A.V.M. S.p.A.
Isola Nova del Tronchetto, 33
30135 Venezia

T. +39 041 27 22 111
F. +39 041 27 22 098
avm@avmspa.it

Guida Privacy aggiornata al 2016

GUIDA PRIVACY
D.Lgs. 30 Giugno 2003 n. 196
CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Il 1° gennaio 2004 è entrato in vigore il Codice della Privacy (d'ora innanzi il "Codice"), approvato con D.Lgs. 196/2003, emanato al fine di salvaguardare il diritto alla riservatezza di tutti i soggetti i cui dati personali siano trattati a qualsiasi titolo da terzi. Detto Codice ha abrogato sia la L.675/96 (c.d. Legge sulla Privacy), sia il DPR n. 318/99 in tema di misure minime di sicurezza.
Riportiamo di seguito alcune definizioni elencate all'art. 4 co. 1 del Codice, onde facilitare la lettura della presente Guida Privacy.
a) "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;
b) "dato personale", qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;
d) "dati 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;
e) "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1,lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
f) "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;
g) "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;
h) "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
i) "interessato", la persona fisica, cui si riferiscono i dati personali;
f) "contraente", qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;
Guida Privacy aggiornata con le modifiche introdotte dal D.Lgs. n.69 del 28 maggio 2012
g) "utente", qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

l) "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;
m) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
n) "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
o) "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
p) "banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
q) "Garante", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

Oggetto e Ambito di applicazione
Il Codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.
Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del presente codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione.
Il Codice prevede, a carico del titolare del trattamento, una serie di specifici adempimenti:
- l'obbligo di notificare preventivamente al Garante, (Autorità pubblica preposta al controllo della puntuale osservanza delle disposizioni in materia di privacy), la propria intenzione di procedere al trattamento di dati personali, qualora ne ricorrano i presupposti indicati all'art. 37 del Codice;
- l'obbligo di fornire al soggetto, i cui dati vengono trattati ("interessato"), l'informativa ex art. 13 del Codice contenente: le modalità e le finalità del trattamento, la natura obbligatoria o facoltativa del conferimento dei dati al titolare e la conseguenza di un eventuale rifiuto di rispondere, i soggetti o le categorie di soggetti cui verranno comunicati i dati raccolti (compresi responsabili e incaricati che possono venire a conoscenza dei dati medesimi);
- il riconoscimento all'interessato dei diritti previsti dall'art. 7 del Codice; gli estremi identificativi del titolare e dei responsabili, risultando sufficiente, qualora quest'ultima categoria sia costituita di più soggetti, l'indicazione di uno solo di essi, oltre all'indicazione di un sito o altro luogo, ove trovare l'elenco completo ed aggiornato dei responsabili.
- l'acquisizione del consenso dell'interessato al trattamento dei dati personali, ai sensi dell'art. 23 del Codice, secondo il quale "Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato".
L'art. 24 del Codice disciplina le ipotesi in cui il trattamento può essere eseguito anche senza il consenso dell'interessato (fermo restando l'obbligo di informativa); ciò è previsto quando ad esempio il trattamento:
- è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- è 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;
- riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;
- riguarda i dati contenuti nei curricula inviati spontaneamente dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro, ecc..

- riguarda la comunicazione di dati tra società, enti o associazioni con società controllanti, controllate o collegate ai sensi dell'articolo 2359 del codice civile ovvero con società sottoposte a comune controllo, nonché tra consorzi, reti di imprese e raggruppamenti e associazioni temporanei di imprese con i soggetti ad essi aderenti, per le finalità amministrativo contabili, di cui all'art. 34, comma 1-ter del Codice e purché dette finalità siano contenute nell'informativa rilasciata agli interessati, ex art. 13 del Codice.

Dati sensibili e giudiziari

I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti. Tale principio generale non trova applicazione per i seguenti trattamenti:

a) trattamenti di dati 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. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante;

b) trattamenti di dati 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;

b-bis) trattamenti di dati contenuti nei curricula, nei casi di cui all'articolo 13, comma 5-bis del Codice (ricezione di curricula spontaneamente trasmessi dagli interessati).

