

DL 30/6/2003 n. 196 nuovo Codice di Sicurezza

Note sulla creazione e gestione del Documento Programmatico sulla Sicurezza e sulle altre misure richieste dalla legge (con riferimento ai Dati Personali)

Premessa

Prima di entrare nei dettagli della legislazione vigente in materia (Codice di Sicurezza DL 30/6/2003 n. 196), valgono le **considerazioni generali** di seguito riportate.

1. La creazione del **Documento Programmatico** è sancita nell'**art. 34 punto g) del Codice di Sicurezza** DL 30/6/2003 n. 196 e le specifiche relative al suo contenuto sono indicate in diversi punti dell'allegato B del Codice stesso (Disciplinare Tecnico in materia di misure minime di Sicurezza – artt. da 33 a 36 del Codice).
2. La **Relazione accompagnatoria** del Codice in oggetto ne prevede **aggiornamenti periodici** con decreti congiunti del Ministero della Giustizia e del Ministero della Innovazione Tecnologica (art. 36) che, di conseguenza, dovranno essere seguiti con attenzione nel tempo. Di qui anche la richiesta della **compilazione di una versione aggiornata annua entro il 31/3** (punto 19 – All. B).
3. In modo più completo, nella Relazione accompagnatoria alla legge stessa si legge specificamente che "Oltre alle altre definizioni sono dati personali anche quelli relativi all'uso di servizi di comunicazione elettronica" e si evidenzia quanto segue.
 - a. Distinzione fra elaboratori non accessibili e elaboratori in rete (disponibile o non disponibile al pubblico)
 - b. Obbligo di fare copie delle password
 - c. Obbligo autenticazione IT
 - d. Aggiornamento periodico compiti incaricati
 - e. Obbligo protezione strumenti elettronici e dati rispetto a trattamenti illeciti e accessi non consentiti
 - f. Aggiornamento DPSS
 - g. Cifratura dati salute e sessuali
 - h. Documento a data certa per impedimenti alle misure minime di sicurezza (ad ogni modo tempo un anno per adeguare i propri elaboratori!)
 - i. Scadenze semestrali per sw anti intrusione (all. B 16), annuali per autorizzazioni, lista incaricati (anche per classi omogenee di incarico e profili relativi – all. B 15), aggiornamento programmi
 - j. Salvataggio dati almeno settimanale (all. B 18)

qubi s.r.l.

sede Legale : Via Ozanam, 2- 24126 - Bergamo

Sede Operativa Via F.lli Bandiera, 2 - 24048- TREVILOLO - (BG) - Italy

Tel. ++39 35 20 13 90 (2 linee r.a.) - Fax ++39 35 622 60 85

P.I. 02826610160 - REA 3264221/2000 - C.F. 04571250481 - Cap. Soc. 50.00 Euro i.v.

<http://www.qubi.it> - <http://www.qubinet.it>

4. Il Codice di Sicurezza DL 30/6/2003 n. 196 è *entrato in vigore il 1/1/2004 con obbligo di notifica dei dati personali al Garante (art. 37), fatta eccezione per i dati attinenti ai dipendenti, entro il 30/4* (art. 181 - punto c).

5. In particolare il Codice si applica (art. 4) ai seguenti *soggetti*:
 - “persone fisiche
 - giuridiche
 - Pubblica Amministrazione (centrale e locale)
 - “qualsiasi altro ente od organismo cui competono le decisioni in ordine al trattamento di dati personali, ivi compreso il profilo della sicurezza”.

6. I dati di riferimento del Codice di Sicurezza sono:
 - dati personali
 - dati sensibili
 - dati giudiziari

7. Sono definiti come **dati personali** (art. 4): *“qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale”*.

8. In particolare tali dati personali possono essere oggetto di trattamenti sia all’interno del soggetto che inseriti in comunicazioni attraverso la posta elettronica.

9. Gli art 7, 10 e segg. definiscono i diritti dell’interessato, il diritto al riscontro e quando deve essere richiesto il consenso al trattamento dei dati personali.

