sistemi
Professione Informatica

Le novità e gli adempimenti previsti dal nuovo Codice della *privacy*

SCHEDE
DI AGGIORNAMENTO
marzo 2004

ESTRATTO

EUTEKNE

Le novità e gli adempimenti previsti dal nuovo Codice della *privacy*

di Massimo Negro*[1] *e Vittorio Serito

Con il DLgs. 30.6.2003 n. 196 è stato approvato il nuovo Codice in materia di protezione dei dati personali, che raccoglie e riorganizza la disciplina in materia di tutela della *privacy* emanata a partire dalla L. 31.12.96 n. 675.

Il Codice è entrato in vigore l'1.1.2004 e contiene importanti novità sia come disciplina sia come adempimenti.

L'aspetto che ha subito le maggiori innovazioni, con rilevanti ricadute anche in relazione all'attività degli studi professionali, riguarda la disciplina delle misure minime di sicurezza.

La presente scheda intende:

- effettuare una breve analisi delle novità apportate dal Codice alla disciplina di tutela della privacy;
- fornire alcuni materiali pratici per adempiere agli obblighi previsti dalla nuova normativa.

In pratica, una volta esaminate le nuove disposizioni, per la maggior parte dei titolari occorrerà:

a. **aggiornare i riferimenti normativi** nei modelli di informativa e di richiesta di consenso dell'interessato;
b. **modificare le misure di sicurezza**, adeguandole ai nuovi requisiti minimi;
c. **predisporre il documento programmatico sulla sicurezza**;
d. **indicare, nella relazione accompagnatoria al bilancio**, ove obbligatoria, l'avvenuta redazione o aggiornamento del suddetto documento programmatico sulla sicurezza.

Il secondo e il terzo adempimento dovranno essere effettuati, perlopiù, entro il prossimo 30.6.2004; in caso di inosservanza si può incorrere in pesanti sanzioni pecuniarie e penali.

La normativa, pur avendo finalità di razionalizzazione e di semplificazione, appare riferita soprattutto a realtà di grandi dimensioni, per cui, in sede di applicazione pratica a studi professionali e a piccole e medie imprese, appare eccessivamente onerosa, specie per gli aspetti burocratici delle misure minime di sicurezza.

Le sanzioni non appaiono poter essere adeguatamente graduate in funzione della gravità della violazione, specie ove abbiano a sanzionare l'inosservanza di semplici obblighi formali.

indice

[1] m.negro@eutekne.it.

normativa

DLgs. 30.6.2003 n. 196 (nuovo Codice in materia di protezione dei dati personali)
DL 24.12.2003 n. 354 convertito nella L. 26.2.2004 n. 45 (prime modifiche al nuovo Codice della *privacy*)
L. 31.12.96 n. 675 (precedente disciplina di tutela del trattamento dei dati personali)
DPR 28.7.99 n. 318 (precedente disciplina sulle misure "minime" di sicurezza per il trattamento dei dati personali)
DPR 31.3.98 n. 501 (regolamento sull'organizzazione ed il funzionamento dell'Ufficio del Garante della *privacy*)
Provvedimenti Garante per la protezione dei dati personali 31.1.2002 (approvazione delle "autorizzazioni *standard*")
Provvedimento Garante per la protezione dei dati personali 24.6.2003 (proroga delle "autorizzazioni *standard*")[2]

dottrina

Atelli M. "Quando il cittadino «bussa» l'archivio deve aprire le porte", *Il Sole - 24 Ore*, *Documenti* 15.12.2003, p. 13
Atelli M. "Nella Ue senza limiti trasferimenti di dati all'estero", *Guida Normativa*, Dossier mensile n. 1, gennaio 2004, p. 140
Berghella F. "Nuove misure per il trattamento dei dati", *@lfa Il Sole - 24 Ore*, 10.7.2003, p. 6
Berghella F. "Più tutele con il Codice", *@lfa Il Sole - 24 Ore*, 10.7.2003, p. 6
Berghella F. "Guida pratica alle nuove misure di sicurezza per la privacy", Bancaria Editrice, Roma, 2003
Baffigo L. "Anche la password del Pc deve rispettare regole precise", *Il Sole - 24 Ore*, *Documenti* 15.12.2003, p. 6
Baffigo L. "Il codice puntualizza la sicurezza nei flussi di dati", *Guida Normativa*, Dossier mensile n. 1, gennaio 2004, p. 118
Cherchi A. "Un Testo unico mette ordine in otto anni di leggi sulla privacy", *Il Sole - 24 Ore*, 9.5.2003, p. 31
Cherchi A. "Un Testo unico per la privacy", *Il Sole - 24 Ore*, 28.6.2003, p. 23
Cherchi A. "Il Codice apre alla semplificazione", *Il Sole - 24 Ore*, 14.7.2003, p. 21
Ciccia A. "Una privacy leggera per le imprese", *Italia Oggi*, 28.6.2003, p. 20
Ciccia A. "Il consenso viaggia su doppio binario", *Italia Oggi*, 14.7.2003, p. 33

[2] Si segnala che l'Ufficio del Garante ha sede in Piazza di Monte Citorio 121, 00186, Roma; telefono 06696771, *fax* 0669677785, sito *internet www.garanteprivacy.it*, *e-mail garante@garanteprivacy.it* oppure *urp@garanteprivacy.it* (ufficio relazioni con il pubblico). Presso tale sito è disponibile il testo integrale del DLgs. 196/2003, degli altri atti normativi e dei chiarimenti del Garante, nonché la documentazione e le istruzioni per effettuare gli adempimenti previsti dalla disciplina sulla *privacy*.

Ciccia A. “La privacy ora è un diritto garantito”, *Italia Oggi*, 30.7.2003, p. 2
Ciccia A. “Codice della privacy, tutti gli adempimenti per le imprese”, *Italia Oggi*, 29.12.2003, p. 16
Ciccia A. “Da rifare tutte le notifiche”, *Italia Oggi*, 3.1.2004, p. 33
Finocchiaro G. “Definiti i trattamenti a notifica obbligatoria”, *Il Sole - 24 Ore*, 30.7.2003, p. 19
Finocchiaro G. “Nuove misure minime di sicurezza entro il 30 giugno 2004”, *Il Sole - 24 Ore*, 30.7.2003, p. 19
Finocchiaro G. “La privacy trova il riordino”, *Il Sole - 24 Ore*, 31.12.2003, p. 21
Ghini P. e Ledda F. “Privacy: gli adempimenti di fine e inizio d’anno”, *Guida al Lavoro*, 50, 2003, p. 10
Imperiali Ri., Imperiali Ro. “Gestire informazioni personali rende «incaricato»”, *Guida Normativa*, Dossier mensile n. 1, gennaio 2004, p. 110
Imperiali Ri., Imperiali Ro. “Basta il danno per aprire la via al risarcimento”, *Guida Normativa*, Dossier mensile n. 1, gennaio 2004, p. 111
Imperiali Ri., Imperiali Ro. “Le notizie sensibili viaggiano solo su consenso scritto”, *Guida Normativa*, Dossier mensile n. 1, gennaio 2004, p. 113
Imperiali Ri., Imperiali Ro. “Non è più generale l’obbligo di notificare all’Authority”, *Guida Normativa*, Dossier mensile n. 1, gennaio 2004, p. 116

1 IL NUOVO CODICE DELLA PRIVACY

- *L’1.1.2004 è entrato in vigore il nuovo Codice in materia di protezione dei dati personali, che raccoglie e modifica la disciplina relativa alla tutela della privacy emanata a partire dalla L. 31.12.96 n. 675.*

La L. 31.12.96 n. 675, entrata in vigore l’8.5.97, ha introdotto un’organica e complessa disciplina per la tutela delle persone e degli altri soggetti rispetto al trattamento dei dati personali (c.d. “tutela della *privacy*”).
La complessità della materia e l’evoluzione tecnologica legata all’informatica e alle telecomunicazioni ha però fatto sì che tale disciplina sia stata oggetto di numerosi successivi provvedimenti di modifica e di integrazione, creando un *corpus* normativo di difficile gestione da parte degli interpreti e degli operatori.

Consapevole di tale situazione, la L. 24.3.2001 n. 127[3] ha quindi delegato il Governo ad emanare, entro il 30.6.2003[4], un Testo unico delle disposizioni in materia di tutela della *privacy*, al fine di:

- recepire la direttiva del Parlamento europeo e del Consiglio 12.7.2002 n. 2002/58/CE, in materia di trattamento dei dati personali e di tutela della vita privata nel settore delle comunicazioni elettroniche[5];
- riunire in un unico provvedimento normativo le norme vigenti che si erano “stratificate” nel corso degli anni, apportando alle medesime le modifiche e le integrazioni necessarie al loro coordinamento o per assicurarne la migliore attuazione.

Tale delega è stata attuata mediante l’emanazione del DLgs. 30.6.2003 n. 196[6], che costituisce il “*Codice in materia di protezione dei dati personali*” (c.d. “Codice della *privacy*”).
Il Codice ricomprende, in forma sistematica, la normativa in materia di tutela della *privacy* emanata a partire dalla L. 31.12.96 n. 675, e successive modifiche ed integrazioni, nonché dei relativi provvedimenti attuativi e dei chiarimenti del Garante per la protezione dei dati personali (c.d. “Garante della *privacy*”), ma non si limita ad un mero “assemblaggio” di norme o interpretazioni, in quanto introduce numerose novità[7].

3 Come modificata dall’art. 26 della L. 3.2.2003 n. 14 (legge Comunitaria 2002).

4 La scadenza precedentemente prevista era stabilita al 31.12.2002.

5 Pubblicata sulla *G.U.C.E.* 31.7.2002 n. L 201.

6 Pubblicato sul S.O. n. 123/L alla *G.U.* 29.7.2003 n. 174.

7 Per l’analisi della precedente disciplina in materia di *privacy*, si vedano Negro M. e Serito V. “Tutela del trattamento dei dati personali (c.d. privacy informatica)”, *Schede di Aggiornamento*, 3, 1997, p. 483 - 510, Negro M. e Serito V. “Tutela del trattamento dei dati personali (c.d. “privacy informatica”) - Aggiornamento”, *Schede di Aggiornamento*, 5, 1997, p. 815 - 820, Negro M. “Tutela del trattamento dei dati personali (c.d. “privacy informatica”) - Aggiornamento”, *Schede di Aggiornamento*, 9, 1997, p. 1289 - 1306, Negro M. e Serito V. “Tutela del trattamento dei dati personali (c.d. “privacy informatica”) - Materiali pratici”, *Schede di Aggiornamento*, 11, 1997, p. 1623 - 1636, Negro M. e Serito V. “Tutela del trattamento dei dati personali (L. 675/96) - Aggiornamento - Principali obblighi ed esoneri”, *Schede di Aggiornamento*, 1, 1998, p. 103 - 109, Negro M. “Tutela della privacy - Regolamento attuativo”, *Schede di Aggiornamento*, 7, 1999, p. 1153 - 1166, Negro M. “Tutela della privacy - Le misure minime di sicurezza”, *Schede di Aggiornamento*, 12, 1999, p. 1773 - 1784 e Negro M. “Conservazione delle dichiarazioni e adozione delle misure «minime» di sicurezza per la privacy”, *Schede di Aggiornamento*, 11, 2000, p. 1685 - 1692.

Peraltro, alcune nuove disposizioni non appaiono chiare e sono quindi necessari chiarimenti ufficiali da parte del Garante.

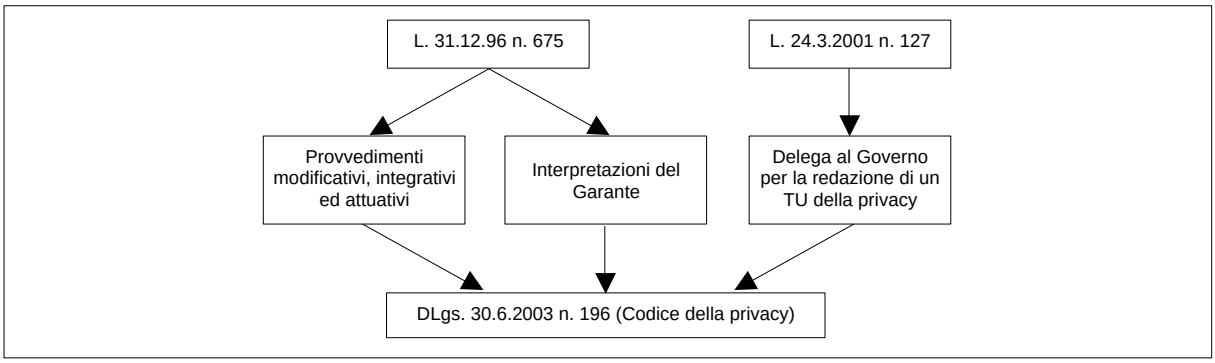

Fig. 1 - *Disciplina di tutela della privacy - Evoluzione normativa*

Il contenuto del "Codice della privacy"

Il Codice della *privacy* contiene, in particolare:

- i principi generali relativi alla protezione dei dati personali;
- le regole generali relative ai trattamenti di dati personali, in particolare i diritti dell'interessato ed il trattamento dei dati "sensibili" e giudiziari;
- le disposizioni relative ai titolari, ai responsabili ed agli incaricati del trattamento;
- la disciplina degli adempimenti per il trattamento dei dati personali (es. notificazione e autorizzazione del Garante, informativa e consenso dell'interessato, ecc.);
- la disciplina relativa al trasferimento dei dati personali all'estero;
- le disposizioni relative alle misure di sicurezza;
- la disciplina relativa al trattamento dei dati personali in determinati settori (es. in ambito giudiziario, da parte delle forze di polizia, in ambito sanitario, in altri ambiti pubblici, per scopi storici, statistici o scientifici, per finalità di lavoro e di previdenza sociale, in ambito bancario, finanziario ed assicurativo, nello svolgimento dell'attività giornalistica o di commercio elettronico, ecc.);
- la disciplina del "Garante della *privacy*";
- le disposizioni relative alle forme di tutela giurisdizionale e amministrativa previste a favore dell'interessato;
- le sanzioni amministrative e penali per le violazioni attinenti alla disciplina di tutela dei dati personali[8].

