

# Codice della Privacy e Documento Programmatico sulla Sicurezza (DPS)

Guida pratica di approfondimento per le aziende, per capire quali sono gli adempimenti e le norme da seguire, per essere in regola con la legge.

Il **Codice della Privacy**, entrato in vigore il 1 gennaio 2004, conferma e aggiorna la disciplina in materia di sicurezza dei dati personali e dei sistemi informatici introdotta nel 1996. In particolare evidenzia due distinti obblighi:

a) *l'obbligo più generale di ridurre al minimo determinati rischi.*

• In pratica **l'azienda deve cercare di custodire e controllare i dati personali, oggetto di trattamento, limitando al massimo il rischio di distruzione o cancellazione** anche accidentale degli stessi, e cercando di evitare di comunicarli a terzi (salvo i casi consentiti) o di utilizzati in modo illecito.

b) *nell'ambito del predetto obbligo più generale, il dovere di adottare in ogni caso le "misure minime".*

• In pratica **l'azienda deve assicurare un livello minimo di protezione dei dati personali.**

Questo livello minimo di sicurezza è chiaramente espresso nel Codice agli art. 33-34-35-36 e nell'Allegato B)

## Cosa dice la legge?

Il **Codice della Privacy**, cioè il decreto legislativo n. 196 del 30 giugno 2003 prevede nuovi adempimenti in merito alla protezione dei dati personali. Uno di questi adempimenti è **l'obbligo di redigere il DPS ovvero il Documento Programmatico sulla Sicurezza. E soddisfare tutti i "requisiti minimi" previsti dalla legge.**

## Chi deve mettersi in regola?

Le pubbliche amministrazioni (es. comuni, ospedali, scuole, enti), le aziende, i liberi professionisti, le associazioni, le cooperative. In pratica **tutti coloro che trattano dati personali** di clienti, dipendenti, fornitori, cittadini, utenti, pazienti, colleghi, soci, associati, ecc. Ovviamente gli adempimenti sono diversi a seconda delle dimensioni della struttura e della tipologia di trattamento dei dati.

## Cosa rischia chi non è in regola?

Chi non sarà in regola con la nuova normativa rischierà una sanzione penale che prevede **l'arresto sino a 2 anni o un'ammenda da 10.000 a 50.000 euro.**

## Quali sono gli adempimenti?

- **Redigere il Documento Programmatico sulla Sicurezza (DPS)**, nel quale dovrà essere specificato ad esempio il trattamento dei dati personali, l'attribuzione di compiti e responsabilità, l'analisi del rischio dei dati, l'elenco delle misure adottate atte a garantire integrità, la disponibilità e la riservatezza dei dati, la formazione del personale sui temi della sicurezza, la descrizione delle misure minime di sicurezza adottate in conformità al codice della privacy e la descrizione delle misure adottate per la cifratura dei dati sensibili/giudiziari.

- **Adottare una serie di "misure minime" di sicurezza** sia per il trattamento dei dati con strumenti elettronici che per il trattamento di dati su supporto cartaceo.

• **Se si utilizzano strumenti elettronici** si dovrà dotare il sistema di strumenti di autenticazione, redigere delle procedure per la gestione delle credenziali di autenticazione, provvedere all'aggiornamento periodico del personale preposto al trattamento dei dati e di quello addetto ai sistemi informativi, mettere in atto misure di protezione degli elaboratori rispetto al trattamento illecito dei dati e ad accessi non consentiti, effettuare procedure per il backup dei dati ed il loro ripristino e adottare tecniche di cifratura per i dati sensibili/giudiziari.

• **Se si utilizzano strumenti cartacei** si dovranno stabilire procedure per la gestione e la custodia di atti e documenti, l'analisi del rischio, la formazione del personale sui temi della sicurezza e la descrizione delle misure minime di sicurezza adottate in conformità al Codice della Privacy.

## Quali sono le scadenze?

Il decreto legislativo n. 196 del 30 giugno 2003 è entrato in vigore il 1 gennaio 2004.