10. **Più specificamente** (art. 37- a - d - e - f) si definiscono dati personali (per i quali occorre notificarne il trattamento al Garante)(entro il 30/4– art. 181 c) “dati che:
 - a. indicano la *posizione geografica di persone o oggetti* (quindi tutte le informazioni di tipo anagrafico)
 - b. dati volti a definireo ad analizzare *le scelte dell’interessato* (ad es. tutte le sue scelte di acquisto, le sue risposte a test e/o offerte inviate, i mezzi di risposta utilizzati, le opzioni commerciali selezionate, ecc.)
 - c. dati relativi alla *fornitura di beni*
 - d. dati necessari ai fini della *selezione del personale*
 - e. dati registrati in apposite banche e..... relativi al rischio sulla *solvibilità economica, relativi alla situazione patrimoniale e/o al corretto adempimento di obbligazioni commerciali* (quindi la maggior parte delle informazioni di tipo amministrativo contabile riguardanti clienti, fornitori, ecc.)

11. Inoltre l’art. 126 Titolo X: **“Comunicazione elettronica”**, definisce personali i dati relativi all’ubicazione dell’apparato terminale dell’utente di un servizio di comunicazione elettronica accessibile al pubblico.

12. Gli art. 130 e 140 forniscono regole di comportamento per le comunicazioni pubblicitari e promozionali e per il marketing diretto (via Internet).
13. Gli art. 11, 114 e 134 definiscono i principi ai quali attenersi per la videosorveglianza dei lavoratori.
14. In particolare per i *minori* (art. 50 del Codice “notizie ... idonee ad identificare un minore”) si applicano le limitazioni previste dal DPR 448 del 22/9/88.
15. Le indicazioni in tema di definizione di *argomenti* da inserire direttamente nel **Documento Programmatico sulla Sicurezza** sono definite al punto 19 All. B, così come la periodicità degli aggiornamenti e le altre misure minime per trattamenti elettronici (art. 34 Codice e punti diversi in All. B).

Altri adempimenti di legge, sempre in termini di documentazione, sono previsti ai punti 1-18 e 25 dello stesso Allegato B.

1. Il **contenuto del Documento Programmatico** suddetto dovrà soprattutto essere descrittivo delle misure adottate rinviando ad allegati specifici i dettagli tecnici relativi alle diverse misure di sicurezza attivate.
2. Si dovranno ancora tenere presenti le principali differenze, in termini di compiti e di responsabilità delle *figure professionali aziendali coinvolte (titolare, responsabile della sicurezza, incaricati del trattamento dei dati)*, rispetto al disposto del precedente DPR 318/99 (art. 4 e segg. del Codice di Sicurezza).

A questo scopo vedasi la definizione delle stesse e l'obbligatorietà o meno della loro nomina (agli artt.4 e segg. del Codice di Sicurezza DL 30/6/2003 n. 196).

3. Infine si dovrà tenere presente, dopo la prima stesura, la creazione di **una nuova versione del Documento Programmatico entro il 31 marzo di ogni anno** ed in particolare si deve fare riferimento all'avvenuto aggiornamento nella **nota accompagnatoria di bilancio** da parte “del titolare anche attraverso il responsabile” (punti 19 e 26 all. B).
4. Infine, nelle note presenti, **non** si fa volutamente riferimento agli obblighi specifici attinenti altri **dati (sensibili, giudiziari, sanitari, ecc.)** applicabili solo a specifiche organizzazioni operanti prevalentemente nel settore della Pubblica Amministrazione Centrale o Locale. Per tali dati e per i relativi adempimenti di legge si rimanda a quanto previsto nel Codice di Sicurezza – art. 51 e segg.

Documento Programmatico sulla Sicurezza

Nota introduttiva

Il Documento Programmatico di seguito dettagliato secondo le disposizioni di legge, dovrà:

- *essere redatto dal titolare o dal responsabile del trattamento di dati*
- *essere approvato dal Consiglio di Amministrazione*
- *ne dovrà essere confermata la stesura annuale nella relazione accompagnatoria del bilancio (All. B – punto 26)*

Il disposto di legge

L'allegato B del Codice di Sicurezza (Disciplinare tecnico in materia di misure minime di sicurezza), al punto 19 - Documento Programmatico sulla Sicurezza - prevede che lo stesso sia composto dei punti sotto elencati per i quali si suggeriscono i contenuti di seguito indicati:

1. Elenco dei trattamenti di dati personali (all. B - 19.1)

Al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle tipologie di trattamenti effettuati.