I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante:

a) quando il trattamento 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'articolo 13 del Codice;

b) quando il trattamento 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;

c) quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

d) quando 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 del codice di deontologia e di buona condotta di cui all'articolo 111 del Codice.
Con riferimento alla richiesta di autorizzazione, il Garante ha emanato una serie di provvedimenti (sette autorizzazioni generali) con i quali ha autorizzato determinate categorie di soggetti (tra i quali datori di lavoro, associazioni, fondazioni, liberi professionisti, esercenti l'attività sanitaria, investigatori privati, agenzie di viaggio e altre società di servizi) al trattamento in via generale dei dati sensibili di coloro con i quali intercorre un rapporto di lavoro, o di altro tipo, connesso, comunque, all'attività istituzionalmente svolta da tali categorie di soggetti.
Ciò consente alle suddette categorie di evitare l'adempimento della richiesta di autorizzazione al Garante per tale ambito di trattamento, fermo restando, in ogni caso, l'obbligo (quantomeno per i dati sensibili) di richiedere il consenso scritto all'interessato, salvo i casi per i quali il consenso non è richiesto.
Per quanto riguarda il trattamento dei dati giudiziari da parte di privati o di enti pubblici economici, l'art. 27 del Codice lo consente solo se autorizzato da espressa disposizione di legge o provvedimento da parte del Garante, che specifichi le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e le operazioni eseguibili. In presenza di tali requisiti il trattamento dei dati giudiziari non richiede il consenso da parte dell'interessato e, pertanto, in assenza degli stessi, il trattamento non è consentito neanche in presenza di un eventuale consenso.

Trasferimento dati all'estero
Gli articoli da 42 a 45 del Codice disciplinano il trasferimento dei dati all'estero.
Il trasferimento è consentito senza la necessità di porre in essere alcuna formalità qualora lo stesso avvenga (dall'Italia) verso Paesi dell'U.E.
In altri casi il trasferimento verso un Paese non appartenente all'Unione Europea è consentito quando è autorizzato dal Garante sulla base di adeguate garanzie per i diritti degli interessati.
Tali garanzie possono essere individuate:

- dal Garante, qualora il trasferimento avvenga nell'ambito di società appartenenti al medesimo gruppo, tra le quali siano state sottoscritte apposite clausole contrattuali, o esistano apposite regole di condotta;
- da decisioni della Commissione Europea che constata che alcune clausole contrattuali offrono garanzie sufficienti. In tal senso, ad oggi la Commissione ha individuato due differenti tipologie di clausole tipo: una per il trasferimento dei dati da titolare a titolare e una per il trasferimento dei dati da titolare a responsabile.

In ogni caso il trasferimento di dati all'estero è possibile solo nel caso in cui sussistano taluni presupposti espressamente individuati all'art. 43 del Codice (lett. da a) ad f), tra i quali i più frequenti risultano essere il consenso dell'interessato (lett. a) - consenso che deve essere dato per iscritto nel caso di dati sensibili - e la necessità del trasferimento 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 (lett. b).

MISURE DI SICUREZZA
TITOLO V, Capi I e II, e Allegato B del Codice
Le disposizioni in materia di misure di sicurezza sono contenute negli artt. 31-36 del Codice e nel disciplinare tecnico in materia di misure minime di sicurezza, che è parte integrante del Codice, di cui costituisce l'Allegato B.

Prima di procedere ad indicare il contenuto delle dette disposizioni, onde favorirne la comprensione, si elencano le seguenti definizioni.
Definizioni
a) "misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
b) "strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
c) "autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
d) "credenziali di autenticazione", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
e) "parola chiave", 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;
f) "profilo di autorizzazione", 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;
g) "sistema di autorizzazione", 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.
Disposizioni contenute nel Codice
Con riferimento alle disposizioni, il cui contenuto viene di seguito riassunto, precisiamo che il legislatore ha operato una prima distinzione tra misure di sicurezza (artt. 31 e 32) e misure minime di sicurezza (art. 33-36).
Quanto alle **misure minime di sicurezza**, con riferimento alle quali si distingue a seconda che il trattamento avvenga con o senza strumenti elettronici, si ricorda quanto segue.
1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31 del Codice, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel Capo II, Titolo V, Parte I del Codice o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali (art. 33).
2. Nel caso in cui un trattamento avvenga con strumenti elettronici (art. 34), occorre adottare, in particolare, 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.
**(comma 1 bis dell'art. 34) Per i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori, anche se extracomunitari, compresi quelli relativi al coniuge e ai parenti, la tenuta di un aggiornato documento programmatico sulla sicurezza è sostituita dall'obbligo di autocertificazione, resa dal titolare del trattamento ai sensi dell' articolo 47 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, di trattare soltanto