[8] Si segnala che, ancora prima della sua entrata in vigore, il DLgs. 30.6.2003 n. 196 (Codice della *privacy*) è già stato modificato dagli artt. 3 - 5 del DL 24.12.2003 n. 354 (pubblicato sulla *G.U.* 29.12.2003 n. 300), in relazione alla conservazione dei dati personali per finalità di accertamento e repressione dei reati; la disciplina del suddetto DL 354/2003 è stata peraltro sensibilmente modificata in sede di conversione nella L. 26.2.2004 n. 45 (pubblicata sulla *G.U.* 27.2.2004 n. 45). In pratica, con gli artt. 3 e 4 del DL 354/2003 convertito nella L. 45/2004 sono stati modificati gli artt. 132 e 181 del DLgs. 196/2003 (l'art. 5, che modificava anche l'art. 183 del Codice, è stato invece soppresso in sede di conversione), determinando l'aumento da 30 a 48 mesi del termine di conservazione dei dati di traffico telefonico in relazione alle finalità di accertamento e repressione dei reati. Tuttavia, per i primi 24 mesi (30 nel testo originario del DL), la conservazione riguarda le indagini per tutti i reati, mentre per i successivi 24 mesi (30 nel testo originario del DL), la conservazione riguarda solo più le indagini su gravi fatti connessi alla criminalità organizzata ed al terrorismo e sui delitti in danno di sistemi informatici o telematici. Inoltre, rispetto al testo originario del DL 354/2003, in sede di conversione è stata eliminata l'estensione delle nuove disposizioni al traffico telematico di accesso ad Internet (es. "navigazione" sui siti, posta elettronica).

Di seguito si riporta, in forma tabellare, la struttura del DLgs. 30.6.2003 n. 196 (Codice della *privacy*).

PARTE - TITOLO - CAPO - ARGOMENTO		ARTICOLI
Parte I – Disposizioni generali		
	Titolo I – Principi generali	1 - 6
	Titolo II – Diritti dell'interessato	7 - 10
	Titolo III – Regole generali per il trattamento di dati • Capo I – Regole per tutti i trattamenti • Capo II – Regole ulteriori per i soggetti pubblici • Capo III – Regole ulteriori per privati ed enti pubblici economici	 11 - 17 18 - 22 23 - 27
	Titolo IV – Soggetti che effettuano il trattamento	28 - 30
	Titolo V – Sicurezza dei dati e dei sistemi • Capo I – Misure di sicurezza • Capo II – Misure minime di sicurezza	 31 - 32 33 - 36
	Titolo VI – Adempimenti	37 - 41
	Titolo VII – Trasferimento dei dati all'estero	42 - 45
Parte II – Disposizioni relative a specifici settori		
	Titolo I – Trattamenti in ambito giudiziario • Capo I – Profili generali • Capo II – Minori • Capo III – Informatica giuridica	 46 - 49 50 51 - 52
	Titolo II – Trattamenti da parte di forze di polizia • Capo I – Profili generali	 53 - 57
	Titolo III – Difesa e sicurezza dello Stato • Capo I – Profili generali	 58
	Titolo IV – Trattamenti in ambito pubblico • Capo I – Accesso a documenti amministrativi • Capo II – Registri pubblici e albi professionali • Capo III – Stato civile, anagrafi e liste elettorali • Capo IV – Finalità di rilevante interesse pubblico • Capo V – Particolari contrassegni	 59 - 60 61 62 - 63 64 - 73 74
	Titolo V – Trattamenti di dati personali in ambito sanitario • Capo I – Principi generali • Capo II – Modalità semplificate per informativa e consenso • Capo III – Finalità di rilevante interesse pubblico • Capo IV – Prescrizioni mediche • Capo V – Dati generici • Capo VI – Disposizioni varie	 75 - 76 77 - 84 85 - 86 87 - 89 90 91 - 94
	Titolo VI – Istruzione • Capo I – Profili generali	 95 - 96
	Titolo VII – Trattamenti per scopi storici, statistici o scientifici • Capo I – Profili generali • Capo II – Trattamento per scopi storici • Capo III – Trattamento per scopi statistici o scientifici	 97 - 100 101 - 103 104 - 110
	Titolo VIII – Lavoro e previdenza sociale • Capo I – Profili generali • Capo II – Annunci di lavoro e dati riguardanti prestatori di lavoro • Capo III – Divieto di controllo a distanza e telelavoro • Capo IV – Istituti di patronato e assistenza sociale	 111 - 112 113 114 - 115 116

PARTE - TITOLO - CAPO - ARGOMENTO		ARTICOLI
	Titolo IX – Sistema bancario, finanziario ed assicurativo • Capo I – Sistemi informativi	117 - 120
	Titolo X – Comunicazioni elettroniche • Capo I – Servizi di comunicazione elettronica • Capo II – Internet e reti telematiche • Capo III – Videosorveglianza	121 - 132 133 134
	Titolo XI – Libere professioni e investigazione privata • Capo I – Profili generali	135
	Titolo XII – Giornalismo ed espressione letteraria ed artistica • Capo I – Profili generali • Capo II – Codice di deontologia	136 - 138 139
	Titolo XIII – Marketing diretto • Capo I – Profili generali	140
Parte III - Tutela dell'interessato e sanzioni		
	Titolo I – Tutela amministrativa e giurisdizionale • Capo I – Tutela dinanzi al Garante • Capo II – Tutela giurisdizionale	141 - 151 152
	Titolo II – L'autorità • Capo I – Il Garante per la protezione dei dati personali • Capo II – L'ufficio del Garante • Capo III – Accertamenti e controlli	153 - 154 155 - 156 157 - 160
	Titolo III – Sanzioni • Capo I – Violazioni amministrative • Capo II – Illeciti penali	161 - 166 167 - 172
	Titolo IV – Disposizioni modificative, abrogative, transitorie e finali • Capo I – Disposizioni di modifica • Capo II – Disposizioni transitorie • Capo III – Abrogazioni • Capo IV – Norme finali	173 - 179 180 - 182 183 184 - 186
Allegato A) – Codici di deontologia A1) Trattamento dei dati personali nell'esercizio dell'attività giornalistica A2) Trattamento di dati personali per scopi storici A3) Trattamento di dati personali a scopi statistici in ambito Sistan		
Allegato B) – Disciplinare tecnico in materia di misure minime di sicurezza		
Allegato C) – Trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia		
Tavola di corrispondenza dei riferimenti previgenti al codice in materia di protezione dei dati personali		

Di seguito si riporta, in forma tabellare, un breve prospetto di raccordo tra i principali adempimenti previsti dalla L. 675/96 e dal DLgs. 196/2003, indicando il paragrafo della presente scheda dove saranno analizzati.

ADEMPIMENTO	L. 675/96	DLGS. 196/2003	§ SCHEDA
Individuare gli eventuali responsabili ed incaricati	Sì	Sì	2, 4
Esame degli aspetti organizzativi	Sì	Sì	14.1.1 - 14.1.5
Individuare le misure di sicurezza	Sì	Sì	9, 14.1.6, 14.2
Predisporre le bozze di informativa e di consenso	Sì	Sì	6, 7
Richiedere l'autorizzazione al Garante	Sì	Sì, casi residuali	6.3
Notificare il trattamento al Garante	Sì	Sì, casi residuali	5
Invio di informativa agli interessati	Sì	Sì	6.1
Raccogliere il consenso degli interessati	Sì	Sì	6.2, 6.3, 7
Adottare/adeguare le misure di sicurezza	Sì	Sì, nuove misure minime	9
Controllo del rispetto delle procedure	Sì	Sì	9

L'entrata in vigore del "Codice della privacy"

Ai sensi dell'art. 186, le disposizioni del Codice sono entrate in vigore, in generale, l'**1.1.2004**.

Erano infatti già entrate in vigore il 30.7.2003[9] alcune disposizioni riguardanti:

- l'Ufficio e il personale del Garante;
- i termini per i ricorsi al Garante;
- la trasformazione dell'"Autorità per l'informatica nella pubblica amministrazione" (AIPA) nel "Centro nazionale per l'informatica nella pubblica amministrazione" (CNIPA).

Abrogazione e coordinamento di norme

Il DLgs. 196/2003, costituendo un Codice, provvede quindi, mediante l'art. 183, ad abrogare espressamente quasi tutti i provvedimenti in materia di tutela della *privacy* che erano stati precedentemente emanati, a partire dalla L. 31.12.96 n. 675.

A fini di coordinamento, il Codice:

- contiene, nell'allegato C), una tavola di corrispondenza tra le nuove disposizioni e quelle dei precedenti provvedimenti;
- stabilisce, all'art. 184 co. 2, che ogni riferimento alla precedente disciplina si intende effettuato alle corrispondenti disposizioni del Codice, secondo la suddetta tavola di corrispondenza.

[9] Giorno successivo alla pubblicazione del Codice sulla *G.U.*

2 DEFINIZIONI

- *Il Codice riunisce le definizioni dei termini utilizzati nell'ambito della disciplina di tutela della privacy, prevedendo alcune novità rispetto a quanto precedentemente stabilito.*

L'art. 4 del Codice fornisce una serie di definizioni valide ai fini della disciplina sulla *privacy*, che riprendono, con modifiche ed integrazioni, quelle precedentemente previste dalla L. 675/96 o da altri provvedimenti.

Le definizioni più importanti sono riepilogate nella seguente tabella.

TERMINE	DEFINIZIONE
DATO PERSONALE	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.
DATI PERSONALI SENSIBILI	I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
DATI GIUDIZIARI	I dati personali idonei a rivelare i provvedimenti che devono essere iscritti al casellario giudiziale, o quelli riguardanti la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 c.p.p.
TRATTAMENTO	Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.
INTERESSATO	La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.
TITOLARE	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
RESPONSABILE	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
INCARICATI	Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile[10].
COMUNICAZIONE	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
DIFFUSIONE	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

I dati giudiziari

Più analiticamente, i "dati giudiziari" sono quelli:

- riguardanti la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 c.p.p.[11];
- idonei a rivelare i provvedimenti che devono essere iscritti nel Casellario giudiziale, ai sensi dell'art. 3 co. 1 lettere da a) a o) e da r) a u) del DPR 14.11.2002 n. 313[12].

Gli atti relativi alla qualità di indagato sono quelli relativi alle indagini preliminari.

La qualità di imputato, invece:

- si assume nella richiesta di rinvio a giudizio, di giudizio immediato, di decreto penale di condanna, di applicazione della pena su richiesta delle parti, nel decreto di citazione diretta a giudizio e nel giudizio direttissimo;

[10] In precedenza la figura dell'incaricato, per quanto prevista, non era definita. La nuova disciplina stabilisce espressamente che l'incaricato deve essere una persona fisica, così come era stato chiarito dal Garante (si vedano Imperiali Ri., Imperiali Ro. "Gestire informazioni personali rende «incaricato»", *Guida Normativa,* Dossier mensile n. 1, gennaio 2004, p. 110).

[11] Tali specie di dati non erano ricompresi nella precedente nozione di "dati giudiziari", ai sensi dell'art. 24 della L. 675/96.

[12] Testo unico in materia di Casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti (pubblicato sul S.O. n. 22/L alla *G.U.* 13.2.2003 n. 36).

- si mantiene fino a che diventi definitiva la sentenza di non luogo a procedere, di proscioglimento o di condanna, ovvero diventi esecutivo il decreto penale di condanna.

Con riferimento, invece, alla seconda categoria, rientrano tra gli atti da iscrivere nel Casellario giudiziale, ad esempio:

- le sentenze e i decreti penali di condanna divenuti irrevocabili, compresa la sospensione condizionale e la non menzione;
- i provvedimenti di applicazione di pene accessorie, di misure alternative alla detenzione, di misure di sicurezza personali e patrimoniali;
- i provvedimenti relativi all'amnistia, all'indulto, alla grazia, alla dichiarazione di abitualità, di professionalità nel reato o di tendenza a delinquere;
- i provvedimenti definitivi di proscioglimento o di non luogo a procedere;
- i provvedimenti di riabilitazione.

Sono invece esclusi dalla nozione di "dati giudiziari" ai fini della *privacy* i seguenti provvedimenti giudiziari, ancorché da iscrivere nel Casellario:

- che dichiarano fallito l'imprenditore, di omologazione del concordato fallimentare, di chiusura del fallimento, di riabilitazione del fallito;
- in materia di interdizione e inabilitazione (compresa la relativa revoca)[13].

3 AMBITO DI APPLICAZIONE

o *Come in precedenza, la disciplina di tutela della privacy si applica a tutti i soggetti che trattano dati personali, sia con mezzi elettronici che manuali.*

Ai sensi dell'art. 5 del Codice, la disciplina sulla *privacy* si applica al trattamento di dati personali effettuati:

- **da chiunque** (es. società di persone o di capitali, imprenditori individuali, professionisti, enti e associazioni *no-profit*, altri soggetti sia privati che pubblici);
- **con qualunque mezzo**, quindi sia con strumenti elettronici che in modo manuale con riferimento ad archivi cartacei;
- nel **territorio italiano**, o in un luogo comunque soggetto alla sovranità italiana (es. navi e aerei), anche se i dati personali sono detenuti all'estero;
- da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea ed impiega, per il trattamento dei dati, **strumenti situati nel territorio italiano** anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito dei dati nel territorio dell'Unione europea[14].

Trattamenti effettuati da persone fisiche per fini esclusivamente personali

Ai sensi dell'art. 5 co. 3 del Codice, sono esclusi dal relativo ambito di applicazione i trattamenti effettuati da persone fisiche per fini esclusivamente personali (cioè al di fuori dell'attività di impresa o professionale eventualmente svolta)[15], a condizione che i dati non siano destinati ad una comunicazione sistematica o alla diffusione.
Tuttavia, i dati trattati per fini esclusivamente personali sono "*in ogni caso*" soggetti alle disposizioni del Codice in materia di:

- misure di sicurezza (art. 31)[16];
- responsabilità civile (art. 15)[17].

---

13 I dati che non rientrano nella nozione di "dati giudiziari" sono da considerare dati personali "comuni" (es. qualità di fallito), ma potrebbero anche rientrare nella categoria dei dati "sensibili" (si pensi, ad esempio, ai provvedimenti di interdizione e inabilitazione per infermità mentale).