Ogni banca di dati o archivio devono essere classificati in relazione alle informazioni in essi contenute.

2. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati (all. B - 19.2)

L'art. 4 del Codice definisce le figure suddette (titolare, responsabile della sicurezza dei dati, incaricato del trattamento dei dati), mentre negli artt. successivi si precisa che:

- la nomina di uno o più responsabili della sicurezza informatica è facoltativa
- l'affidamento delle operazioni di trattamento dei dati a figure denominate incaricati non prevede la loro responsabilità diretta per l'adozione di misure minime di sicurezza

Da ciò consegue che è necessario indicare, con riferimento a quanto specificato nel punto precedente (vale a dire ai diversi trattamenti di dati personali):

- i compiti e le responsabilità delle figure professionali di titolare, responsabile/i, incaricato/i del trattamento dei dati personali.

In particolare si suggerisce la redazione e l'inserimento nel Documento Programmatico:

- del documento di nomina delle diverse figure professionali con le seguenti precisazioni

Il Titolare del trattamento dei dati deve informare ciascun Responsabile del trattamento dei dati, delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore.



A ciascun Responsabile del trattamento il Titolare del trattamento deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina del Responsabile del trattamento è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina del Responsabile del trattamento può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

Ai Responsabili del trattamento è affidato il compito di nominare, con comunicazione scritta, uno o più Incaricati del trattamento dei dati.

La nomina di ciascun Incaricato del trattamento dei dati deve essere effettuata con una lettera di incarico in cui sono specificati i compiti che gli sono affidati (a meno che gli stessi siano già stati precisati nella lettera di assunzione o di nomina ad un nuovo incarico aziendale).

Gli Incaricati del trattamento devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

Agli Incaricati deve essere assegnata una parola chiave e un codice identificativo personale.

La nomina degli Incaricati del trattamento deve essere controfirmata dall'interessato per presa visione e copia della stessa e deve essere conservata a cura del Responsabile del trattamento per la sicurezza dei dati in luogo sicuro.

Agli Incaricati del trattamento il Responsabile del trattamento per la sicurezza dei dati deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina degli Incaricati è a tempo indeterminato, e decade per revoca, per sue dimissioni, o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.

- del documento di assegnazione di compiti e responsabilità tenendo presente che:

E' onere del Titolare del trattamento individuare, nominare e incaricare per iscritto uno o più Responsabili del trattamento dei dati, che assicurino e garantiscano che vengano adottate le misure di sicurezza ai sensi dell'art. 15, commi 1 e 2, della legge 675/1996.

Il Titolare del trattamento affida al Responsabile del trattamento dei dati il compito di adottare le misure tese a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previa idonee istruzioni fornite per iscritto.

In relazione all'attività del Titolare del trattamento, è prevista la nomina di uno o più Responsabili del trattamento, con compiti diversi a seconda delle funzioni svolte.

Il Titolare del trattamento affida ai singoli Responsabili del trattamento l'onere di individuare, nominare ed indicare per iscritto uno o più Incaricati del trattamento.



Il Responsabile del trattamento dei dati ha il compito di:

- • Redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione connessi in rete pubblica, nonché l'elenco delle tipologie dei trattamenti effettuati;
- • Attribuire, con l'ausilio degli Amministratori di sistema, ad ogni Utente (USER) o incaricato un Codice identificativo personale (USER-ID) per l'utilizzazione dell'elaboratore, che deve essere individuale e non riutilizzabile;
- • Autorizzare i singoli incaricati del trattamento e della manutenzione, nel caso di trattamento di dati sensibili e giudiziari, qualora si utilizzino elaboratori accessibili in rete; per gli stessi dati, qualora il trattamento sia effettuato tramite elaboratori accessibili in rete disponibili al pubblico, saranno oggetto di autorizzazione anche gli strumenti da utilizzare;
- • Verificare, con l'ausilio degli amministratori di sistema, con cadenza almeno semestrale, l'efficacia dei programmi di protezione ed antivirus, nonché definire le modalità di accesso ai locali e le misure indicate in seguito;
- • Garantire che tutte le misure di sicurezza riguardanti i dati in possesso dell'Azienda siano applicate all'interno dell'Azienda stessa ed eventualmente al di fuori della stessa, qualora siano cedute a soggetti terzi quali Responsabili del trattamento tutte o parte delle attività di trattamento;
- • Informare il Titolare nella eventualità che si siano rilevati dei rischi.
- • Compilare il documento di eventuale variazione dei suddetti compiti e responsabilità
- • Redigere il documento di decadenza dai compiti indicati a seguito di variazione di attività o cessazione del proprio rapporto di lavoro.