tali dati in osservanza delle misure minime di sicurezza previste dal presente codice e dal disciplinare tecnico contenuto nell'allegato B) al Codice, in ordine all'adozione delle sopra indicate misure minime.
**(Segnaliamo che all'art. 34 del Codice è stata soppressa la lettera g) ed è stato abrogato il comma 1 bis, per effetto dell'entrata in vigore del D.L. del 9 febbraio 2012 n. 5 "Disposizioni urgenti in materia di semplificazione e di sviluppo", convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35).
3. Nel caso di trattamenti senza l'ausilio di strumenti elettronici (art. 35) occorre adottare le seguenti misure minime:
a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c) 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.
Disposizioni contenute nell'Allegato B al Codice.

Trattamenti con strumenti elettronici
Di seguito vengono illustrate le modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici.

Sistema di autenticazione informatica (punti da 1 a 11 dell'All. B)
Il trattamento di dati personali con strumenti elettronici e' consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

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

Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione (punti da 12 a 14 dell'All. B)
Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione. 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.
Altre misure di sicurezza (punti da 15 a 18 dell'All. B)
Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

***Documento programmatico sulla sicurezza (punto 19 dell'All. B)**
Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:
- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi

che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.
*(Segnaliamo che la regola 19 dell'Allegato B) che disciplina il Documento Programmatico sulla sicurezza, è stata soppressa, per effetto dell'entrata in vigore del D.L. del 9 febbraio 2012 n. 5 "Disposizioni urgenti in materia di semplificazione e di sviluppo", convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35).

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari (punti da 20 a 23 dell'All. B)

I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del Codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti, accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia (punti 25-26 dell'All. B)

Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
*Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

*(Segnaliamo che la regola 26 dell'Allegato B) è stata soppressa, per effetto dell'entrata in vigore del D.L. del 9 febbraio 2012 n. 5 "Disposizioni urgenti in materia di semplificazione e di sviluppo", convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35).

Trattamenti senza l'ausilio di strumenti elettronici (punti da 27 a 29 dell'All. B)
Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici.
Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
L'accesso agli archivi contenenti dati sensibili o giudiziari e' controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

PRINCIPALI SANZIONI
Le sanzioni previste dalla normativa sono di natura penale, amministrativa e civile.

A) ILLECITI PENALI
• **Trattamento illecito di dati - Art. 167**
1.trattamento dei dati personali in violazione degli artt. 18 (trattamenti effettuati da soggetti pubblici), 19 (trattamento di dati diversi da quelli sensibili o giudiziari); 23 (consenso); 123 (trattamento di dati relativi ad abbonati e utenti con riferimento a comunicazione elettronica); 126 (trattamento di dati relativi all'ubicazione con riferimento a comunicazione elettronica); 130 (comunicazioni indesiderate), ovvero in applicazione dell'art. 129, da parte di chiunque, al fine di trarne per sé o per gli altri profitto o di recare ad altri un danno, salvo che il fatto costituisca più grave reato.
Sanzione: reclusione da 6 a 18 mesi. Se il fatto consiste nella comunicazione o nella diffusione reclusione da 6 a 24 mesi.
2. trattamento di dati personali in violazione degli artt. 17 (trattamento che presenta rischi specifici), 20 (trattamento dei dati sensibili), 21 (trattamento dei dati giudiziari), 22 co. 8 e 11 (trattamento dei dati idonei a rivelare lo stato di salute), 25 (dati sensibili e giudiziari nell'ambito di test psico-attitudinali), 26 (garanzie per i dati sensibili); 27 (garanzie per i dati giudiziari) e 45 (trasferimenti vietati) al fine di trarne per sé o per altri profitto o di recare ad altri un danno, salvo che il fatto non costituisca più grave reato.
Sanzione: reclusione da 1 a 3 anni se dai fatti deriva nocumento.
• **Falsità nelle dichiarazioni e notificazioni al Garante - Art. 168**
chiunque nelle comunicazioni di cui all'articolo 32-bis, commi 1 e 8, nelle notificazioni ex art. 37 o in comunicazioni, atti, documenti resi o esibiti in un procedimento dinanzi al Garante dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi.
Sanzione: reclusione, salvo che il fatto costituisca più grave reato, da sei mesi a tre anni.
• **Misure minime di sicurezza – art. 169**

1. chiunque essendovi tenuto omette di adottare le misure minime previste dall'art. 33 del Codice
Sanzione: arresto sino a due anni.
2. all'autore del reato, all'atto dell'accertamento è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa.
L'adempimento e il pagamento estinguono il reato.