14 In tal caso, il titolare stabilito nel territorio di un Paese non appartenente all'Unione europea deve designare un proprio rappresentante in Italia ai fini dell'applicazione della disciplina in esame.

15 Il classico esempio è quello dell'agenda personale, non contenente dati personali di soggetti comunque attinenti all'attività svolta.

16 Si veda il successivo § 9.

17 Si veda il successivo § 13.

4 I SOGGETTI CHE EFFETTUANO IL TRATTAMENTO DEI DATI PERSONALI

- *Il Codice definisce meglio i ruoli del "titolare del trattamento", del "responsabile" e degli "incaricati".*

4.1 IL "TITOLARE"

L'art. 28 del Codice stabilisce ora espressamente che quando il trattamento è effettuato da una persona giuridica, o da un qualsiasi altro ente, associazione od organismo, "**titolare del trattamento**" è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza[18].
Ovviamente tali titolari opereranno mediante le persone fisiche che rivestono le funzioni di amministrazione e rappresentanza.

4.2 IL "RESPONSABILE"

L'art. 29 del Codice prevede che il titolare possa designare un "**responsabile del trattamento dei dati personali**", individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia, ivi compreso il profilo relativo alla sicurezza.
Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.
I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare, il quale vigila sulla puntuale osservanza delle disposizioni di legge e delle istruzioni impartite, anche tramite verifiche periodiche.

4.3 GLI "INCARICATI"

Infine, l'art. 30 del Codice disciplina, in maniera molto più puntuale rispetto all'art. 8 della L. 675/96, la figura degli "**incaricati del trattamento**", stabilendo che le operazioni di trattamento di dati personali possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. In pratica, si tratta delle persone fisiche addette ai terminali e agli archivi che, materialmente, si occupano delle fasi di raccolta, gestione, elaborazione e conservazione dei dati personali.
La designazione degli incaricati è effettuata per iscritto, individuando puntualmente l'ambito del trattamento di dati consentito. Si considera "designazione" anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima[19].

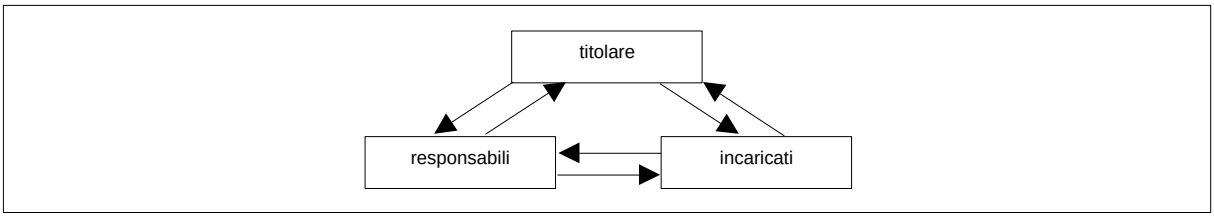

Fig. 2 - *Soggetti che effettuano il trattamento di dati personali*

[18] Finocchiaro G. "Definiti i trattamenti a notifica obbligatoria", *Il Sole - 24 Ore*, 30.7.2003, p. 19, osserva come "*questa disposizione è particolarmente importante per tutti i casi in cui un'impresa abbia sedi periferiche dotate di una certa autonomia, che quindi devono configurarsi come titolari e non come responsabili di trattamento*".

[19] Imperiali Ri., Imperiali Ro. "Gestire informazioni personali rende «incaricato»", *Guida Normativa*, Dossier mensile n. 1, gennaio 2004, p. 110, osservano che "*ne consegue la validità di circolari aziendali o amministrative di nomine effettuate per categorie di dipendenti appartenenti al medesimo settore qualora l'ambito di trattamento dagli stessi eseguito sia il medesimo*".

5 LA NOTIFICAZIONE PREVENTIVA AL GARANTE

- *Il Codice prevede che la notificazione al Garante dei trattamenti dei dati personali debba avvenire solo più in determinate ipotesi.*

Uno degli obblighi previsti dalla normativa sulla *privacy* è quello di effettuare una notificazione al Garante dei trattamenti di dati personali, ora disciplinato dagli artt. 37 e 38 del Codice.

5.1 L'AMBITO DI APPLICAZIONE DELLA NOTIFICAZIONE

Originariamente, l'art. 7 della L. 675/96 prevedeva che l'obbligo di notificazione al Garante avesse un ambito di applicazione generalizzato; le successive modifiche hanno però introdotto numerose ipotesi di esclusione da tale adempimento.

Con il nuovo Codice, la prospettiva viene ribaltata, in quanto l'art. 37 prevede che l'obbligo di notifica ricorra solo se il trattamento riguarda:

- dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
- dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
- dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
- dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
- dati "sensibili" registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati "sensibili" utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
- dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

Modifica ad opera del Garante dei trattamenti soggetti a notificazione

Tuttavia, viene stabilito che il Garante, con proprio provvedimento pubblicato sulla *Gazzetta Ufficiale*:

- da una parte, possa individuare altri trattamenti suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali, per i quali sussiste l'obbligo di notificazione;
- dall'altra, possa individuare eventuali trattamenti non suscettibili di recare detto pregiudizio e pertanto sottratti all'obbligo di notificazione.

5.2 IL CONTENUTO DELLA NOTIFICAZIONE

Sulla base del nuovo modello approvato dal Garante, la notificazione contiene, in particolare, l'indicazione:

- dei dati relativi al titolare;
- dei dati relativi ad uno solo dei responsabili del trattamento eventualmente nominati;
- delle categorie dei trattamenti di dati personali per i quali vi è l'obbligo di notificazione;
- delle categorie di interessati cui si riferiscono i dati;
- delle finalità e delle modalità del trattamento;
- dell'eventuale comunicazione o diffusione dei dati;
- dei luoghi di custodia dei dati;

- dei trasferimenti di dati personali all'estero;
- delle misure di sicurezza adottate, anche ulteriori rispetto a quelle "minime" previste dal Codice.

5.3 IL TERMINE DI EFFETTUAZIONE DELLA NOTIFICAZIONE

La notificazione del trattamento deve essere effettuata al Garante **prima dell'inizio** del trattamento ed una sola volta, a prescindere dal numero delle operazioni e della durata del trattamento da effettuare, e può anche riguardare uno o più trattamenti con finalità correlate.

5.4 LE MODALITÀ DI EFFETTUAZIONE DELLA NOTIFICAZIONE

La notificazione è validamente effettuata solo se:

- è trasmessa per via telematica utilizzando il modello predisposto dal Garante[20];
- osservando le prescrizioni da questi impartite, anche per quanto riguarda le modalità di sottoscrizione con firma digitale e di conferma del ricevimento della notificazione.

Al riguardo, il Garante[21] ha chiarito che:

- verrà inviato all'indirizzo di posta elettronica indicato dal notificante un messaggio di conferma del ricevimento della notificazione, che attesta il buon esito della procedura;
- è possibile stampare copia della notificazione; tale copia cartacea, comunque, non deve essere trasmessa al Garante.

5.4.1 I diritti di segreteria

La notificazione al Garante comporta la corresponsione dei previsti diritti di segreteria[22].

Al riguardo, il Garante[23] ha chiarito che:

- ogni notificazione inviata al Garante deve essere accompagnata dal pagamento dei diritti di segreteria, il cui importo è fissato in 150,00 euro;
- per indicare la modalità di pagamento prescelta va compilato l'apposito riquadro; viene suggerito di privilegiare il pagamento *on line* mediante carta di credito su protocollo sicuro, pur essendo consentite altre modalità (bonifico bancario, conto corrente postale, banco posta); per questi casi occorre indicare gli estremi del pagamento nell'apposito riquadro.

Le coordinate bancarie per effettuare il pagamento sono: conto corrente n. 000000018373 intestato a "Garante per la protezione dei dati personali" - ABI 05164 - CAB 03202 - presso Banca Popolare di Lodi, agenzia n. 2 di Roma, via Bevagna 24, 00191, Roma.
Il pagamento anche può essere effettuato sul conto corrente postale n. 97204002 intestato a "Garante per la protezione dei dati personali", Piazza di Monte Citorio, 115/121, 00186, Roma, indicando come causale "diritti di segreteria per notificazione".

5.4.2 La firma digitale

Per perfezionare la notificazione è necessario sottoscriverla con firma digitale, ai sensi dell'art. 10 co. 3 del DPR 28.12.2000 n. 445.
A tal fine, il titolare del trattamento deve utilizzare un dispositivo di firma digitale disponibile presso uno dei certificatori accreditati ai sensi dell'art. 2 co. 1 lett. c) del DLgs. 23.1.2002 n. 10[24].

---

20 Il Garante ha approvato il nuovo modello di notificazione, da utilizzare a partire dall'1.1.2004, disponibile sul sito *internet https://web.garanteprivacy.it/rgt/*, assieme alle relative istruzioni di compilazione e ad altre informazioni e chiarimenti.

21 Si veda l'informativa disponibile sul sito *internet www.garanteprivacy.it*.

22 Ai sensi dell'art. 11 del DPR 31.3.98 n. 501, norma che non è stata abrogata dal Codice.

23 Si veda l'informativa disponibile sul sito *internet www.garanteprivacy.it*.

24 L'elenco dei certificatori è rinvenibile sul sito *www.cnipa.gov.it*.

L'utilizzo di intermediari

Il Garante ha però reso noto che stipulerà apposite convenzioni con soggetti qualificati (denominati "intermediari"), al fine di permettere la sottoscrizione della notificazione con firma digitale laddove il notificante non fosse in possesso del dispositivo di firma digitale[25].
In questo caso il notificante deve recarsi presso uno dei soggetti convenzionati munito del proprio ID temporaneo e di un documento di riconoscimento (ed eventualmente della ricevuta di versamento dei diritti di segreteria, ove non avesse già provveduto ad inserire gli estremi nell'apposito campo) e, avvalendosi della firma digitale dell'intermediario, trasmettere in via telematica la notificazione.
L'intermediario dovrà:

- annotare nella notificazione, ove non già eseguito dal notificante, gli estremi della ricevuta del pagamento dei diritti di segreteria;
- rilasciare la ricevuta, controfirmata anche dal notificante, di avvenuto invio della notificazione;
- consegnare, a richiesta del notificante, una copia a stampa della notificazione.

Attualmente il Garante ha stipulato convenzioni con:

- Poste Italiane spa, per permettere l'inoltro della notificazione tramite gli uffici Pt *business*[26];
- l'Unione nazionale professionisti pratiche amministrative (UNAPPA), associazione *no-profit* che organizza gli imprenditori che svolgono attività di disbrigo di pratiche amministrative[27].

In entrambi i casi il servizio ha un costo massimo di 25,00 euro, che l'utente paga direttamente all'operatore.

5.4.3 Anomalie e regolarizzazioni

Pervenuta la notificazione al Garante, viene effettuato un controllo sulla veridicità della firma digitale apposta e vengono segnalate al notificante eventuali anomalie. In tal caso il Garante invia un messaggio di richiesta di regolarizzazione/completamento assegnando un termine, decorso inutilmente il quale la notificazione viene eliminata dalla memoria del sistema informativo del Garante, dandone avviso al notificante.
La sottoscrizione digitale che, verificata, non risulti conforme, invalida la notificazione.

In caso di regolarizzazione, la data della notificazione è quella in cui la regolarizzazione stessa è memorizzata nel sistema informativo del Garante.

5.5 LA VARIAZIONE DEI DATI E LA CESSAZIONE DEL TRATTAMENTO

Una nuova notificazione deve essere effettuata in caso di:

- mutamento di taluno degli elementi da indicare nella notificazione medesima (es. ragione o denominazione sociale del titolare o della relativa sede, nomina, revoca o variazione del responsabile precedentemente indicato, ecc.);
- cessazione del trattamento (nel caso in cui l'intero trattamento precedentemente notificato venga a cessare definitivamente).

Termine

La notificazione deve avvenire **anteriormente** alla variazione o alla cessazione del trattamento.

Modalità

Si applicano le stesse modalità viste nel precedente § 5.4.

5.6 IL REGISTRO DEI TRATTAMENTI

Il Garante inserisce le notificazioni ricevute in un registro dei trattamenti accessibile a chiunque e determina le modalità per la sua consultazione gratuita per via telematica, anche mediante convenzioni con soggetti pubblici o presso il proprio Ufficio[28].

25 L'elenco degli organismi convenzionati è reso noto sul sito *internet www.garanteprivacy.it.*

26 L'elenco degli uffici postali abilitati è rinvenibile nel sito *internet* di Poste Italiane spa (*www.poste.it*).

27 L'elenco degli intermediari abilitati è rinvenibile nel sito *internet* di UNAPPA (*www.unappa.it*).

5.7 IL TITOLARE NON TENUTO AD EFFETTUARE LA NOTIFICAZIONE

Viene però stabilito che il titolare che non è tenuto a notificare i trattamenti al Garante deve fornire le notizie contenute nel relativo modello a chi ne fa richiesta, salvo che il trattamento riguardi pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

5.8 DISCIPLINA TRANSITORIA

In via transitoria, l'art. 181 del Codice stabilisce che, in sede di prima applicazione dello stesso, per i trattamenti di dati personali iniziati prima dell'1.1.2004, la notificazione deve essere effettuata entro il **30.4.2004**, utilizzando i nuovi modelli e le nuove modalità.

Tale obbligo riguarda tutti i titolari, anche quelli che hanno già effettuato la notificazione ai sensi della L. 675/96 e che non dovrebbero comunicare variazioni; l'obiettivo di tale disposizione appare quello di permettere di costituire un nuovo archivio delle notificazioni, sulla base dalla nuova disciplina.

Al riguardo, il Garante ha chiarito che[29]:

- l'obbligo di notificazione riguarda solo i trattamenti in essere all'1.1.2004 che rientrano nelle ipotesi previste dal nuovo art. 37 del Codice;
- chi esegue la notificazione secondo le nuove procedure deve dichiarare che sta effettuando una "nuova notificazione", anche se in passato ha già presentato la notificazione in base alla L. 675/96;
- ulteriori eventuali notificazioni costituiscono "modifiche del trattamento", oppure "cessazione del trattamento".