3. Analisi dei rischi che incombono sui dati (all. B - 19.3)

L'argomento è di non facile interpretazione.

I rischi che incombono sui dati in esame sono strettamente dipendenti da una serie notevole di fattori quali:

- l'entità dei dati gestiti
- la frequenza di trattamento
- le tecniche di salvataggio periodico dei dati
- le tecnologie informatiche presenti in azienda
- il numero di utenti (interni ed esterni) che accedono a tali dati
- le modalità di aggiornamento delle Basi Dati che li contengono

qubi s.r.l.

sede Legale : Via Ozanam, 2- 24126 - Bergamo

Sede Operativa Via F.lli Bandiera,2 - 24048- TREVILOLO - (BG) - Italy

Tel. ++39 35 20 13 90 (2 linee r.a.) - Fax ++39 35 622 60 85

P.I. 02826610160 - REA 3264221/2000 - C.F. 04571250481 - Cap. Soc. 50.00 Euro i.v.

<http://www.qubi.it> - <http://www.qubinet.it>



- ..e altri ancora quali le modalità di erogazione del servizio (interno, esterno, on line, web, batch, ecc.), l'importanza del trattamento in oggetto per il settore di attività e/o per l'azienda specifica e così via.

Sulla scorta di quanto sopra, si suggerisce di indicare:

- il rischio sia in termini descrittivi che di valore (o stima) dello stesso e di probabilità di accadimento
- le misure adottate al fine di ridurlo per la perdita (totale o parziale) dei dati trattati (v. punto successivo)
- il rinvio ad eventuali documenti tecnici che descrivano in dettaglio le misure stesse
- il rischio residuo che permane per ogni trattamento degli stessi dati
- il valore di tale rischio

In particolare per quanto concerne la *Protezione da virus informatici*, al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita di dati a causa degli stessi, si suggerisce che il titolare o il responsabile della sicurezza dei dati stabilisca, con il supporto tecnico dell'Amministratore di sistema, quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.

4. Misure per l'integrità e la disponibilità dei dati (all. B - 19.4.1)

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, il Responsabile del trattamento dei dati stabilisce, con il supporto tecnico dell'Amministratore di sistema, la periodicità con cui devono essere effettuate le copie di sicurezza delle banche di dati trattati.

I criteri devono essere definiti dall'Amministratore di sistema in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In particolare per ogni banca di dati devono essere definite diverse specifiche.

5. Protezione delle aree e dei locali (all. B - 19.4.2)

Al titolare o al responsabile della sicurezza dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle aree nelle quali viene effettuato il trattamento dei dati, nominando un apposito Incaricato, con il compito di controllare direttamente i sistemi, le apparecchiature, o i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.

Il titolare o il responsabile della sicurezza dei dati deve definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.

Il titolare o il responsabile della sicurezza dei dati deve informare con una comunicazione scritta l'Incaricato dell'ufficio dei compiti che gli sono stati affidati utilizzando apposito modulo.



In termini di documentazione si tratta di descrivere, in modo esauriente e completo, tutte le eventuali misure adottate per le aree aziendali contenenti dati personali sia in formato elettronico (.....) sia in formato cartaceo (.....).

6. Criteri e modalità di ripristino della disponibilità dei dati in caso di distruzione o danneggiamento (all. B - 19.5)

L'Amministratore di sistema è responsabile della custodia e della conservazione di supporti utilizzati per il back-up dei dati.

7. Previsione di interventi formativi degli incaricati del trattamento (all. B – 19.6)

Al titolare o al responsabile della sicurezza dei dati è affidato il compito di verificare ogni anno, le necessità di formazione del personale incaricato.

Per ogni incaricato del trattamento il titolare o il responsabile della sicurezza dei dati definisce, sulla base dell'esperienza e delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessaria una formazione tecnica adeguata, utilizzando apposito modulo che deve essere trasmesso in copia controllata al titolare o al responsabile della sicurezza dei dati.