• **Inosservanza di provvedimenti del Garante - Art. 170**

inosservanza dei provvedimenti adottati dal Garante ai sensi degli artt. 26, co. 2 (dati sensibili), 90 (dati genetici), 150 co. 1 e 2, (provvedimenti a seguito di ricorso), 143 co. 1 lett. c) (blocco o divieto di trattamento di dati personali).
Sanzione: reclusione da tre mesi a due anni.

B) VIOLAZIONI AMMINISTRATIVE

• **Omessa o inidonea informativa all'interessato - Art. 161**

per le violazioni di cui all'art. 13 del Codice (informativa).
Sanzione: pagamento di una somma da 6.000 euro a 36.000 euro.

• **Altre fattispecie - Art. 162**

1. La cessione dei dati in violazione di quanto previsto dall'articolo 16, comma 1, lettera b) del Codice, o di altre disposizioni in materia di disciplina del trattamento dei dati personali è punita con la sanzione amministrativa del pagamento di una somma da 10.000 euro a 60.000 euro.
2. La violazione della disposizione di cui all'articolo 84, co. 1 del Codice, è punita con la sanzione amministrativa del pagamento di una somma da 1.000 euro a 6.000 euro.
2-bis In caso di trattamento di dati personali effettuato in violazione delle misure indicate nell'art. 33 (misure minime di sicurezza) o delle disposizioni indicate nell'art. 167 (trattamento illecito di dati) è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da 10.000 euro a 120.000 euro. Nei casi di cui all'art. 33 è escluso il pagamento in misura ridotta.
2-ter In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieti di cui, rispettivamente, all'articolo 154, comma 1, lettere c) e d), è altresì applicata, in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da 30.000 euro a 180.000 euro.
2-quater. La violazione del diritto di opposizione nelle forme previste dall'articolo 130, comma 3- bis, e dal relativo regolamento è sanzionata ai sensi del comma 2-bis del presente articolo.

• **Omessa o incompleta notificazione - Art. 163**

Sanzione: pagamento di una somma da 20.000 euro a 120.000 euro.

• **Omessa informazione o esibizione al Garante - Art. 164**

Sanzione: pagamento di una somma da 10.000 euro a 60.000 euro.

• **Casi di minore gravità e ipotesi aggravate – Art. 164-bis**

1. Se taluna delle violazioni di cui agli articoli 161, 162, 162 ter, 163 e 164 è di minore gravità, avuto altresì riguardo alla natura anche economica o sociale dell'attività svolta, i limiti minimi e massimi stabiliti dai medesimi articoli sono applicati in misura pari a due quinti.
2. In caso di più violazioni di un'unica o di più disposizioni di cui al Capo I, Titolo III, Parte II del Codice, a eccezione di quelle previste dagli articoli 162, comma 2, 162-bis e 164, commesse anche in tempi diversi in relazione a banche di dati di particolare rilevanza o dimensioni, si applica la sanzione amministrativa del pagamento di una somma da 50.000 a 300.000 euro. Non è ammesso il pagamento in misura ridotta.

3. In altri casi di maggiore gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolge numerosi interessati, i limiti minimo e massimo delle sanzioni di cui al Capo I, Titolo III, Parte II del Codice sono applicati in misura pari al doppio.
4. Le sanzioni di cui al Capo I, Titolo III, Parte II del Codice (ovvero le sanzioni amministrative) possono essere aumentate fino al quadruplo quando possono risultare inefficaci in ragione delle condizioni economiche del contravventore.

C) SANZIONI CIVILI

• **Danni cagionati per effetto del trattamento – Art. 15**

Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto risarcimento del danno ai sensi dell'articolo 2050 del codice civile.