da tre allegati:

- Allegato A: codici di deontologia;
- Allegato B: disciplinare tecnico in materia di misure minime di sicurezza;
- Allegato C: elenco dei trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia che dovranno essere individuati entro il 30 giugno 2004 dai Ministeri competenti.

In relazione all'ambito di applicazione la suddetta normativa si applica:

- ai trattamenti di dati personali effettuati da titolari assoggettati alla normativa italiana;
- ai trattamenti di dati personali effettuati sul territorio nazionale anche da titolari stranieri;
- ai trattamenti di dati destinati alla comunicazione e diffusione.

Non si applica invece:

- ai trattamenti di dati anonimi;
- ai trattamenti di dati per scopi esclusivamente personali ed al semplice transito di dati sul territorio nazionale.

Devono adeguarsi alle nuove misure tutti coloro che trattano dati personali: aziende, professionisti, cooperative, associazioni, P.A., scuole, comuni, ospedali, enti pubblici ecc. (ovvero chiunque tratti dati personali di clienti, cittadini, dipendenti, fornitori, utenti, pazienti, colleghi, soci, associati ecc.).

La presente circolare ha lo scopo di fornire le informazioni di base circa la disciplina Privacy applicabile alla generalità delle imprese. Queste possono pertanto ricavarne le indicazioni essenziali per orientarsi circa gli adempimenti cui sono sottoposti, fermo rimanendo che sarà indispensabile effettuare un'analisi delle singole fattispecie, sulla base delle caratteristiche del trattamento dei dati personali di volta in volta realizzato.

**SOGGETTI CHE EFFETTUANO IL TRATTAMENTO DEI DATI PERSONALI: TITOLARE,
RESPONSABILE E INCARICATI.**

La raccolta e la conservazione dei dati personali (trattamento dei dati) può coinvolgere, oltre al soggetto obbligato per legge, anche altri soggetti che, in ausilio del soggetto obbligato, collaborano agli adempimenti relativi.

La legge distingue in proposito le seguenti figure:

a. Il Titolare del trattamento

È la persona fisica o la persona giuridica, cui competono (anche unitamente ad altro titolare), le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Nel caso delle aziende, *titolare del trattamento* è considerata l'azienda stessa in quanto persona giuridica nella persona del Legale Rappresentante.

Accanto alla figura del *titolare del trattamento*, definita direttamente dalla legge, sono individuabili due altre figure solo eventuali, traendo esse origine da un atto di nomina facoltativo: il responsabile del trattamento e l'incaricato.

b. Il Responsabile del trattamento

È la persona fisica o giuridica preposta dal *titolare* al trattamento dei dati personali. La designazione del responsabile è atto discrezionale ma, se compiuto, obbliga al rispetto di precisi criteri nella scelta del soggetto.

Il responsabile, infatti, deve essere individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo della sicurezza.

Inoltre, i compiti affidati al responsabile devono essere *specificati per iscritto* dal titolare (art. 29, comma 4 del Codice).

c. Gli Incaricati del trattamento

Sono le persone fisiche autorizzate a compiere operazioni di trattamento dal *titolare* e dal *responsabile*. Si tratta di una figura subordinata rispetto al titolare e al responsabile, il cui incarico si limita allo svolgimento materiale delle operazioni relative al trattamento dati.

STUDIO PARISI PRESICCE

DOTTORI COMMERCIALISTI · REVISORI CONTABILI

La designazione degli incaricati deve essere *effettuata per iscritto*, e deve indicare puntualmente l'ambito del trattamento consentito (art. 30, comma 2 del Codice).

In relazione a quanto detto va sottolineato che la norma (D. Lgs. 196/2003) **impone** all'azienda la sola individuazione, e relativa nomina, del Titolare del trattamento nella persona del legale rappresentante.

REGOLE GENERALI PER IL TRATTAMENTO DEI DATI PERSONALI

I soggetti che trattino dati personali, obbligati pertanto alla osservanza delle disposizione sulla privacy, devono provvedere in ogni caso:

- a trattare i dati secondo le modalità ed i requisiti richiesti dalla legge;
- a dare una serie di informazioni (*informativa*) ai soggetti i cui dati si vogliono raccogliere;
- ad ottenere che i medesimi soggetti prestino il consenso alla raccolta dei dati personali.

Modalità del trattamento e requisiti dei dati

I dati personali oggetto di trattamento devono essere:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

I dati personali che non vengono trattati in conformità a tale disciplina non possono essere utilizzati.

Informativa

Prima di poter trattare qualsiasi tipo di dato personale (sia esso solo personale o anche *sensibile* o *giudiziario*), è necessario dare talune informazioni (*informativa*) a coloro che forniscono i propri dati. Tra le novità del Codice Privacy è adesso consentito che l'*informativa* sia resa per iscritto o anche, in forma orale.

L'informazione resa deve riguardare:

- le finalità e le modalità del trattamento cui i dati sono destinati;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto a rispondere;

- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di *responsabili* o *incaricati*, e l'ambito di diffusione dei medesimi;
- i diritti di cui all'art. 7 del Codice;
- gli estremi identificativi del *titolare* e, se designato, del *responsabile*.