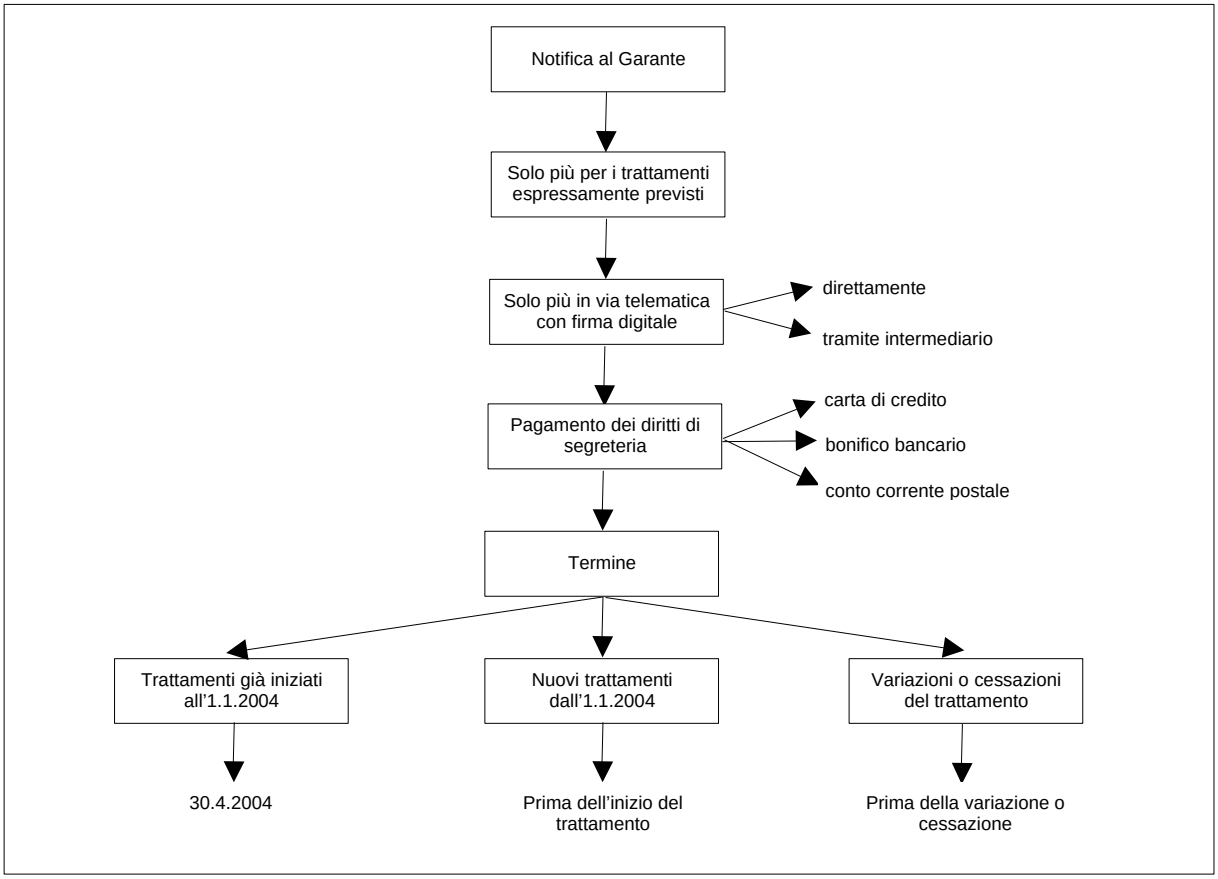

Fig. 3 - *Notifica dei trattamenti al Garante - Procedura*

28 Il Garante ha stabilito che l'interessato può accedere direttamente in ogni momento ai dati che lo riguardano senza necessità di rivolgere un'istanza, consultando la notificazione tramite il sito *internet https://web.garanteprivacy.it/rgt/* o inviando una richiesta anche utilizzando l'*e-mail rgt-info@garanteprivacy.it.*

29 Si veda l'informativa disponibile sul relativo sito *internet*.

6 GLI OBBLIGHI RELATIVI ALLA RACCOLTA E AL TRATTAMENTO DEI DATI PERSONALI

o *Il Codice conferma gli obblighi che erano previsti in relazione alla raccolta e al trattamento dei dati personali, vale a dire l'informativa e il consenso dell'interessato, nonché l'eventuale autorizzazione del Garante per i "dati sensibili".*

Oltre alla notificazione preventiva al Garante, il nuovo Codice, così come la L. 675/96, prevede ulteriori obblighi in relazione alla raccolta e al trattamento di dati personali.

In via preliminare, l'art. 11 del Codice, analogamente all'art. 9 della L. 675/96, stabilisce che 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 sono stati raccolti o successivamente trattati.

I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

6.1 L'INFORMATIVA ALL'INTERESSATO

L'art. 13 del Codice, analogamente all'art. 10 della L. 675/96, stabilisce che l'interessato o la persona presso la quale sono raccolti i dati personali devono essere preventivamente informati, oralmente o per iscritto, circa:

- le finalità e le modalità del trattamento cui sono destinati i dati;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- i diritti spettanti all'interessato, ai sensi dell'art. 7[30];
- gli estremi identificativi del titolare e, se designati, del suo rappresentante in Italia e di almeno un responsabile, da individuare nel soggetto eventualmente preposto ai fini dell'esercizio dei diritti dell'interessato di cui all'art. 7; il titolare deve comunque indicare le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato di tutti i responsabili (es. sito *internet*).

L'informativa può tuttavia non comprendere gli elementi:

- già noti alla persona che fornisce i dati;
- la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato, oppure di prevenzione, accertamento o repressione di reati.

Aggiornamento dei precedenti moduli

Si sottolinea che, in assenza di variazioni nei dati del titolare, del responsabile, delle modalità e finalità dei trattamenti, nonché degli altri elementi oggetto dell'informativa, l'adeguamento al nuovo Codice è limitato ad un aggiornamento dei riferimenti normativi. Peraltro, non sembrano esservi controindicazioni nel continuare ad utilizzare, in via transitoria, i vecchi moduli e formulari.

6.1.1 Dati personali non raccolti presso l'interessato

Se i dati personali non sono raccolti presso l'interessato, l'informativa è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.
Tale disposizione non si applica quando:

- i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

[30] Si veda il successivo § 6.1.2.

- l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

6.1.2 I diritti dell'interessato

I diritti dei soggetti interessati al trattamento dei propri dati personali sono ora disciplinati dall'art. 7 del Codice, in maniera più ampia rispetto all'art. 13 della L. 675/96.

I più importanti diritti dell'interessato sono quelli di:

- ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile;
- essere informato sull'origine dei dati personali, sulle finalità e modalità del trattamento, sulla logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, sugli estremi identificativi del titolare, dei responsabili e del rappresentante in Italia, dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante in Italia, di responsabili o incaricati;
- ottenere l'aggiornamento, la rettificazione, ovvero, quando vi ha interesse, l'integrazione dei dati;
- ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- opporsi, in tutto o in parte:
  - per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
  - al trattamento dei dati personali che lo riguardano ai fini dell'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale[31].

L'interessato può esercitare i propri diritti con richiesta rivolta al titolare o al responsabile, mediante lettera raccomandata, telefax o posta elettronica. In relazione ai diritti di cui all'art. 7 co. 1 e 2 (esistenza di dati e indicazione delle caratteristiche del trattamento), la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile[32].

6.2 IL CONSENSO DELL'INTERESSATO

L'art. 23 del Codice, analogamente all'art. 11 della L. 675/96, stabilisce che il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato[33].

6.2.1 Caratteristiche del consenso

Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

Il consenso è validamente prestato solo se:

- è espresso liberamente e specificatamente in riferimento ad un trattamento chiaramente individuato;
- è documentato per iscritto;
- sono state rese all'interessato le informazioni relative alla raccolta dei dati di cui al precedente art. 13[34].

Poiché il Codice stabilisce che il consenso dell'interessato deve essere "*espresso*", ma "*documentato per iscritto*", sembra che la forma scritta del consenso non sia richiesta per la validità dello stesso, ma solo a fini probatori[35].

---

31 In questi casi non è necessario che ricorrano i "*motivi legittimi*".

32 Ai sensi dell'art. 10 del Codice, il titolare ha diritto ad un rimborso spese per i costi effettivamente sopportati per la ricerca effettuata a seguito della richiesta dell'interessato, nei limiti massimi che saranno stabiliti dal Garante. Con il Codice tale rimborso spese viene ora previsto in ogni caso, mentre in precedenza l'art. 17 del DPR 501/98 (norma ora abrogata) lo prevedeva solo quando non fosse risultata confermata l'esistenza di dati che riguardavano l'interessato.

33 Salvo i previsti casi di esclusione (si veda il successivo § 6.2.2).

34 Si veda il precedente § 6.1.

35 In tal senso Ciccia A. "Il consenso viaggia su doppio binario", *Italia Oggi*, 14.7.2003, p. 33. Peraltro, appare opportuno richiedere sempre il consenso scritto, in quanto quello rilasciato oralmente, seppur valido, potrebbe comportare difficoltà a livello probatorio ed esporre a contenziosi.

La forma scritta del consenso è, invece, richiesta per il trattamento dei dati "sensibili" di cui all'art. 26 del Codice[36].
In relazione alle modalità di prestazione del consenso, si ricorda che, con la decisione del 28.5.97, il Garante ha chiarito che:

- il consenso non può essere generalizzato e fondato su informazioni generiche o insufficienti, accompagnate dall'esplicita previsione di una possibile rottura dei rapporti contrattuali;
- occorre una chiara distinzione tra:
  - dati che devono essere forniti in base ad un obbligo di legge;
  - informazioni strettamente funzionali all'esecuzione del rapporto contrattuale;
  - dati relativi allo svolgimento di ulteriori attività, subordinate a uno specifico consenso dell'interessato.

L'interessato può, infatti, rifiutarsi di fornire il proprio consenso al trattamento dei dati per situazioni non dipendenti dall'economia negoziale (es. invio in futuro di materiale pubblicitario); in tali casi non si può prospettare la mancata attivazione o l'interruzione del rapporto.

Aggiornamento dei precedenti moduli

Anche in relazione alla richiesta di consenso, si sottolinea che, in assenza di variazioni nelle modalità e finalità dell'utilizzo dei dati raccolti, nonché degli altri aspetti oggetto di consenso dell'interessato, l'adeguamento al nuovo Codice è limitato ad un aggiornamento dei riferimenti normativi. Peraltro, non sembrano esservi controindicazioni nel continuare ad utilizzare, in via transitoria, i vecchi moduli e formulari.

Revoca del consenso

Il consenso potrà, inoltre, essere revocato[37].

6.2.2 Casi di esclusione del consenso

L'art. 24 del Codice, analogamente all'art. 12 della L. 675/96, stabilisce i casi in cui il consenso non è richiesto, fermo restando l'obbligo di informativa di cui all'art. 13[38], ad esempio:

- dati raccolti e detenuti in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- trattamento 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;
- dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;
- dati relativi allo svolgimento di attività economiche, nel rispetto della vigente normativa in materia di segreto aziendale e industriale[39];
- trattamento necessario per far valere o difendere un diritto in sede giudiziaria;
- trattamenti effettuati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, con esclusione della comunicazione all'esterno e della diffusione.

6.3 IL TRATTAMENTO DEI "DATI SENSIBILI" E GIUDIZIARI

Ai sensi dell'art. 26 del Codice, analogamente all'art. 22 della L. 675/96, i "dati sensibili"[40] possono essere oggetto di trattamento, in generale, solo:

- con il consenso scritto dell'interessato;
- e previa autorizzazione del Garante.

36 Si veda il successivo § 6.3.

37 In tal senso Imperiali Ri., Imperiali Ro. "La tutela dei dati personali", ed. Il Sole - 24 Ore, Norme e Tributi, Milano, 1997, p. 120.

38 Si veda il precedente § 6.1.

39 Secondo Ciccia A. "Il consenso viaggia su doppio binario", *Italia Oggi*, 14.7.2003, p. 33, si tratta, ad esempio, dei dati relativi alla solvibilità delle persone o delle imprese.

40 Si veda il precedente § 2.

Il successivo art. 27 del Codice, analogamente all'art. 24 della L. 675/96, prevede che il trattamento di dati giudiziari[41] da parte di privati o di enti pubblici economici è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino:

- le rilevanti finalità di interesse pubblico del trattamento;
- i tipi di dati trattati e di operazioni eseguibili.

6.3.1 Il consenso dell'interessato

In caso di "dati sensibili", la forma scritta del consenso dell'interessato deve intendersi prescritta come requisito di validità dello stesso.

6.3.2 Le "autorizzazioni standard" del Garante

Per quanto riguarda l'autorizzazione del Garante, l'art. 40 del Codice prevede, analogamente all'art. 41 co. 7 della L. 675/96, che esso possa rilasciare autorizzazioni relativamente a determinate categorie di titolari o di trattamenti (c.d. "autorizzazioni *standard*"). Ai sensi dell'art. 41 del Codice, i soggetti che trattano i "dati sensibili" nel rispetto di quanto indicato nelle "autorizzazioni *standard*" sono esonerati dal richiedere al Garante un'autorizzazione individuale.

Attualmente sono applicabili le seguenti sette autorizzazioni *standard*, approvate con provvedimenti del Garante del 31.1.2002[42], la cui efficacia è stata prorogata fino al **30.6.2004** dal provvedimento del Garante del 24.6.2003[43], relative al trattamento dei:

- "dati sensibili" nell'ambito di rapporti di lavoro (n. 1/2002);
- dati relativi allo stato di salute e alla vita sessuale (n. 2/2002);
- "dati sensibili" da parte degli organismi di tipo associativo e delle fondazioni (n. 3/2002);
- "dati sensibili" da parte dei liberi professionisti (n. 4/2002);
- "dati sensibili" da parte di banche, assicurazioni, SIM, imprese turistiche, di elaborazione dati, di sondaggi di opinione e ricerche di mercato, di ricerca e selezione del personale, di agenzie matrimoniali, ecc. (n. 5/2002)[44];
- "dati sensibili" da parte degli investigatori privati (n. 6/2002);
- dati di carattere giudiziario (n. 7/2002).