8. Criteri per le misure minime di sicurezza in caso di trattamenti esterni di dati personali (all. B – 19.7)

La normativa in materia prevede che:

Il Titolare del trattamento può decidere di affidare il trattamento dei dati in tutto o in parte a soggetti terzi, in outsourcing, nominandoli Responsabili del trattamento.

In questo caso devono essere specificati i soggetti interessati e i luoghi dove fisicamente avviene il trattamento dei dati stessi.

Nel caso in cui questi non vengano espressamente nominati, i Responsabili del trattamento in outsourcing ai sensi dell'art. 8 della legge 657/96 devono intendersi autonomi titolari del trattamento e quindi soggetti ai corrispettivi obblighi, e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.

qubi s.r.l.

sede Legale : Via Ozanam, 2- 24126 - Bergamo

Sede Operativa Via F.lli Bandiera,2 - 24048- TREVILOLO - (BG) - Italy

Tel. ++39 35 20 13 90 (2 linee r.a.) - Fax ++39 35 622 60 85

P.I. 02826610160 - REA 3264221/2000 - C.F. 04571250481 - Cap. Soc. 50.00 Euro i.v.

<http://www.qubi.it> - <http://www.qubinet.it>

Altre misure minime per trattamenti con strumenti elettronici

Come già accennato l'art. 34 del Codice l'All. B prevedono una serie di misure minime che dovranno essere adottate e documentate dalle aziende a completamento del Documento Programmatico.

Vediamole in dettaglio.

1. Sistema di autenticazione delle informazioni (all. B – 1-11)

La legge specifica quanto segue (con conseguente necessità di approntare, da parte dell'azienda, i necessari interventi oltre all'opportuna documentazione a supporto) con riferimento ad ogni tipo di trattamento (ne consegue che le stesse informazioni devono essere ripetute sia per tutte le applicazioni di trattamento di dati personali, sia perché gli incaricati possono essere diversi, sia perché gli stessi possono aver ricevuto credenziali diverse):

- ogni incaricato al trattamento dei dati personali (quindi personale operativo della Direzione sistemi, personale esterno, utenti dei sistemi) deve aver ricevuto “credenziali di autenticazione che consentono il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti”(punto 1)

Per redigere l'elenco degli Incaricati del trattamento si suggerisce di utilizzare un apposito modulo, che dovrà essere conservato a cura del titolare o del responsabile della sicurezza dei dati in luogo sicuro ed essere trasmesso in copia controllata.

Ciò premesso si deve quindi documentare come l'azienda ha provveduto concretamente, per ogni trattamento dei dati personali, ad ottemperare al disposto degli specifici articoli di legge più sopra indicati.

2. Sistema di autorizzazione (all. B – 12-14)

In generale al punto 12 si richiedono profili di autorizzazione quando gli incaricati hanno accesso a funzionalità diverse dei trattamenti dei dati personali.

3. Lista di tutti gli incaricati al trattamento dei dati personali (Direzione sistemi, persone esterne, utenti) o di gruppi degli stessi (All. B - punto 15)

Il titolare o il responsabile della sicurezza dei dati, in accordo con l'Amministratore di sistema, deve definire le modalità di assegnazione dei nomi identificativi per consentire a ciascun Incaricato del trattamento di accedere ai sistemi di trattamento delle banche di dati.

4. Descrizione del sw anti intrusione utilizzato per evitare il danneggiamento dei dati personali (All. B - punto 16)

5. Documentazione degli aggiornamenti dei programmi “volti a prevenire la vulnerabilità di strumenti elettronici e a correggere difetti” (All. B - punto 17)

All'Amministratore di sistema è affidato il compito di verificare ogni anno, la situazione delle applicazioni installate sulle apparecchiature con cui vengono trattati i dati.

6. Le procedure di salvataggio dei dati (che devono avere frequenza almeno settimanale) (All. B - punto 18)

qubi s.r.l.

sede Legale : Via Ozanam, 2- 24126 - Bergamo

Sede Operativa Via F.lli Bandiera, 2 - 24048- TREVILOLO - (BG) - Italy

Tel. ++39 35 20 13 90 (2 linee r.a.) - Fax ++39 35 622 60 85

P.I. 02826610160 - REA 3264221/2000 - C.F. 04571250481 - Cap. Soc. 50.00 Euro i.v.