L'omessa o inidonea informativa è punita con sanzione amministrativa dai 3.000 ai 18.000 Euro nel caso dei dati personali, e da 5.000 a 30.000 Euro per dati sensibili o giudiziari.

Si ricorda che, seguito delle modificazioni legislative intervenute, dal 1° gennaio 2004 l'informativa deve essere resa ai sensi dell'art. 13 del D.Lgs. 196/2003. Vanno conseguentemente modificati i riferimenti normativi da citare nelle comunicazioni da dare al soggetto interessato.

Si è già detto che l'informativa può essere resa sia per iscritto che in forma orale. Tenuto conto tuttavia della complessità dell'informazione da dare, motivi di praticità e di cautela inducono a consigliare il rilascio dell'informativa in forma scritta (attraverso la predisposizione di un modello da conservare previa acquisizione della firma dell'interessato).

Consenso

In aggiunta all'informativa, è necessario che i soggetti i cui dati personali (anche se sensibili e giudiziari) si vogliono raccogliere prestino il proprio consenso alla raccolta dei loro dati personali.

In deroga a tale regola di generale applicazione, l'art. 24 del D.Lgs. 196/2003 prevede alcune ipotesi in cui il trattamento dei dati personali può essere effettuato senza che sia necessario raccogliere il consenso. Tra queste, si segnalano qui di seguito quelle principali:

- i casi previsti nella II parte del testo unico (disposizioni relative a specifici settori: trattamenti in ambito giudiziario, da parte di forze di polizia, per la difesa e sicurezza dello Stato, trattamenti in ambito pubblico, in ambito sanitario, riguardanti l'istruzione in ambito scolastico, per scopi storici, statistici o scientifici, riguardanti lavoro e previdenza sociale, il sistema bancario, finanziario ed assicurativo, effettuati da coloro che gestiscono servizi di comunicazione elettronica, trattamenti effettuati con finalità giornalistiche e di marketing diretto);

- quando il trattamento dei dati personali sia necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- quando il trattamento sia necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;
- quando il trattamento riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;
- quando il trattamento riguarda dati relativi allo svolgimento delle attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
- quando è necessario per la salvaguardia della vita e dell'incolumità fisica di un terzo.

Va comunque ricordato che, nel caso di trattamento di dati sensibili è sempre necessario il consenso scritto dell'interessato.

Al di fuori dei casi menzionati, il consenso dell'interessato al trattamento dei dati è sempre obbligatorio.

LE MISURE DI SICUREZZA DA ADOTTARE PER LA TUTELA DEI DATI PERSONALI

I soggetti che trattino dati personali, obbligati pertanto alla osservanza delle disposizioni sulla privacy (aziende, pubbliche amministrazioni, professionisti), **devono provvedere in ogni caso ad adottare le misure di sicurezza** che valgano ad evitare che i dati raccolti possano venire a conoscenza di terzi o possano comunque andare dispersi.

La legge distingue in proposito le misure di sicurezza da adottare in due categorie:

1. le misure di sicurezza *idonee*;
2. le misure di sicurezza *minime*.

La distinzione ha rilevanza ai fini sanzionatori, in quanto la inosservanza delle misure minime comporta una sanzione di natura penale. L'inosservanza delle misure *idonee* non comporta sanzioni ma espone ad eventuali azioni dei soggetti lesi per il risarcimento del danno.

Le misure di sicurezza "idonee"

L'obbligo di adottare misure di sicurezza *idonee* si sostanzia in un obbligo generico di predisporre qualunque precauzione necessaria alla tutela dei dati, per evitare, cioè, il rischio di distruzione o dispersione anche accidentale degli stessi ovvero di conoscenza da parte di terzi.

L'art. 31 del Codice infatti prevede che " *I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.*"

L'inadempienza di tale obbligo espone a responsabilità civile per danno.

Le misure di sicurezza "minime"

Nel quadro generale degli obblighi di sicurezza, la norma individua alcune misure di sicurezza ritenute indispensabili alla tutela dei dati personali e quindi assolutamente obbligatorie per tutte le imprese. Sono le così dette misure *minime* di sicurezza, previste dagli artt. 34 e 35 del Codice e specificate nell'allegato B (disciplinare tecnico).

Le misure minime di sicurezza sono differenziate a seconda delle modalità di trattamento dei dati:

- misure di sicurezza relative a dati trattati senza l'ausilio di strumenti elettronici;
- misure di sicurezza relative a dati trattati con l'ausilio di strumenti elettronici.

Il mancato adeguamento alle misure minime di sicurezza costituisce reato, con la previsione della pena dell'arresto sino a 2 anni o dell'ammenda da 10.000 a 50.000 € (art. 169 del Codice). Il Codice Privacy prevede che le misure minime di sicurezza di nuova istituzione debbano invece essere adottate **entro il 30 giugno 2004**. Si raccomanda, pertanto, a *tutti i soggetti che trattino dati personali*, di provvedere all'adozione delle misure minime di sicurezza, quali modificate dal Codice, entro la predetta data.