6.3.3 Le "autorizzazioni individuali" del Garante

Per i trattamenti di "dati sensibili" che non rientrano nella "copertura" delle suddette autorizzazioni *standard*, l'art. 41 del Codice stabilisce che l'autorizzazione del Garante è richiesta:

- utilizzando esclusivamente il modello dallo stesso predisposto;
- mediante trasmissione per via telematica oppure mediante telefax o lettera raccomandata.

I diritti di segreteria

La richiesta di autorizzazione al Garante comporta la corresponsione dei previsti diritti di segreteria[45].

Decisione del Garante - Silenzio-rifiuto

Ai sensi dell'art. 26 del Codice, il Garante decide sulle richieste di autorizzazione entro 45 giorni (prima 30).
Come in precedenza, la mancata pronuncia del Garante entro tale termine equivale a rifiuto dell'autorizzazione.

6.3.4 Trattamenti di "dati sensibili" esclusi dal consenso e dall'autorizzazione del Garante

Ai sensi dell'art. 26 co. 3 del Codice, la disciplina dei "dati sensibili" non si applica al trattamento dei dati[46]:

41 Si veda il precedente § 2.

42 Pubblicati sul S.O. n. 70 alla *G.U.* 9.4.2002 n. 83.

43 Pubblicato sulla *G.U.* 19.8.2003 n. 191.

44 Rientrano nell'ambito di tale "autorizzazione *standard*" anche le società di servizi dei professionisti che svolgono attività di elaborazione dati in ambito contabile, fiscale, retributivo, previdenziale e assistenziale.

45 Ai sensi dell'art. 11 del DPR 31.3.98 n. 501, norma che non è stata abrogata dal Codice.

46 Analogamente a quanto era previsto dall'art. 22 co. 1-*bis* e 1-*ter* della L. 675/96.

- relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni;
- riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria.

6.3.5 Trattamenti di "dati sensibili" esclusi dal consenso, previa autorizzazione del Garante

L'art. 26 co. 4 del Codice prevede alcune ipotesi nelle quali i "dati sensibili" possono essere oggetto di trattamento anche senza il consenso dell'interessato, previa autorizzazione del Garante[47].

Le più importanti sono quando il trattamento:

- è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni dell'apposito codice di deontologia e di buona condotta[48];
- è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'art. 13;
- è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato.

6.3.6 I dati personali "semisensibili"

L'art. 17 del Codice riprende la disciplina dell'art. 24-*bis* della L. 675/96, in materia di trattamento dei dati diversi da quelli "sensibili" e giudiziari che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare (c.d. "dati semisensibili").

Il trattamento di tali dati è ammesso nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato, prescritti dal Garante.

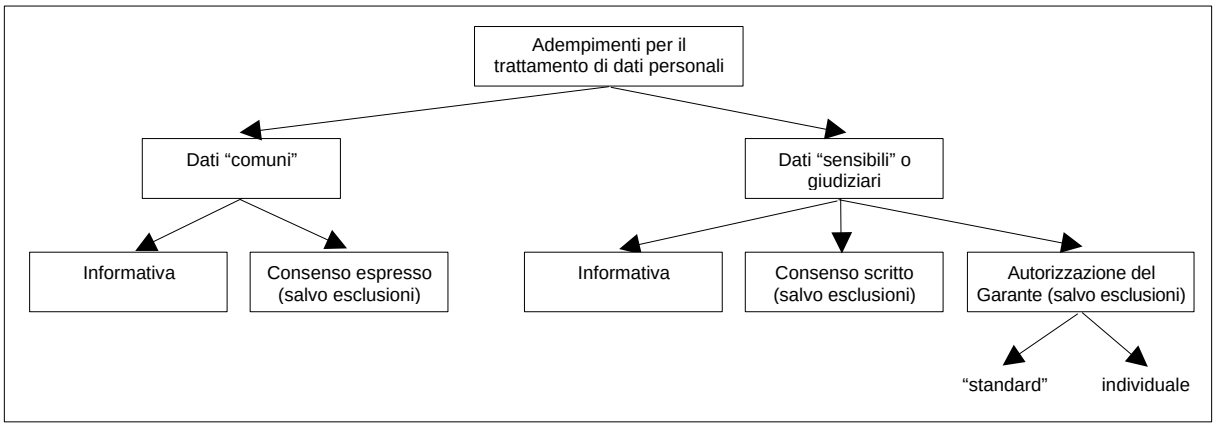

Fig. 4 - *Adempimenti per il trattamento dei dati personali*

[47] Tale disciplina riprende ed amplia quanto era previsto dall'art. 22 co. 4 della L. 675/96.

[48] Di cui all'art. 111 del Codice.

7 LA COMUNICAZIONE E LA DIFFUSIONE DEI DATI PERSONALI

- *In caso di comunicazione e diffusione dei dati, continua ad essere richiesto il consenso espresso dell'interessato, salvi i casi di esclusione previsti dalla legge.*

In materia di comunicazione e diffusione dei dati, l'art. 25 del Codice effettua una notevole semplificazione normativa rispetto ai precedenti artt. 20 e 21 della L. 675/96, in quanto si limita solo più a stabilire che la comunicazione e la diffusione dei dati personali da parte di privati e di enti pubblici economici sono vietate:

- in caso di provvedimento disposto dal Garante o dall'autorità giudiziaria:
- in riferimento a dati personali dei quali è stata ordinata la cancellazione, ovvero quando è decorso il periodo di tempo necessario agli scopi per i quali erano stati raccolti o successivamente trattati;
- per finalità diverse da quelle indicate nella notificazione del trattamento, ove prescritta.

Tuttavia, ai sensi dell'art. 23 del Codice, permane l'obbligo di richiesta del consenso espresso dell'interessato alla comunicazione e diffusione dei dati, salvo che si rientri nelle ipotesi di esclusione previste dal successivo art. 24[49].

8 IL TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO

- *Il Codice conferma le limitazioni al trasferimento dei dati personali in Stati non appartenenti all'Unione europea.*

Gli artt. 42 - 45 del Codice disciplinano i trasferimenti all'estero dei dati personali, riprendendo la precedente disciplina dell'art. 28 della L. 675/96; la disciplina è differenziata a seconda che il trasferimento avvenga in Stati appartenenti all'Unione europea oppure in Stati extra-comunitari.

8.1 TRASFERIMENTI IN STATI APPARTENENTI ALL'UNIONE EUROPEA

Per quanto riguarda i trasferimenti all'interno dell'Unione europea, viene stabilito che le disposizioni del Codice non possono essere applicate in modo tale da restringere o vietare la libera circolazione dei dati personali fra gli Stati membri dell'Unione europea, fatta salva l'adozione di eventuali provvedimenti in caso di trasferimenti di dati effettuati al fine di eludere le relative disposizioni.

8.2 TRASFERIMENTI IN STATI NON APPARTENENTI ALL'UNIONE EUROPEA

Il trasferimento dei dati personali, anche temporaneo, con qualsiasi forma o mezzo, verso uno Stato non appartenente all'Unione europea è consentito quando:

- l'interessato ha manifestato il proprio consenso espresso o, se si tratta di "dati sensibili", in forma scritta;
- è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;
- il trattamento concerne dati riguardanti persone giuridiche, enti o associazioni;
- è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo o di un interesse pubblico rilevante individuato con legge o con regolamento, ovvero per far valere o difendere un diritto in sede giudiziaria;
- è effettuato in accoglimento di una richiesta di accesso ai documenti amministrativi, ovvero di una richiesta di informazioni estraibili da un pubblico registro, elenco, atto o documento conoscibile da chiunque, con l'osservanza delle norme che regolano la materia;
- è necessario, in conformità ai rispettivi codici di deontologia, per esclusivi scopi scientifici, statistici o storici;
- è autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, prestate anche con un contratto, oppure sulla base delle decisioni della Commissione europea che riconoscono che lo Stato estero garantisce un livello di protezione adeguato o che alcune clausole contrattuali offrono garanzie sufficienti[50].

[49] Si veda il precedente § 6.2.

[50] Si vedano le autorizzazioni del Garante relative al trasferimento di dati personali verso gli Stati Uniti (delibera del 10.10.2001 n. 36), la Svizzera (delibera del 17.10.2001 n. 37), l'Ungheria (delibera del 17.10.2001 n. 38), il Canada (delibera del 30.4.2003 n. 6) e, in generale, gli altri Paesi non appartenenti all'Unione europea (delibere del 10.10.2001 n. 35 e del 10.4.2002 n. 3). Si ricorda che dall'1.5.2004 entreranno a far parte dell'Unione europea la Slovenia, la Slovacchia, la Repubblica Ceca, l'Ungheria, la Polonia, la

Il Codice ha quindi eliminato, in generale, l'obbligo di preventiva notificazione al Garante e di attendere 15 o 20 giorni dalla notificazione stessa per poter effettuare il trasferimento, come era previsto dall'art. 22 della L. 675/95, salvi i casi in cui il trasferimento era comunque ammesso.
Tuttavia, l'art. 37 co. 3 del Codice prevede che "*la notificazione è effettuata con unico atto anche quando il trattamento comporta il trasferimento all'estero dei dati*". Sul punto il Garante[51] ha chiarito che "*se si trasferiscono dati all'estero, la circostanza va indicata nella stessa, unica notificazione che riguarda questi dati*", vale a dire quelli oggetto di notificazione ai sensi del suddetto art. 37[52].

Trasferimenti vietati

Il trasferimento dei dati personali in Stati extracomunitari è però vietato quando l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato, tenendo conto anche delle modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza.

9 LE MISURE DI SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI

- *Le novità più rilevanti del Codice, anche a fini pratici, riguardano le misure minime di sicurezza.*

  In particolare, scompaiono le precedenti classificazioni con graduazione degli adempimenti in funzione dell'aumento dei rischi (trattamenti ad uso personale, archivi cartacei, utilizzo di computer in rete, disponibilità al pubblico della rete); la nuova disciplina distingue solo più tra trattamenti effettuati con o senza strumenti elettronici.

  Nei confronti di soggetti privati, professionisti, piccole e medie imprese, enti non commerciali, ecc., nella larghissima maggioranza dei casi le nuove disposizioni comporteranno un netto aggravio di oneri.

Gli artt. 31 - 36 del Codice disciplinano le misure di sicurezza relative al trattamento di dati personali, in sostituzione dell'art. 15 della L. 675/96 e del DPR 28.7.99 n. 318 (che viene espressamente abrogato)[53].

In linea generale, l'art. 31 del Codice stabilisce che 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;
- accesso non autorizzato;
- trattamento non consentito o non conforme alle finalità della raccolta.

9.1 LE MISURE "MINIME" DI SICUREZZA

L'art. 33 del Codice stabilisce che i titolari del trattamento sono comunque tenuti ad adottare le misure volte ad assicurare un livello minimo di protezione dei dati personali, previste nei successivi artt. 34 e 35 e nel disciplinare tecnico contenuto nell'allegato B) allo stesso Codice.
Le nuove misure minime di sicurezza sono differenziate solo più a seconda che il trattamento dei dati personali avvenga o meno mediante strumenti elettronici. Inoltre, non vi sono più disposizioni specifiche relative ai trattamenti effettuati da persone fisiche per fini esclusivamente personali[54], al fine di limitarne gli adempimenti.

In precedenza, invece, il DPR 318/99 differenziava le misure minime di sicurezza in relazione ai trattamenti di dati personali effettuati:

- mediante computer "non in rete";
- mediante computer "in rete" non disponibile al pubblico;
- mediante computer "in rete" disponibile al pubblico;

Lituania, l'Estonia, la Lettonia, Malta e Cipro.

51 Si veda l'informativa disponibile sul relativo sito *internet*.

52 Si veda il precedente § 5.1.

53 In relazione alla disciplina delle misure minime di sicurezza prevista dal DPR 318/99, si veda Negro M. "Tutela della privacy - Le misure minime di sicurezza", *Schede di Aggiornamento*, 12, 1999, p. 1773 - 1784 e "Conservazione delle dichiarazioni e adozione delle misure «minime» di sicurezza per la privacy", *Schede di Aggiornamento*, 11, 2000, p. 1685 - 1692.

54 Si veda il precedente § 3.

- con strumenti non elettronici (archivi cartacei);
- da persone fisiche per fini esclusivamente personali.

Aggiornamento periodico

Ai sensi dell'art. 36 del Codice, le misure minime di sicurezza sono aggiornate 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[55].

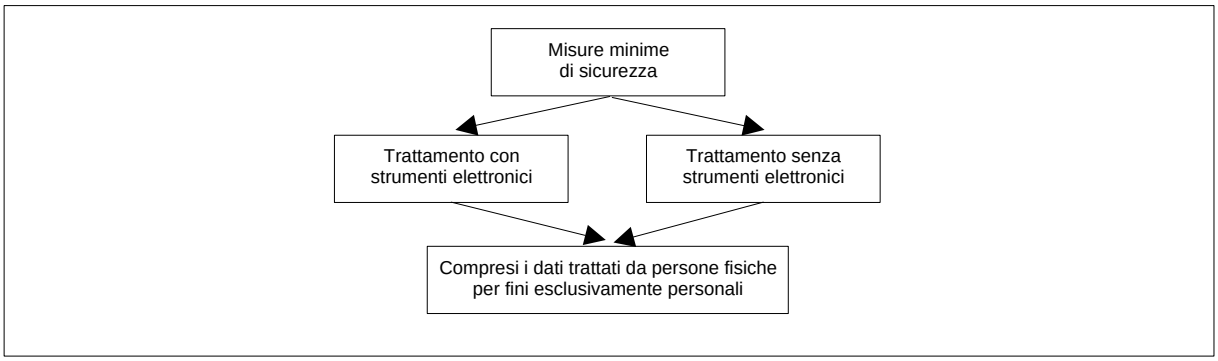

Fig. 5 - *Applicazione delle misure minime di sicurezza*

9.2 LE MISURE "MINIME" DI SICUREZZA PER I TRATTAMENTI DI DATI PERSONALI MEDIANTE STRUMENTI ELETTRONICI

Ai sensi dell'art. 34 del Codice, il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, a cura del titolare, del responsabile ove designato e dell'incaricato, le seguenti misure minime:

a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) tenuta di un aggiornato documento programmatico sulla sicurezza;
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[56].