**Il DPS, cioè il Documento Programmatico sulla Sicurezza, deve essere redatto entro il 31 dicembre 2004** e aggiornato ogni anno. Entro la stessa data devono essere adottate anche le misure minime di sicurezza previste dagli articoli 33, 34 e 35 del Codice della Privacy.

**Il Documento Programmatico sulla Sicurezza (DPS)** rientra tra le *“misure minime”* richieste dal Codice della Privacy e **deve essere aggiornato annualmente dal titolare del trattamento dei dati sensibili o dei dati giudiziari** e dichiarato nella relazione consuntiva del bilancio d'esercizio.

Il DPS è un documento cartaceo ufficiale di pianificazione della sicurezza dei dati aziendali che attesta quando e come la struttura informatica dell'azienda è stata adeguata alla normativa vigente.

Una copia del DPS deve essere custodita presso la sede per essere consultabile e deve essere esibita in caso di controlli. Sul sito <http://www.garanteprivacy.it> del Garante della Privacy si può trovare la guida alla compilazione del DPS e il testo integrale del Codice della Privacy.

## Codice della Privacy SICUREZZA DEI DATI E DEI SISTEMI

### Gli articoli 31 e 32 riguardanti le MISURE DI SICUREZZA

#### MISURE DI SICUREZZA

##### Art. 31 – Obblighi di sicurezza

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base 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.

##### Art. 32 – Particolari titolari

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta ai sensi dell'articolo 31 idonee misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi, l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comunicazioni elettroniche rispetto ad ogni forma di utilizzazione o cognizione non consentita.

2. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente.

3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e, ove possibile, gli utenti, se sussiste un particolare rischio di violazione della sicurezza della rete, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare ai sensi dei commi 1 e 2, tutti i possibili rimedi e i relativi costi presumibili. Analoga informativa è resa al Garante e all'Autorità per le garanzie nelle comunicazioni.

## Codice della Privacy SICUREZZA DEI DATI E DEI SISTEMI

### Gli articoli 33, 34, 35 e 36 riguardanti le MISURE MINIME DI SICUREZZA.

#### MISURE MINIME DI SICUREZZA

##### Art. 33 – Misure minime

1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, **i titolari del trattamento sono comunque tenuti ad adottare le misure minime** individuate nel presente capo o ai sensi dell'articolo 58, comma 3, **volte ad assicurare un livello minimo di protezione dei dati personali.**

##### Art. 34 – Trattamenti con strumenti elettronici

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:

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- tenuta di un aggiornato **documento programmatico sulla sicurezza**;
- 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.

##### Art. 35 – Trattamenti senza l'ausilio di strumenti elettronici

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

##### Art. 36 – Adeguamento

- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- previsione di procedure per un'adeguata custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

1. Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

## ALLEGATO B) - DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Artt. da 33 a 36 del Codice della Privacy)

### Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici.

### Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le **credenziali di autenticazione** consistono in un **codice per l'identificazione** dell'incaricato associato a una **parola chiave riservata** conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, **oppure** in una **caratteristica biometrica** dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

5. La **parola chiave**, quando è prevista dal sistema di autenticazione, è composta da **almeno otto caratteri** oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è **modificata** da quest'ultimo al primo utilizzo e successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata **almeno ogni tre mesi**.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente

riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

### Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

### Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti **contro il rischio di intrusione** e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'**attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale**.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il **salvataggio dei dati con frequenza almeno settimanale**.

## Documento programmatico sulla sicurezza

**19. 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** contenente idonee informazioni riguardo:

**19.1. l'elenco dei trattamenti** di dati personali;

**19.2. la distribuzione dei compiti e delle responsabilità** nell'ambito delle strutture preposte al trattamento dei dati;

**19.3. l'analisi dei rischi** che incombono sui dati;

**19.4. 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 e accessibilità;

**19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati** in seguito a distruzione o danneggiamento di cui al successivo punto 23;

**19.6. 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 di dati personali;

**19.7. 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;

**19.8.** per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, **l'individuazione dei criteri da adottare per la cifratura o per la separazione** di tali dati dagli altri dati personali dell'interessato.

### Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

**20.** I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

**21.** Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

**22.** I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

**23.** Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

**24.** 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.

### Misure di tutela e garanzia

**25.** Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

**26.** Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

**Trattamenti senza l'ausilio di strumenti elettronici**  
Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici.

**27.** Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

**28.** Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

**29.** L'accesso agli archivi contenenti dati sensibili o giudiziari è 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.

# CODICE SULLA PRIVACY "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI"

In vigore dal 1 gennaio 2004 [Decreto legislativo n. 196 del 30 giugno 2003]

## PARTE I - DISPOSIZIONI GENERALI

Tutti gli adempimenti e le regole del trattamento con riferimento ai settori pubblico e privato.

### • PRINCIPI GENERALI

- Art. 1 – Diritto alla protezione dei dati personali
- Art. 2 – Finalità
- Art. 3 – Principio di necessità nel trattamento dei dati
- Art. 4 – Definizioni
- Art. 5 – Oggetto ed ambito di applicazione
- Art. 6 – Disciplina del trattamento

### • DIRITTI DELL'INTERESSATO

- Art. 7 – Diritto di accesso ai dati personali ed altri diritti
- Art. 8 – Esercizio dei diritti
- Art. 9 – Modalità di esercizio
- Art. 10 – Riscontro all'interessato

### • REGOLE GENERALI PER IL TRATTAMENTO DEI DATI

- Art. 11-17 – Regole per tutti i trattamenti
- Art. 18-22 – Regole ulteriori per i soggetti pubblici
- Art. 23-27 – Regole ulteriori per privati ed enti pubblici economici

### • SOGGETTI CHE EFFETTUANO IL TRATTAMENTO

- Art. 28 – Titolare del trattamento
- Art. 29 – Responsabile del trattamento

### • SICUREZZA DEI DATI E DEI SISTEMI

#### - MISURE DI SICUREZZA

- Art. 31 – Obblighi di sicurezza
- Art. 32 – Particolari titolari

#### - MISURE MINIME DI SICUREZZA

- Art. 33 – Misure minime
- Art. 34 – Trattamenti con strumenti elettronici
- Art. 35 – Trattamenti senza l'ausilio di strumenti elettronici
- Art. 36 – Adeguamento

### • ADEMPIMENTI

- Art. 37 – Notificazione del trattamento
- Art. 38 – Modalità di notificazione
- Art. 39 – Obblighi di comunicazione
- Art. 40 – Autorizzazioni generali
- Art. 41 – Richieste di autorizzazione

## PARTE II - DISPOSIZIONI RELATIVE A SPECIFICI SETTORI

Tutti gli adempimenti e le regole del trattamento con riferimento ai settori specifici. Questa sezione, oltre a disciplinare aspetti in parte inediti (informazione giuridica, notificazioni di atti giudiziari, dati sui comportamenti debitori), completa anche la disciplina attesa da tempo per il settore degli organismi sanitari e quella dei controlli sui lavoratori.

### TRATTAMENTO IN AMBITO GIUDIZIARIO

#### • PROFILI GENERALI

- Art. 46 – Titolari dei trattamenti
- Art. 47 – Trattamenti per ragioni di giustizia
- Art. 48 – Banche di dati di uffici giudiziari
- Art. 49 – Disposizioni di attuazione

#### • MINORI

- Art. 50 – Notizie o immagini relative a minori

#### • INFORMATICA GIURIDICA

- Art. 51 – Principi generali,
- Art. 52 – Dati identificativi degli interessati

### TRATTAMENTI DA PARTE DI FORZE DI POLIZIA

#### • PROFILI GENERALI

- Art. 53 – Ambito applicativo e titolari dei trattamenti
- Art. 54 – Modalità di trattamento e flussi di dati
- Art. 55 – Particolari tecnologie
- Art. 56 – Tutela dell'interessato
- Art. 57 – Disposizioni di attuazione

### DIFESA E SICUREZZA DELLO STATO

#### • PROFILI GENERALI

- Art. 58 – Disposizioni applicabili

### TRATTAMENTI IN AMBITO PUBBLICO

#### • ACCESSO A DOCUMENTI AMMINISTRATIVI

- Art. 59 – Accesso a documenti amministrativi
- Art. 60 – Dati idonei a rivelare lo stato di salute e la vita sessuale