<http://www.qubi.it> - <http://www.qubinet.it>



Le procedure di salvataggio dei dati personali riguardano tutti gli archivi interessati dal trattamento degli stessi.

Per ogni archivio deve essere, di conseguenza, descritta la procedura adottata ed in particolare devono essere coperti diversi punti.

7. Dichiarazione scritta della conformità degli interventi esterni (All. B – punto 25)

Risorse esterne alla struttura che operano sui mezzi elettronici del soggetto, devono descrivere l'intervento effettuato e attestarne l'esecuzione in conformità a tutte le disposizioni dell'All. B.

8. Trattamento dati personali senza l'ausilio di strumenti elettronici (art. 35 del Codice di Sicurezza)

A completamento di quanto predisposto per il trattamento elettronico dei dati, la legge prevede anche in questo caso alcune misure minime (che devono essere opportunamente documentate).

Notificazione al Garante

La legge prevede, infine, (art. 37) la notificazione al Garante dei dati personali (come più sopra indicato), la cui notificazione sarà inserita in un pubblico registro consultabile elettronicamente.

Tale comunicazione deve avvenire (art. 181 - c) entro il **31/03**.

Le modalità di notificazione sono precisate nell'art. 38 e segg. del Codice di Sicurezza.

In una sua newsletter del luglio 2003 il Garante (ora non più denominato Garante per la privacy bensì Garante per la protezione dei dati personali) precisa che la notificazione è dovuta da parte delle aziende che, con strumenti elettronici :

- utilizzano la profilazione dei consumatori
- usano dati per la selezione del personale
- fanno ricerche di marketing
- usano informazioni commerciali relative alla solvibilità

Adempimenti non previsti dal DPR 318/99

Per gli adempimenti non previsti dal DPR 318/99 la data di scadenza è stata fissata al **31/12/2004** (si precisa che il Documento Programmatico sulla Sicurezza non rientra in questa dilazione).

Controlli e sanzioni

La materia è trattata in modo molto dettagliato nella Parte III del Codice: Tutela dell'interessato e sanzioni (artt. 141 e segg.).

In sintesi si prevede quanto segue:

- art. 158 – 2: il **Garante si avvale di altri organismi statali (v. convenzione 10/02 con GGFF)** per effettuare i controlli
- art. 161: qualora **non** sia stata data **comunicazione agli interessati circa la natura e l'utilizzo dei propri dati** è prevista una sanzione da 3.000 a 30.000 €
- art. 162: qualora siano stati **ceduti a terzi senza autorizzazione i dati personali** trattati è prevista una sanzione da 5.000 a 30.000 €
- art. 163: **l'omessa o incompleta notifica al Garante** (v. sopra) comporta una sanzione da 10.000 a 60.000 €. Una **falsa notifica** comporta una pena da 6 mesi a 3 anni di reclusione.
- art. 164: **l'omessa o incompleta esibizione all'autorità controllante** dei documenti richiesti prevede una sanzione da 4.000 a 24.000 €
- art. 167: il **trattamento illecito dei dati personali** prevede una reclusione da 6 mesi a 3 anni
- art. 169: **la mancata adozione delle misure minime di sicurezza** comporta una pena da 10.000 a 50.000 € ed il blocco del trattamento. L'adempimento entro 60 giorni dall'avvenuto controllo comporta la riduzione dell'ammenda ad ¼ di quella stabilita. In ogni caso il tempo massimo concesso per l'adempimento è di 6 mesi.

Oltre a quanto sopra indicato, l'articolo fa riferimento alla Legge 547/93 “ Crimini informatici commessi da dipendenti ed addebitabili all'azienda” e all'art. 2050 Cod. civile “Responsabilità oggettiva per l'esercizio di attività pericolosa” (il trattamento dei dati è giudicato tale dallo stesso articolo).

Tali norme prevedono:

- **Sanzioni a seguito di controllo ispettivo della GGFF (recente passaggio di responsabilità – v. GU 10/02) fino a 124.000 €.**

art. 170: inosservanza provvedimento Garante su **dati sensibili**(ex art. 26 comma 2): reclusione da 3 mesi a 2 anni.