9.2.1 Il sistema di autenticazione informatica (allegato B) punti 1 - 11 del Codice)

Ai sensi dell'art. 4 co. 3 lett. c) del Codice, l'"*autenticazione informatica*" è "*l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità*".

Le credenziali di autenticazione

Ai sensi dell'art. 4 co. 3 lett. d) del Codice, le "*credenziali di autenticazione*" sono "*i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica*".

Le credenziali di autenticazione consistono:

- in un codice per l'identificazione dell'incaricato (es. *login*, PIN, *username*, ecc.) associato a una "parola chiave" (*password*) riservata e conosciuta solamente dal medesimo;
- oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato[57], eventualmente associato a un codice identificativo o a una parola chiave;

55 L'art. 15 co. 3 della L. 675/96 prevedeva un adeguamento con cadenza almeno biennale, ma tale norma non ha mai trovato applicazione.

56 Si segnala che il Codice non prevede più la figura degli "amministratori di sistema", che erano definiti dal DPR 318/99 come "*i soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione*".

- oppure in una caratteristica biometrica dell'incaricato (es. impronta digitale), eventualmente associata a un codice identificativo o a una parola chiave.

Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione; l'incaricato deve adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo[58].

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

Le credenziali di autenticazione sono disattivate:

- se non utilizzate da almeno sei mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
- in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante l'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.

Peraltro, le disposizioni sul sistema di autenticazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Le "parole chiave"

Ai sensi dell'art. 4 co. 3 lett. e) del Codice, la "*parola chiave*" è la "*componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica*".

La "parola chiave":

- 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;
- non deve contenere riferimenti agevolmente riconducibili all'incaricato[59];
- è modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi (tre mesi in caso di trattamento di "dati sensibili" o giudiziari)[60].

9.2.2 Il sistema di autorizzazione (allegato B) punti 12 – 15 del Codice)

Ai sensi dell'art. 4 co. 3 lett. g) del Codice, il "*sistema di autorizzazione*" è "*l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente*".

Ai sensi della precedente lett. f), il "*profilo di autorizzazione*" è "*l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti*".

---

57 Ad esempio, una *smart card*.

58 Ad esempio, come osservato da Baffigo L. "Anche la password del Pc deve rispettare regole precise", *Il Sole - 24 Ore, Documenti* 15.12.2003, p. 7, "*l'incaricato non deve lasciare incustodito, per esempio quando si assenta per l'intervallo di mensa, il proprio Pc se prima non ha provveduto a chiudere la sessione di lavoro (in altri termini, se prima non si è dato il comando di log-off)*".

59 Ad esempio, come indicato da Baffigo L. "Anche la password del Pc deve rispettare regole precise", *Il Sole - 24 Ore, Documenti* 15.12.2003, p. 6, "*il nome o la data di nascita proprie o di un familiare, oppure il nome del proprio cane o di altri elementi simili: un accorgimento per evitare che la password sia facilmente ricostruibile*". Tale Autore osserva altresì che "*una buona password dovrebbe, inoltre, contenere sia dati alfabetici sia numerici e non utilizzare parole che sono comprese nei vocaboli delle lingue più diffuse*".

60 Come osservato da Baffigo L. "Anche la password del Pc deve rispettare regole precise", *Il Sole - 24 Ore, Documenti* 15.12.2003, p. 6, "*si tratta di precauzioni molto importanti, che hanno lo scopo di garantire che la password sia effettivamente segreta e conosciuta solo dall'incaricato. Inoltre, intendono ridurre, nel caso la password non sia più (all'insaputa dell'interessato) segreta, il tempo di durata della violazione*". Tale Autore prosegue quindi sostenendo che "*tra le precauzioni da adottare c'è il divieto di comunicare la propria password ad altri, di scriverla su un bigliettino e di attaccarlo al video o in altro posto facilmente indovinabile. (…) In ogni caso, l'azienda può, in assenza dell'incaricato, utilizzare la password o le altre credenziali di quest'ultimo. Lo deve fare seguendo precise procedure e solo in presenza di oggettive necessità di lavoro o di sicurezza. Al rientro, l'incaricato deve essere informato di quanto avvenuto e deve immediatamente impostare una nuova password*".

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

Peraltro, le disposizioni sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

9.2.3 I programmi "antivirus" e l'aggiornamento del software (allegato B) punti 16 - 17 del Codice)

I dati personali devono essere protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale (c.d. "virus"), mediante l'attivazione di idonei strumenti elettronici (c.d. "programmi antivirus") da aggiornare con cadenza almeno semestrale[61].

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente (ogni sei mesi in caso di trattamento di "dati sensibili" o giudiziari).

9.2.4 Il "back-up" periodico (allegato B) punto 18 del Codice)

È inoltre previsto il salvataggio dei dati (c.d. "*back-up*") con frequenza almeno settimanale.

9.2.5 Il documento programmatico sulla sicurezza (allegato B) punto 19 del Codice)

In caso di trattamento di "dati sensibili" o giudiziari con strumenti elettronici (es. *computer*), vi è l'obbligo della redazione del documento programmatico sulla sicurezza (DPS).

Soggetto obbligato alla redazione del documento

Soggetto obbligato alla redazione del documento programmatico sulla sicurezza è il titolare dei suddetti trattamenti, "*anche attraverso il responsabile, se designato*".

Contenuto

Il documento programmatico sulla sicurezza contiene idonee informazioni riguardo:

- all'elenco dei trattamenti di dati personali;
- alla distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- all'analisi dei rischi che incombono sui dati;
- alle misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché alla protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- alla descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- alla 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;
- alla 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, all'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Da una lettura sistematica della norma sembrerebbe che il documento programmatico sulla sicurezza debba riguardare i soli trattamenti di "dati sensibili" o giudiziari. Tuttavia, l'esame testuale delle suddette disposizioni non sembra consentire tale interpretazione, per cui il documento sembrerebbe dover riguardare tutti i trattamenti i dati personali.
In proposito si auspicano chiarimenti ufficiali.

[61] Come osservato da Baffigo L. "Anche la password del Pc deve rispettare regole precise", *Il Sole - 24 Ore, Documenti* 15.12.2003, p. 7, "*l'antivirus che protegge il proprio Pc non deve essere mai disattivato da chi ci lavora*".

Termini

Il documento programmatico sulla sicurezza deve essere redatto "*entro il 31 marzo di ogni anno*".

In sede di passaggio dalla vecchia alla nuova normativa, sembrerebbe che la scadenza del 31.3.2004 debba essere rispettata dai soli titolari che erano già assoggettati a tale adempimento sulla base della precedente disciplina[62].

Per i titolari che, invece, diventano assoggettati a tale adempimento sulla base delle nuove disposizioni del Codice, dovrebbe prevalere la disciplina transitoria[63], ai sensi della quale il termine per l'adeguamento sarebbe il 30.6.2004.

Indicazione nella relazione accompagnatoria del bilancio d'esercizio

Il punto 26 dell'allegato B) al Codice prevede che "*il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza*"[64].
Non è richiesto che siano indicate le spese sostenute per l'adozione delle misure di sicurezza previste dal Codice della *privacy*.
D'altra parte, potrebbe però essere opportuno che venga espressamente indicato che non ricorre l'obbligo di redazione del documento programmatico sulla sicurezza.

In prima battuta, la "*relazione accompagnatoria del bilancio d'esercizio*" dovrebbe essere individuata nella "*relazione sulla gestione*", di cui all'art. 2428 c.c.
Tuttavia, le società che redigono il bilancio abbreviato possono essere esonerate da tale adempimento, ai sensi dell'art. 2435-*bis* c.c.; in tal caso, non appare però chiaro se l'indicazione relativa al documento programmatico sulla sicurezza debba confluire nella nota integrativa al bilancio[65].
Su tali aspetti sono quindi necessari chiarimenti ufficiali del Garante.

In relazione all'adempimento in esame, si pone inoltre il problema di individuare il bilancio nella cui relazione accompagnatoria deve essere effettuata l'indicazione relativa al documento programmatico sulla sicurezza. In pratica, ci si chiede se si debba adottare un criterio:

- di "competenza", in base al quale l'indicazione va fornita nella relazione relativa al bilancio dell'esercizio in cui il documento programmatico sulla sicurezza è stato redatto o aggiornato; in base a tale criterio, ad esempio, il documento programmatico sulla sicurezza redatto nel 2004 dovrebbe essere indicato nella relazione accompagnatoria al bilancio dell'esercizio 2004 approvato nel 2005;
- oppure di "successione temporale" degli adempimenti, in base al quale l'indicazione va fornita nella relazione relativa al primo bilancio d'esercizio approvato successivamente alla data in cui il documento programmatico sulla sicurezza è stato redatto o aggiornato; in base a tale criterio, invece, ad esempio, il documento programmatico sulla sicurezza redatto nel 2004 dovrebbe essere indicato nella relazione accompagnatoria al bilancio dell'esercizio 2003, se approvato successivamente alla sua redazione o aggiornamento.

Da un punto di vista sistematico, sembrerebbe preferibile la prima tesi, in modo da "collegare" un adempimento effettuato in un anno alla relazione relativa all'attività svolta in tale anno; peraltro, si potrebbe però sostenere che l'adempimento in esame possa rientrare nei "*fatti di rilievo avvenuti dopo la chiusura dell'esercizio*" che devono essere indicati nella relazione relativa all'anno precedente.
Anche su tali aspetti sono quindi assolutamente necessari chiarimenti ufficiali del Garante[66].

---

62 Si ricorda che, secondo l'art. 6 del DPR 318/99, il documento programmatico sulla sicurezza doveva essere predisposto e aggiornato, con cadenza annuale (senza però indicare una specifica data), da parte dei soggetti che trattano dati "sensibili" o dati giudiziari per mezzo di *computer* accessibili da altri *computer* "*mediante una rete di telecomunicazioni disponibili al pubblico*". Come evidenziato da Ghini P. e Ledda F. "Privacy: gli adempimenti di fine e inizio d'anno", *Guida al Lavoro*, 50, 2003, p. 10, "*in base ai chiarimenti ufficiali diramati dall'Autorità Garante privacy, appartengono al predetto contesto informatico «… tutti gli elaborati connessi ad una rete che ha un collegamento al mondo Internet, anche se protetto da un firewall» posto che «… la rete è da ritenersi non disponibile al pubblico solo se è posta all'interno di un'unica sede ed è priva di qualunque interconnessione esterna, comprese quelle su linee dedicate*".

63 Si veda il successivo § 9.4.

64 Come evidenziato da Berghella F. "Guida pratica alle nuove misure di sicurezza per la privacy", Bancaria Editrice, Roma, 2003, p. 206, con tale disposizione il legislatore ha probabilmente voluto "nobilitare" la redazione del documento programmatico sulla sicurezza "*elevandola tra le comunicazioni formali che un'impresa è tenuta a fare nella relazione accompagnatoria del bilancio d'esercizio. In tal modo portando le necessità di sicurezza, gli interventi svolti, quelli pianificati e il loro aggiornamento, all'attenzione del consiglio di amministrazione delle aziende, dell'assemblea dei soci e del collegio sindacale*".

65 Il fatto che la norma in esame prenda in considerazione la "*relazione accompagnatoria del bilancio d'esercizio, se dovuta*", sembrerebbe far propendere per la tesi negativa, salvo ritenere che, anche se l'interpretazione appare un po' forzata sulla base del dato letterale della disposizione, che la "*relazione accompagnatoria del bilancio d'esercizio*" sia da individuare, in ogni caso, nella nota integrativa.

66 In attesa di tali chiarimenti, appare prudenziale provvedere ad effettuare l'indicazione in esame nel primo bilancio approvato successivamente alla data in cui il documento programmatico sulla sicurezza è stata redatto o aggiornato. In tal senso si veda anche Ciccia A. "Codice della privacy, tutti gli adempimenti per le imprese", *Italia Oggi*, 29.12.2003, p. 17, il quale evidenzia che "*è sorta*

In ogni caso, deve ritenersi che l'adempimento in esame non riguardi i soggetti che non sono tenuti civilisticamente alla redazione del bilancio d'esercizio.

9.2.6 Altre misure di sicurezza in caso di trattamento di dati "sensibili" o giudiziari (allegato B) punti 20 - 24 del Codice)

In caso di trattamento di dati "sensibili" o giudiziari occorre altresì:

- proteggere i dati contro l'accesso abusivo mediante l'utilizzo di idonei strumenti elettronici;
- 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; i supporti rimovibili 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 non sono tecnicamente ricostruibili in alcun modo;
- adottare 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.

9.2.7 Certificazione da parte degli installatori (allegato B) punto 25 del Codice)

Infine, viene stabilito che, qualora l'adozione di misure minime di sicurezza avvenga avvalendosi di soggetti esterni, il titolare deve ricevere dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del disciplinare tecnico contenuto nell'allegato B) al Codice.

9.3 LE MISURE "MINIME" DI SICUREZZA PER I TRATTAMENTI DI DATI PERSONALI SENZA STRUMENTI ELETTRONICI

Qualora il trattamento di dati personali sia effettuato senza l'ausilio di strumenti elettronici (es. archivi cartacei), ai sensi dell'art. 35 del Codice occorre adottate le seguenti misure minime di sicurezza:

- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- previsione di procedure per un'idonea 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.

Le disposizioni attuative sono contenute nell'allegato B) punti 27 - 29 del Codice.

Istruzioni scritte

In particolare, 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.

Con cadenza almeno annuale deve essere aggiornata l'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.

Atti e documenti contenenti dati personali "sensibili" o giudiziari

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[67], e sono restituiti al termine delle operazioni affidate.

Non è però più espressamente richiesto che i suddetti atti e documenti siano conservati in contenitori muniti di serratura.

---

questione sulla scadenza di tale adempimento e in particolare sulla obbligatorietà della attestazione già nei bilanci compilati nel 2004 per il 2003. È da preferirsi prudenzialmente la tesi per cui già nel bilancio redatto nel 2004 l'osservanza degli obblighi di privacy sia un contenuto obbligatorio della relazione".