#### • REGISTRI PUBBLICI E ALBI PROFESSIONALI

- Art. 61 – Utilizzazione di dati pubblici

#### • STATO CIVILE, ANAGRAFI E LISTE ELETTORALI

- Art. 62 – Dati sensibili e giudiziari
- Art. 63 – Consultazione di atti

#### • FINALITÀ DI RILEVANTE INTERESSE PUBBLICO

- Art. 64 – Cittadinanza, immigrazione e condizione dello straniero
- Art. 65 – Diritti politici e pubblicità dell'attività di organi
- Art. 66 – Materia tributaria e doganale
- Art. 67 – Attività di controllo e ispettive
- Art. 68 – Benefici economici ed abilitazioni
- Art. 69 – Onorificenze, ricompense e riconoscimenti
- Art. 70 – Volontariato e obiezione di coscienza
- Art. 71 – Attività sanzionatorie e di tutela
- Art. 72 – Rapporti con enti di culto
- Art. 73 – Altre finalità in ambito amministrativo e sociale

#### • PARTICOLARI CONTRASSEGNI

- Art. 74 – Contrassegni su veicoli e accessi a centri storici

### TRATTAMENTO DI DATI PERSONALI IN AMBITO SANITARIO

#### • PRINCIPI GENERALI

- Art. 75 – Ambito applicativo
- Art. 76 – Esercenti professioni sanitarie e organismi sanitari pubblici

#### • MODALITÀ SEMPLIFICATE PER INFORMATIVA E CONSENSO

- Art. 77 – Casi di semplificazione
- Art. 78 – Informativa del medico di medicina generale o del pediatra
- Art. 79 – Informativa da parte di organismi sanitari
- Art. 80 – Informativa da parte di altri soggetti pubblici
- Art. 81 – Prestazione del consenso
- Art. 82 – Emergenze e tutela della salute e dell'incolumità fisica
- Art. 83 – Altre misure per il rispetto dei diritti degli interessati
- Art. 84 – Comunicazione di dati all'interessato

#### • FINALITÀ DI RILEVANTE INTERESSE PUBBLICO

- Art. 85 – Compiti del Servizio sanitario nazionale
- Art. 86 – Altre finalità di rilevante interesse pubblico

#### • PRESCRIZIONI MEDICHE

- Art. 87 – Medicinali a carico del Servizio sanitario nazionale
- Art. 88 – Medicinali non a carico del Servizio sanitario nazionale
- Art. 89 – Casi particolari

#### • DATI GENETICI

- Art. 90 – Trattamento dei dati genetici e donatori di midollo osseo

#### • DISPOSIZIONI VARIE

- Art. 91 – Dati trattati mediante carte
- Art. 92 – Cartelle cliniche
- Art. 93 – Certificato di assistenza al parto
- Art. 94 – Banche di dati, registri e schedari in ambito sanitario

### ISTRUZIONE

#### • PROFILI GENERALI

- Art. 95 – Dati sensibili e giudiziari
- Art. 96 – Trattamento di dati relativi a studenti

### TRATTAMENTO PER SCOPI STORICI, STATISTICI O SCIENTIFICI

#### • PROFILI GENERALI

- Art. 97 – Ambito applicativo
- Art. 98 – Finalità di rilevante interesse pubblico
- Art. 99 – Compatibilità tra scopi e durata del trattamento
- Art. 100 – Dati relativi ad attività di studio e ricerca

#### • TRATTAMENTO PER SCOPI STORICI

- Art. 101 – Modalità di trattamento
- Art. 102 – Codice di deontologia e di buona condotta
- Art. 103 – Consultazione di documenti conservati in archivi

#### • TRATTAMENTO PER SCOPI STATISTICI O SCIENTIFICI

- Art. 104 – Ambito applicativo e dati identificativi per scopi statistici o scientifici
- Art. 105 – Modalità di trattamento
- Art. 106 – Codici di deontologia e di buona condotta
- Art. 107 – Trattamento di dati sensibili
- Art. 108 – Sistema statistico nazionale
- Art. 109 – Dati statistici relativi all'evento della nascita
- Art. 110 – Ricerca medica, biomedica ed epidemiologica