Sintesi delle misure minime di sicurezza

■ Dati trattati senza l'ausilio di strumenti informatici

Le misure minime di sicurezza da adottare per il trattamento dei dati personali in modo "cartaceo" (senza l'ausilio di strumenti informatici) sono tre:

1. Aggiornamento periodico (con cadenza almeno annuale) dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
2. Previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti.
3. Previsione di procedure per la conservazione di atti e documenti contenenti dati sensibili e giudiziari in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Nota bene: i primi due punti riguardano il caso in cui si sia provveduto ad individuare uno o più *incaricati* del trattamento. In tale ipotesi sarà dunque necessario, così come specificato dal Disciplinare tecnico (allegato B del Codice):

- impartire istruzioni scritte agli *incaricati* specificando l'ambito del trattamento consentito. Tali istruzioni devono essere aggiornate con scadenza almeno annuale;
- quando gli atti e i documenti contenenti *dati sensibili o giudiziari* sono affidati agli *incaricati*, i medesimi atti e documenti devono essere controllati e custoditi dagli *incaricati*, in maniera che ad essi non accedano persone prive di autorizzazione, e siano restituiti al termine delle operazioni affidate.

L'ultima misura minima di sicurezza da adottare riguarda anche coloro che non abbiano designato alcun incaricato ed è posta a tutela dei locali in cui vengono conservati i dati.

L'allegato B specifica in proposito che:

- l'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato;
- le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate;
- quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

■ **Dati trattati con l'ausilio di strumenti informatici**

Il trattamento dati effettuato con strumenti informatici prevede l'adozione di più complesse misure minime di sicurezza. Qui di seguito ne riportiamo l'elenco:

- a) adozione di procedure di autenticazione informatica e gestione delle credenziali di autenticazione (c.d. password);
- b) utilizzazione di un sistema di autorizzazione²;
- c) aggiornamento periodico (almeno trimestrale) dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- d) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, ad accessi non consentiti e a determinati programmi informatici;
- e) adozione di procedure per la custodia di copie di sicurezza (back-up), il ripristino della disponibilità dei dati in caso di danneggiamento e/o distruzione;

Per quanto riguarda tutti i punti si tratta di precauzioni da adottare sui sistemi informatici secondo le modalità prescritte dall'allegato B del Codice. Sarà dunque opportuno rivolgersi ai tecnici che forniscono la manutenzione per i propri *computer* per farsi rilasciare un'attestazione comprovante l'adozione delle misure privacy.

² I profili di autorizzazione diversi per classi omogenee di incaricati sono facoltativi. Qualora siano previsti sono individuati e configurati in modo tale da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

IL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Nell'ambito delle misure minime di sicurezza da adottare per il trattamento dati con l'ausilio di strumenti elettronici, rientra anche la predisposizione del **Documento Programmatico sulla Sicurezza (DPS)**.

Il DPS deve essere redatto entro il **30 giugno 2004**. Dal 2005 dovrà essere redatto o aggiornato entro il 31 marzo di ogni anno.

Il DPS deve riportare le seguenti informazioni:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia ed accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento dei dati personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al Codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione dagli altri dati personali dell'interessato.

**SCHEMA RIASSUNTIVO DEI SOGGETTI OBBLIGATI E DEGLI ADEMPIMENTI
PER LE IMPRESE IN MATERIA DI PRIVACY**

Sono tenuti ad osservare le disposizioni sulla privacy tutti coloro che trattano dati personali tra cui sicuramente **le imprese**. La disciplina di tutela dei dati personali, ora contenuta nel cosiddetto Codice Privacy, prevede una serie di obblighi. Si possono distinguere in proposito:

- 1) Individuazione dei soggetti che effettuano il trattamento dei dati personali, distinguendo tra Titolare, Responsabile ed Incaricato e loro nomina;
- 2) Informativa ai sensi dell'art. 13 D. Lgs. 196/03 per clienti, dipendenti e collaboratori;
- 3) Raccolta del consenso scritto al trattamento dei dati dai clienti e dipendenti/collaboratori;
- 4) Adeguamento alle Misure Minime di Sicurezza previste dall'allegato B al Codice;
- 5) Predisposizione del Documento Programmatico sulla Sicurezza (DPS).

DISPOSIZIONI AI SENSI DEL D. LGS. 196/2003	IMPRESE
Identificazione e nomina del Responsabile e degli Incaricati del trattamento	Facoltativa
Informativa ai clienti, ai dipendenti ed ai collaboratori	Obbligatoria
Raccolta del consenso scritto da clienti, dipendenti e collaboratori	Obbligatoria
Adeguamento alle misure minime di sicurezza	Obbligatoria
Redazione del Documento Programmatico sulla Sicurezza (DPS)	Obbligatoria ³

Lo Studio Parisi Presicce rimane a completa disposizione di quanti desiderino ulteriori chiarimenti in merito.

³ Per coloro che effettuano il trattamento dei dati con strumenti elettronici