67 I documenti devono quindi essere custoditi in maniera tale che "*persone non autorizzate possano leggerli, copiarli, o comunque impossessarsene*" (Baffigo L. "Anche la password del Pc deve rispettare regole precise", *Il Sole - 24 Ore*, *Documenti* 15.12.2003, p. 7).

Accesso agli archivi contenenti dati personali "sensibili" o giudiziari

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 devono essere preventivamente autorizzate.

9.4 LA DISCIPLINA TRANSITORIA

L'art.180 co. 1 del Codice stabilisce, in via transitoria, che le misure minime di sicurezza da esso contemplate e che non erano invece previste dal DPR 318/99, sono adottate entro il **30.6.2004**[68].

I successivi co. 2 - 3 però stabiliscono che il titolare il quale, alla data dell'1.1.2004, dispone di strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione delle nuove misure minime di sicurezza, deve descrivere le ragioni medesime in un documento avente data certa da conservare presso la propria struttura[69]. In tal caso, il titolare è comunque tenuto ad:

- adottare ogni possibile misura di sicurezza in relazione agli strumenti elettronici detenuti, in modo da evitare, anche sulla base di idonee misure organizzative, logistiche o procedurali, un incremento dei rischi previsti dal citato art. 31 del Codice;
- adeguare i medesimi strumenti entro l'**1.1.2005**.

Il documento programmatico sulla sicurezza

Il suddetto regime transitorio dovrebbe applicarsi anche in relazione al documento programmatico sulla sicurezza[70].

Pertanto, i titolari che diventano assoggettati a tale adempimento sulla base delle nuove disposizioni del Codice dovrebbero redigere per la prima volta il documento programmatico sulla sicurezza entro il prossimo **30.6.2004**[71].
A partire dal 2005, invece, dovrà essere rispettata la scadenza a regime del 31 marzo.

Su tali aspetti appaiono comunque necessari chiarimenti ufficiali da parte del Garante[72].
Le conclusioni relative al termine per redigere il documento programmatico sulla sicurezza si riflettono poi in relazione all'obbligo della relativa indicazione nella relazione accompagnatoria del bilancio d'esercizio[73].

10 LA CESSAZIONE DEL TRATTAMENTO DEI DATI PERSONALI

- *In caso di cessazione del trattamento di dati personali non è più previsto un generale obbligo di notificazione al Garante della loro destinazione.*

68 Il concetto di misure minime di sicurezza "*non previste*" dalla precedente normativa dovrebbe essere interpretato sia da un punto di vista "oggettivo" (nuove misure introdotte dal Codice), che "soggettivo" (misure già previste dal DPR 318/99, ma il cui ambito di applicazione è stato esteso dal Codice ad altri titolari).

69 Sulla base del dato letterale della norma, non appare chiaro entro quale data deve essere redatto tale documento. Secondo una parte della dottrina, tale termine è scaduto al 31.12.2003 (si veda Baffigo L. "Anche la password del Pc deve rispettare regole precise", *Il Sole - 24 Ore, Documenti* 15.12.2003, p. 7) oppure all'1.1.2004 (si vedano Ghini P. e Ledda F. "Privacy: gli adempimenti di fine e inizio d'anno", *Guida al Lavoro*, 50, 2003, p. 11); suscita però qualche perplessità il fatto che tale adempimento si fosse dovuto effettuare addirittura prima o contestualmente dell'entrata in vigore del DLgs. 196/2003. Pertanto, appaiono auspicabili chiarimenti ufficiali che consentano di porre in essere tale adempimento entro il termine del 30.6.2004, come sostenuto da altra parte della dottrina (si vedano Berghella F. "Guida pratica alle nuove misure di sicurezza per la privacy", Bancaria Editrice, Roma, 2003, p. 214 e Ciccia A. "Codice della privacy, tutti gli adempimenti per le imprese", *Italia Oggi*, 29.12.2003, p. 16).

70 Si veda il precedente § 9.2.5.

71 Appare dubbia, invece, la possibilità di differire tale adempimento all'1.1.2005, nel rispetto delle condizioni previste dall'art. 180 co. 2 - 3 del Codice, in quanto la redazione del documento programmatico sulla sicurezza non sembra strettamente collegata all'adeguatezza tecnica degli strumenti elettronici posseduti. Sul punto sono comunque auspicabili chiarimenti ufficiali del Garante.

72 Si segnala, infatti, che alcuni Autori fanno decorrere il nuovo adempimento dal 2005 (si vedano Cherchi A. "Il Codice apre alla semplificazione", *Il Sole - 24 Ore*, 14.7.2003, p. 21, Finocchiaro G. "Nuove misure minime di sicurezza entro il 30 giugno 2004", *Il Sole - 24 Ore*, 30.7.2003, p. 19 e Baffigo L. "Il codice puntualizza la sicurezza nei flussi di dati", *Guida Normativa*, Dossier mensile n. 1, gennaio 2004, p. 120).

73 Si veda il precedente § 9.2.5.

In caso di cessazione, per qualsiasi causa, del trattamento dei dati personali, l'art. 16 co. 1 del Codice prevede, analogamente all'art. 16 co. 2 della L. 675/96, che i dati personali stessi possono essere:

- distrutti;
- ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati erano stati raccolti;
- conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;
- conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta.

Rispetto all'art. 16 co. 1 della L. 675/95, l'art. 16 del Codice non prevede più, in via generale, l'obbligo del titolare di notificare preventivamente al Garante la destinazione dei dati personali il cui trattamento è cessato.
Tuttavia, tale obbligo permane in relazione ai trattamenti di dati personali per i quali la notifica è ancora obbligatoria[74].

Inefficacia della cessione effettuata in violazione della disciplina

L'art. 16 co. 2 del Codice prevede che la cessione dei dati personali in violazione di quanto previsto "*è priva di effetti*". Secondo l'art. 16 co. 3 della L. 675/96, invece, tale cessione era "*nulla*".

11 I DATI PERSONALI RELATIVI AD ISCRITTI IN ALBI PROFESSIONALI

o *Il Codice prevede particolari disposizioni relative ai trattamenti di dati personali in relazione a soggetti iscritti in Albi professionali.*

L'art. 61 del Codice prevede particolari disposizioni in materia di dati relativi a soggetti iscritti in Albi professionali.

Viene infatti previsto che, agli effetti dell'applicazione delle disposizioni del Codice stesso, i dati personali diversi da quelli "sensibili" o giudiziari, che devono essere inseriti in un Albo professionale in conformità alla legge o ad un regolamento, possono essere comunicati a soggetti pubblici e privati[75] o diffusi[76], anche mediante reti di comunicazione elettronica. Può essere altresì menzionata l'esistenza di provvedimenti che dispongono la sospensione o che incidono sull'esercizio della professione.

Inoltre, l'Ordine o il Collegio professionale può, a richiesta della persona iscritta nell'Albo che vi ha interesse, integrare i suddetti dati con ulteriori dati pertinenti e non eccedenti in relazione all'attività professionale.

Infine, a richiesta dell'interessato, l'Ordine o il Collegio professionale può altresì fornire a terzi notizie o informazioni relative, in particolare, a speciali qualificazioni professionali non menzionate nell'Albo, ovvero alla disponibilità ad assumere incarichi o a ricevere materiale informativo a carattere scientifico inerente anche a convegni o seminari.

12 LE SANZIONI

o *Le violazioni della disciplina sulla privacy sono punite con sanzioni amministrative e penali.*
Suscita però particolare perplessità l'insufficiente graduazione delle sanzioni rispetto all'effettiva gravità della violazione, specie in caso di inosservanza di semplici aspetti formali. Inoltre, non viene prevista alcuna differenziazione in relazione alla natura e alla dimensione del soggetto sanzionato (persone fisiche "private", professionisti, piccole e medie imprese, soggetti no-profit, grandi imprese).

Per la violazione delle disposizioni in materia di trattamento dei dati personali, gli artt. 161 - 172 del Codice prevedono le seguenti sanzioni:

- violazione delle norme sull'**informativa all'interessato** ⇑ sanzioni amministrative pecuniarie da 3.000,00 a 18.000,00 euro o, nei casi di dati "sensibili", "semisensibili" o giudiziari, da 5.000,00 a 30.000,00 euro; la somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore;

[74] Si veda il precedente § 5.

[75] Quando la comunicazione è prevista da una norma di legge o di regolamento, ovvero, in mancanza, quando la comunicazione è comunque necessaria per lo svolgimento di funzioni istituzionali, ai sensi dell'art. 19 co. 2 del Codice.

[76] Quando la diffusione è prevista da una norma di legge o di regolamento, ai sensi dell'art. 19 co. 3 del Codice.

- **omessa o infedele notificazione al Garante** ⇑ sanzioni amministrative pecuniarie da 10.000,00 a 60.000,00 euro;
- violazione delle norme relative sulla **cessazione del trattamento o di altre disposizioni** in materia di disciplina dei dati personali ⇑ sanzioni amministrative pecuniarie da 5.000,00 a 30.000,00 euro;
- **omissione di fornire le informazioni o di esibire i documenti** richiesti dal Garante ⇑ sanzioni amministrative pecuniarie da 4.000,00 a 24.000,00 euro;
- **trattamento illecito di dati personali** (violazione delle norme sul consenso dell'interessato, sullo *spamming*, sui dati "sensibili", "semisensibili" o giudiziari, sulla comunicazione e diffusione, sul trasferimento all'estero, ecc.), **falsità nelle notificazioni** al Garante o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti ⇑ sanzioni penali con reclusione fino a tre anni;
- **inosservanza dei provvedimenti del Garante** ⇑ sanzioni penali con reclusione fino a due anni;
- **omessa adozione delle misure minime di sicurezza** ⇑ sanzioni penali con arresto fino a due anni o con ammenda da 10.000,00 a 50.000,00 euro; l'art. 169 co. 2 del Codice, così come il precedente art. 36 co. 2 della L. 675/96, prevede un meccanismo di "ravvedimento operoso" in relazione a tale violazione, con conseguente estinzione del reato, basato:
  - sulla regolarizzazione entro un determinato termine, comunque non superiore a sei mesi;
  - sul pagamento di una sanzione ridotta, pari al quarto del massimo dell'ammenda (quindi 12.500,00 euro).

Inoltre, altre violazioni sanzionate penalmente sono previste, in particolare:

- dall'art. 491-*bis* c.p. ⇑ falsificazione di documenti informatici;
- dall'art. 615-*ter* c.p. ⇑ accesso abusivo ad un sistema informatico o telematico;
- dall'art. 615-*quater* c.p. ⇑ detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;
- dall'art. 615-*quinquies* c.p. ⇑ diffusione di programmi idonei a danneggiare o interrompere un sistema informatico;
- dagli artt. 616 e 617-*sexies* c.p. ⇑ violazione di corrispondenza telematica;
- dall'art. 617-*quater* c.p. ⇑ intercettazione di comunicazioni informatiche o telematiche;
- dall'art. 635-*bis* c.p. ⇑ danneggiamento di sistemi informatici o telematici;
- dall'art. 640-*ter* c.p. ⇑ frode informatica.

13 LA RESPONSABILITÀ CIVILE

o *Le violazioni della disciplina sulla* privacy *sono altresì fonte di responsabilità civile per danni.*

L'art. 15 del Codice conferma la disposizione dell'art. 18 della L. 675/96, prevedendo una particolare ipotesi di responsabilità extracontrattuale per i danni cagionati per effetto del trattamento di dati personali, con un richiamo alla disciplina prevista dall'art. 2050 c.c. per l'esercizio di attività pericolose.
Viene quindi confermato un orientamento molto rigoroso del legislatore, poiché l'art. 2050 c.c. configura una responsabilità extracontrattuale "quasi oggettiva", in quanto l'obbligo del risarcimento sussiste nei confronti di chiunque abbia cagionato un danno, senza che assuma rilievo l'attribuibilità del fatto a titolo di dolo o colpa, ma con l'unica prova liberatoria di aver adottato *tutte* le misure idonee ad evitare il danno. Tali misure possono essere ulteriori rispetto alle misure minime di sicurezza previste dal Codice.

Il risarcimento del danno non patrimoniale

Viene ora espressamente previsto che, in caso di violazione della disciplina in materia di modalità e trattamento dei dati, di cui all'art. 11 del Codice[77], è risarcibile anche il danno non patrimoniale.

[77] Si veda il precedente § 6. Imperiali Ri., Imperiali Ro. "Basta il danno per aprire la via al risarcimento", *Guida Normativa*, Dossier mensile n. 1, gennaio 2004, p. 111, osservano come "*la quantificazione del danno non patrimoniale si basa su una valutazione di equità, ai sensi degli articoli 1226 e 2056 del codice civile*".

Il "nesso di causalità"

Peraltro, rimane in ogni caso a carico del danneggiato l'onere di provare l'esistenza del nesso causale fra l'attività di trattamento dei dati personali e l'evento dannoso[78].

14 TABELLE RIEPILOGATIVE

Di seguito vengono proposte alcune tabelle riepilogative in relazione agli adempimenti previsti dal Codice della privacy. Il riferimento è, in particolare, a studi professionali e a piccole imprese.

14.1 ASPETTI ORGANIZZATIVI DELLA TUTELA DEI DATI PERSONALI

L'applicazione pratica del DLgs. 196/2003 richiede:

- l'esame delle disposizioni normative;
- l'adeguamento alla realtà organizzativa dello studio professionale/dell'azienda.

Con riferimento ai soggetti che già rispettano le disposizioni della previgente normativa occorre:

- individuare le novità;
- verificare la compatibilità e la sufficienza di quanto già fatto alla luce delle nuove disposizioni;
- effettuare gli adeguamenti richiesti.

In pratica, è verosimile che per la maggior parte dei soggetti gli adeguamenti consistano in:

- aggiornare i modelli di informativa e di richiesta di consenso dell'interessato con i nuovi riferimenti normativi;
- modificare le misure di sicurezza, adeguandole, entro il 30.6.2004, ai nuovi requisiti minimi come illustrato nel precedente § 9;
- predisporre il documento programmatico sulla sicurezza, come illustrato nel precedente § 9.2.5;
- indicare nella relazione accompagnatoria al bilancio, ove obbligatoria, l'avvenuta redazione o aggiornamento del suddetto documento programmatico sulla sicurezza, come illustrato nel precedente § 9.2.5.