#### LAVORO E PREVIDENZA SOCIALE

##### • PROFILI GENERALI

- Art. 111 – Codice di deontologia e di buona condotta
- Art. 112 – Finalità di rilevante interesse pubblico

##### • ANNUNCI DI LAVORO E DATI RIGUARDANTI PRESTATORI DI LAVORO

- Art. 113 – Raccolta di dati e pertinenza

##### • DIVIETO DI CONTROLLO A DISTANZA E TELELAVORO

- Art. 114 – Controllo a distanza
- Art. 115 – Telelavoro e lavoro a domicilio

##### • ISTITUTI DI PATRONATO E DI ASSISTENZA SOCIALE

- Art. 116 – Conoscibilità di dati su mandato dell'interessato

#### SISTEMA BANCARIO, FINANZIARIO ED ASSICURATIVO

##### • SISTEMI INFORMATIVI

- Art. 117 – Affidabilità e puntualità nei pagamenti
- Art. 118 – Informazioni commerciali
- Art. 119 – Dati relativi al comportamento debitorio
- Art. 120 – Sinistri

#### COMUNICAZIONI ELETTRONICHE

##### • SERVIZI DI COMUNICAZIONE ELETTRONICA

- Art. 121 – Servizi interessati
- Art. 122 – Informazioni raccolte nei riguardi dell'abbonato o dell'utente
- Art. 123 – Dati relativi al traffico
- Art. 124 – Fatturazione dettagliata
- Art. 125 – Identificazione della linea
- Art. 126 – Dati relativi all'ubicazione
- Art. 127 – Chiamate di disturbo e di emergenza
- Art. 128 – Trasferimento automatico della chiamata
- Art. 129 – Elenchi di abbonati
- Art. 130 – Comunicazioni indesiderate
- Art. 131 – Informazioni ad abbonati ed utenti
- Art. 132 – Conservazione di dati di traffico per altre finalità

##### • INTERNET E RETI TELEMATICHE

- Art. 133 – Codice di deontologia e di buona condotta

##### • VIDEOSORVEGLIANZA

- Art. 134 – Codice di deontologia e di buona condotta

#### LIBERE PROFESSIONI E INVESTIGAZIONE PRIVATA

##### • PROFILI GENERALI

- Art. 135 – Codice di deontologia e di buona condotta

#### GIORNALISMO ED ESPRESSIONE LETTERARIA ED ARTISTICA

##### • PROFILI GENERALI

- Art. 136 – Finalità giornalistiche e altre manifestazioni del pensiero
- Art. 137 – Disposizioni applicabili
- Art. 138 – Segreto professionale

##### • CODICE DI DEONTOLOGIA

- Art. 139 – Codice di deontologia relativo ad attività giornalistiche

#### MARKETING DIRETTO

##### • PROFILI GENERALI

- Art. 140 – Codice di deontologia e di buona condotta

#### PARTE III - TUTELA DELL'INTERESSATO E SANZIONI

Le tutele amministrative e giurisdizionali con il consolidamento delle sanzioni amministrative e penali e con le disposizioni relative all'Ufficio del Garante.

#### TUTELA AMMINISTRATIVA E GIURISDIZIONALE

##### • CAPO I – TUTELA DINANZI AL GARANTE – PRINCIPI GENERALI

- Art. 141 – Forme di tutela

##### • TUTELA AMMINISTRATIVA

- Art. 142 – Proposizione dei reclami
- Art. 143 – Procedimento per i reclami
- Art. 144 – Segnalazioni

##### • TUTELA ALTERNATIVA A QUELLA GIURISDIZIONALE

- Art. 145 – Ricorsi
- Art. 146 – Interpello preventivo
- Art. 147 – Presentazione del ricorso
- Art. 148 – Inammissibilità del ricorso
- Art. 149 – Procedimento relativo al ricorso
- Art. 150 – Provvedimenti a seguito del ricorso
- Art. 151 – Opposizione

##### • CAPO II – TUTELA GIURISDIZIONALE

- Art. 152 – Autorità giudiziaria ordinaria)

#### L'AUTORITÀ

##### • IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

- Art. 153 – Il Garante
- Art. 154 – Compiti

##### • L'UFFICIO DEL GARANTE

- Art. 155 – Principi applicabili
- Art. 156 – Ruolo organico e personale

##### • ACCERTAMENTI E CONTROLLI

- Art. 157 – Richiesta di informazioni e di esibizione di documenti
- Art. 158 – Accertamenti
- Art. 159 – Modalità
- Art. 160 – Particolari accertamenti

#### SANZIONI

##### • VIOLAZIONI AMMINISTRATIVE

- Art. 161 – Omessa o inidonea informativa all'interessato
- Art. 162 – Altre fattispecie
- Art. 163 – Omessa o incompleta notificazione
- Art. 164 – Omessa informazione o esibizione al Garante
- Art. 165 – Pubblicazione del provvedimento del Garante
- Art. 166 – Procedimento di applicazione

##### • ILLECITI PENALI

- Art. 167 – Trattamento illecito di dati
- Art. 168 – Falsità nelle dichiarazioni e notificazioni al Garante
- Art. 169 – Misure di sicurezza
- Art. 170 – Inosservanza di provvedimenti del Garante
- Art. 171 – Altre fattispecie
- Art. 172 – Pene accessorie

#### DISPOSIZIONI MODIFICATIVE, ABROGATIVE, TRANSITORIE E FINALI

##### • DISPOSIZIONI DI MODIFICA

- Art. 173 – Convenzione di applicazione dell'Accordo di Schengen
- Art. 174 – Notifiche di atti e vendite giudiziarie
- Art. 175 – Forze di polizia
- Art. 176 – Soggetti pubblici
- Art. 177 – Disciplina anagrafica dello stato civile e delle liste elettorali
- Art. 178 – Disposizioni in materia sanitaria
- Art. 179 – Altre modifiche

##### • DISPOSIZIONI TRANSITORIE

- Art. 180 – Misure di sicurezza
- Art. 181 – Altre disposizioni transitorie
- Art. 182 – Ufficio del Garante

##### • ABROGAZIONI

- Art. 183 – Norme abrogate

##### • NORME FINALI

- Art. 184 – Attuazione di direttive europee
- Art. 185 – Allegazione dei codici di deontologia e di buona condotta
- Art. 186 – Entrata in vigore

**Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
Tel: 001 408 526-4000  
001 800 553-NETS (6387)  
Fax: 001 408 526-4100  
Sito World Wide Web:  
<http://www.cisco.com>

**Sede europea**

Cisco Systems Europe  
11 rue Camille Desmoulins  
92782 Issy-les-Moulineaux  
Cedex 9, France  
Tel: 0033 1 58 04 60 00  
Fax: 0033 1 58 04 61 00

**Sede italiana**

Cisco Systems Italy  
Via Torri Bianche, 7  
20059 Vimercate (MI)  
Tel: 039 6295 1  
Fax: 039 6295 299  
Sito World Wide Web:  
<http://www.cisco.com/it>

**Filiale di Roma**

Cisco Systems Italy  
Via del Serafico, 200  
00142 Roma  
Tel: 06 516451  
Fax: 06 51645001

**Le filiali Cisco Systems nel mondo sono oltre 200. Gli indirizzi e i numeri di telefono e fax sono disponibili sul sito Cisco Connection Online all'indirizzo <http://www.cisco.com/go/offices>**

Arabia Saudita • Argentina • Australia • Austria • Belgio • Brasile • Bulgaria • Canada • Cile • Cina • Colombia • Corea • Costa Rica • Croazia • Danimarca • Emirati Arabi • Filippine • Finlandia • Francia • Germania • Giappone • Gran Bretagna • Grecia • Hong Kong • India • Indonesia • Irlanda • Israele • Italia • Lussemburgo • Malesia • Messico • Norvegia • Nuova Zelanda • Olanda • Perù • Polonia • Portogallo • Portorico • Romania • Repubblica Ceca • Russia • Scozia • Singapore • Slovacchia • Slovenia • Spagna • Stati Uniti • Sud Africa • Svezia • Svizzera • Thailandia • Taiwan • Turchia • Ucraina • Ungheria • Venezuela • Vietnam • Zimbabwe