Si ricorda che l'omessa adozione delle misure minime di sicurezza è punita con la sanzione penale dell'arresto fino a due anni o con l'ammenda da 10.000,00 a 50.000,00 euro.

14.1.1 L'esame delle disposizioni normative

Dall'esame delle disposizioni normative emerge che:

- il DLgs. 196/2003 non si applica a tutti i dati aziendali (o degli studi professionali), né a tutti i trattamenti di dati, ma esclusivamente ai trattamenti di dati personali, come definiti dallo stesso;
- il DLgs. 196/2003 non costituisce l'unica fonte di obblighi legali in caso di trattamenti di dati;
- per i vari trattamenti di dati esistono numerose altre fonti di obblighi:
  - disposizioni normative (ad es. obblighi contabili, previdenziali, di sicurezza del lavoro, ecc.);
  - obblighi contrattuali (ad es. nascenti dallo svolgimento di un rapporto di prestazione d'opera intellettuale[79] o di mandato[80]).

14.1.2 Le specifiche finalità e l'interesse del soggetto obbligato

Inoltre, indipendentemente dagli obblighi giuridici, esiste un interesse del titolare ad organizzare e a gestire i trattamenti di dati in condizioni di economicità, di efficienza e di sicurezza.
Per certi tipi di attività uno o più trattamenti di dati costituiscono l'elemento centrale dell'attività stessa, tutelato, valorizzato e frutto, a volte, di importanti investimenti.

78 Si vedano le sentenze della Corte di Cassazione 8.5.1984 n. 2796 e 21.6.84 n. 3678.

79 Artt. 2230 ss. c.c., con obbligo di specifiche modalità di esecuzione dell'opera (art. 2232 c.c., norme deontologiche sul segreto professionale) e di specifici termini di durata del trattamento (art. 2235 c.c.).

80 Artt. 1703 ss. c.c., con, ad esempio, l'obbligo di rimettere al mandante tutto ciò che il mandatario ha ricevuto a causa del mandato (art. 1713 c.c.).

14.1.3 Alcuni tipici trattamenti di dati e categorie degli stessi

A scopo esemplificativo, si elencano nella seguente tabella alcuni tipici trattamenti di dati, frequentemente presenti in studi professionali o in piccole aziende, indicando la possibile classificazione ai sensi del DLgs. 196/2003.

TRATTAMENTI DI DATI	CLASSIFICAZIONE EX DLGS. 196/2003
Elenchi soci / amministratori /sindaci	Dati personali, eventualmente dati giudiziari
Archivi di contabilità generale	Dati/Dati personali
Elenchi clienti / fornitori	Dati personali
Dati di dipendenti / collaboratori / consulenti	Dati personali, eventualmente dati "sensibili"
Rubriche telefoniche	Dati personali
Biblioteca	Dati
Raccolta dati su autori	Dati/Dati personali
Fascicoli tecnici / di studio	Dati
Mailing list / elenchi di clienti potenziali	Dati personali, eventualmente dati "sensibili"
Dichiarazioni e dati fiscali	Dati personali, eventualmente dati "sensibili" per spese mediche, erogazioni a favore di partiti e confessioni religiose, scelte per la destinazione dell'otto per mille dell'IRPEF, ecc.
Dichiarazioni e dati previdenziali	Dati personali, eventualmente dati "sensibili"
Contenzioso	Dati personali, eventualmente dati "sensibili"
Archivio unico informatico (L. 197/91)	Dati personali

Legenda
Dati: non rientrano nei presupposti applicativi del DLgs. 196/2003.
Dati personali: rientrano nei presupposti applicativi del DLgs. 196/2003.
Dati sensibili: rientrano nei presupposti applicativi del DLgs. 196/2003, con le specifiche ulteriori misure cautelative.

14.1.4 Aspetti organizzativi e giuridici della tutela dei dati - Bozza di procedura

L'applicazione pratica delle disposizioni normative sulla tutela dei dati richiede quindi di sapere *capire* ed *organizzare* tali diversi aspetti.
Schematizzando, l'analisi e l'organizzazione ai fini della tutela dei dati sembra richiedere le fasi e le verifiche giuridiche indicate nella seguente tabella.

ASPETTI ORGANIZZATIVI	ASPETTI GIURIDICI
Individuare i trattamenti di dati	
Classificare i trattamenti di dati	Analizzare: • disposizioni normative • obblighi contrattuali • definizioni del DLgs. 196/2003
Individuare i fattori di rischio	
Individuare le misure di sicurezza	Analizzare: • norme e allegati tecnici del DLgs. 196/2003 • eventuali altre disposizioni normative • eventuali provvedimenti/chiarimenti del Garante
Predisporre l'organigramma e le procedure	
Applicare le procedure	
Controllare il rispetto delle procedure	

Tali fasi del processo organizzativo sembra vadano rispettate per ogni attività, di ogni dimensione o forma giuridica, indipendentemente dalle caratteristiche dei trattamenti di dati eseguiti.
Ovviamente, i *problemi giuridici* e le *soluzioni organizzative* potranno essere ben *diversi a seconda dei casi*.

14.1.5 Trattamenti di dati personali - Bozza di procedura

Indicativamente, nella seguente tabella si fornisce una bozza di procedura per i trattamenti di dati personali.
Preliminarmente, occorrerà individuare i soggetti obbligati (titolare, responsabile, incaricato), come definiti dal DLgs. 196/2003.
Tale procedura potrà poi essere adottata per singolo trattamento o per categorie di trattamenti, a seconda delle proprie scelte organizzative.

Aspetti organizzativi della tutela dei dati - Mansionario

TRATTAMENTO/I: .....

SOGGETTI: .....

Titolare/i: .....

Responsabile/i: .....

Incaricato/i: .....

ADEMPIMENTI	SOGGETTI		
	Titolare	***Responsabile***	***Incaricato***
Decidere le finalità e le modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza	X		
Individuare gli eventuali responsabili ed incaricati	X		
Eventuali adempimenti pubblicitari per la nomina	X		
Esame degli aspetti organizzativi	X	X	
Individuare le misure di sicurezza	X	X	
Predisporre le bozze di informativa e di consenso	X	X	
Richiedere l'autorizzazione al Garante, se obbligatorio	X	X	
Notificare il trattamento al Garante, se obbligatorio	X	X	
Rilasciare l'informativa agli interessati		X	X
Raccogliere il consenso degli interessati		X	X
Adottare le misure di sicurezza		X	X
Controllare il rispetto delle procedure	X		

14.1.6 Trattamenti di dati - Fattori di rischio - Possibili soluzioni

Relativamente all'individuazione dei fattori di rischio, sembra opportuno ricordare che questi dipendono dalle modalità concrete di organizzazione della singola attività. L'eventuale adozione delle necessarie misure di sicurezza non potrà certo prescindere da tali modalità. Le soluzioni procedurali, informatiche e non, potranno essere diversissime, a seconda dei casi.
A puro titolo esemplificativo, si elencano nella seguente tabella alcuni tipici fattori di rischio in caso di trattamenti di dati, con alcune soluzioni che *buon senso* e *tecnologia* sembrano consentire.

FATTORI DI RISCHIO NEL TRATTAMENTO DI DATI	POSSIBILI SOLUZIONI
Distruzioni, incendio di dati	Rispetto delle normative sulla sicurezza del lavoro Archiviazioni in armadi antincendio/blindati
Furto di dati (es. documenti, dischetti, ecc.)	Porte/finestre di sicurezza/blindate Controllo degli accessi Armadi/contenitori chiusi
Smarrimento fisico di dati	Organizzazione sistematica dei dati Fare copie/salvataggi
Consegna non autorizzata di dati a terzi	Rendere obbligatoria l'autorizzazione del titolare/responsabile
Distruzione di dati in maniera incompleta	Utilizzo di macchine distruggi-documenti
Accessi indesiderati su trattamenti di dati con elaboratori	Adozione e rispetto delle misure minime di sicurezza Creare directory non accessibili/riservate Chiusura dello schermo in mancanza dell'utilizzatore
Accessi indesiderati su trattamenti di dati con elaboratori connessi in rete	Adozione e rispetto delle misure minime di sicurezza Seguire le "*best practices*" in materia di misure di sicurezza, come[81]: • disattivare i servizi telematici non necessari; • disattivare temporaneamente i servizi in rete eventualmente minacciati (es. da virus); • configurare il server *e-mail* in modo da bloccare o rimuovere le *e-mail* con allegati file che comunemente diffondono i virus; • isolare rapidamente i computer "infettati"; • addestrare tutti gli addetti a non aprire file allegati ad *e-mail* se non di fonte certa e preannunciati; • non eseguire software scaricati da internet senza preventiva verifica con l'antivirus.
Intercettazioni di dati	Utilizzo di sistemi crittografici
Perdita di dati trattati su elaboratori (es. per *black-out*)	Fare copie/salvataggi Tenere le copie in luoghi differenziati e sicuri Utilizzo di gruppi di continuità elettrica

[81] Quanto segue è una libera traduzione di alcune delle "raccomandazioni antivirus" di una delle più note case fornitrici di prodotti di sicurezza informatica.

14.2 TABELLA RIEPILOGATIVA DELLE MISURE MINIME DI SICUREZZA

Di seguito viene proposta una tabella riepilogativa, liberamente semplificata, delle principali misure minime di sicurezza previste dal DLgs. 196/2003[82].

TIPOLOGIA DI TRATTAMENTO	MISURE MINIME DI SICUREZZA	§ DI RIFERIMENTO
Archivi informatici - Trattamenti di dati personali con strumenti elettronici	• individuare e "proceduralizzare" le seguenti fasi:	9.2
	– individuare gli addetti alla gestione o alla manutenzione di strumenti elettronici; procedere al relativo aggiornamento	9.2
	– prima dell'inizio del trattamento, individuare per ciascun incaricato i dati e i trattamenti cui può accedere; procedere all'aggiornamento almeno una volta all'anno	9.2.2 9.2.1
	• l'accesso al/i trattamento/i autorizzato/i è consentito se:	
	– per ogni incaricato si associa PIN (o altro strumento) e *password*[83]	
	– si danno istruzioni per la segretezza della *password* e la custodia dell'eventuale altro strumento di identificazione	
	– l'incaricato modifica la *password* al primo utilizzo	
	– l'incaricato aggiorna la p*assword* almeno ogni sei mesi	9.2.1
	• disattivazione accessi a soggetti non più incaricati	9.2.3
	• protezione di strumenti elettronici e di dati	9.2.4
	• aggiornamento *software* e antivirus ogni anno	9.2.7
	• *back-up* dei dati almeno settimanale	
	• interventi per adozione delle misure minime di sicurezza effettuati da soggetti esterni; farsi rilasciare certificazione dagli installatori	
Archivi informatici - Trattamenti di dati "sensibili" o giudiziari con strumenti elettronici	Come sopra, in più:	
	• l'incaricato aggiorna la *password* almeno ogni tre mesi	9.2.1
	• aggiornamento software e antivirus ogni sei mesi	9.2.3
	• proteggere i dati contro l'accesso abusivo mediante idonei strumenti elettronici	9.2.6
	• dare istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili (es. floppy, cartucce, ecc.) su cui sono memorizzati i dati	9.2.6
	• adottare misure in caso di danneggiamenti dei dati e degli strumenti elettronici	9.2.6 9.2.5
	• il titolare predispone entro il 31 marzo di ogni anno il documento programmatico sulla sicurezza (DPS)	9.2.5
	• il titolare riferisce annualmente sul DPS nella relazione accompagnatoria al bilancio	
Archivi cartacei - Trattamenti di dati personali senza strumenti elettronici	• individuare trattamenti consentiti ai singoli incaricati	

82 Per l'esame completo della disciplina si rimanda ai citati paragrafi della presente scheda.

83 *Password* con almeno otto caratteri o, se inferiore, con il numero massimo consentito dallo strumento elettronico. Non deve contenere riferimenti agevolmente riconducibili all'incaricato.

TIPOLOGIA DI TRATTAMENTO	MISURE MINIME DI SICUREZZA	§ DI RIFERIMENTO
	• dare istruzioni scritte per controllo e custodia degli atti e dei documenti contenenti dati personali • aggiornare periodicamente (almeno annualmente)	9.3
Archivi cartacei - Trattamenti di dati sensibili o giudiziari senza strumenti elettronici	Come sopra, in più: • l'accesso agli archivi è controllato: – le persone ammesse a qualunque titolo dopo l'orario di chiusura sono identificate e registrate – se gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati di vigilanza, le persone che vi accedono sono preventivamente autorizzate	9.3

14.3 TABELLA RIEPILOGATIVA DELLE SCADENZE

Di seguito viene proposta una tabella riepilogativa delle scadenze previste dal DLgs. 196/2003.

DECORRENZA/ TERMINE	ADEMPIMENTO	NORMA
Dall'1.1.2004	Entrata in vigore del Codice della privacy	Art. 186 del DLgs. 196/2003
31 marzo di ogni anno	Redazione del documento programmatico sulla sicurezza. Il titolare deve riferire, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.	Art. 34 e punti 19 e 26 dell'allegato B) del DLgs. 196/2003
30.4.2004	Effettuazione della notificazione al Garante, mediante trasmissione in via telematica con utilizzo della firma digitale, in relazione ai trattamenti di determinati dati personali alla data dell'1.1.2004	Artt. 37, 38 e 181 del DLgs. 196/2003
30.6.2004	Adozione delle nuove misure minime di sicurezza, salvo attestazione del titolare, in un documento avente data certa da conservare presso la propria struttura, che all'1.1.2004 dispone di strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione delle nuove misure minime di sicurezza.	Artt. 31 - 36, 180 e allegato B) del DLgs. 196/2003
1.1.2005	Adozione delle nuove misure minime di sicurezza da parte dei titolari che all'1.1.2004 non disponevano di idonei strumenti elettronici e che lo hanno attestato nell'apposito documento con data certa.	Artt. 31 - 36, 180 e allegato B) del DLgs. 196/2003