Fondazione Eni Enrico Mattei

NORME DI COMPORTAMENTO DEGLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI

RICHIAMI NORMATIVI

SOGGETTI RILEVANTI AI FINI DEL RISPETTO DELLA NORMATIVA PRIVACY

Titolare del trattamento	FEEM
Delegato dal Titolare	Direttore generale pro tempore
Responsabile interno del trattamento ai fini dell'esercizio dei diritti degli interessati	Direttore generale pro tempore
Struttura alla quale è demandato il compito di coordinamento e supervisione nell'ambito della normativa privacy	Servizi Generali
Struttura alla quale è demandato il compito di curare l'implementazione delle misure di sicurezza dal punto di vista informatico	Servizi ICT
Soggetti tenuti al rispetto della normativa privacy e del presente Regolamento	Tutti gli incaricati di FEEM, indipendentemente dal tipo di rapporto contrattuale, anche temporaneo, in essere.

NOTE
Nel testo il termine Fondazione può essere sostituito con azienda.

Ulteriori informazioni e documentazione consultabile
Per avere maggiori dettagli sulle misure di sicurezza in atto e sull'organizzazione di FEEM ai fini del rispetto della normativa può consultare il **Documento privacy**.

Può richiedere ulteriori informazioni rivolgendosi direttamente al Titolare.
Può consultare la normativa di riferimento sul sito:
www.garanteprivacy.it

FORMAZIONE DEGLI INCARICATI

Trattamento dei dati personali e vincoli al loro trattamento
(in corsivo si riportano per comodità stralci della normativa; il riferimento ufficiale per tali testi è il Dlgs 196/03 disponibile nella versione aggiornata sul sito www.garanteprivacy.it)

Dati e trattamenti
Il trattamento dei dati personali è regolamentato nella normativa italiana dal Dlgs 196/03, dai suoi allegati e da una serie di provvedimenti dell'autorità Garante.
La normativa definisce per trattamento:

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;

Una definizione estremamente ampia, che definisce trattamento anche la semplice "consultazione" di un dato personale.

Attualmente la normativa definisce come dato personale:

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;

limitando alle sole persone fisiche la tutela prevista dalla normativa nel suo complesso.
Gli altri soggetti, diversi dalle persone fisiche, sono comunque tutelate quando operano quali utenti o contraenti nell'ambito delle comunicazioni in formato elettronico (*).

Con qualunque informazione si intende ad esempio:
- il nome e cognome
- l'età
- il codice fiscale
- l'indirizzo

La definizione è comunque più ampia; non si intendono infatti informazioni esprimibili esclusivamente mediante una stringa di caratteri alfanumerici come quelli appena citati.

Un dato personale è rappresentato anche:
- dall'immagine
- dalla voce
- dalle caratteristiche biometriche di una persona.

Tali dati costituiscono dati personali se la persona a cui si riferiscono è *identificata o identificabile.*

Il concetto di "persona identificata" è semplice; un esempio classico di identificazione in modo diretto è l'abbinamento dell'indirizzo di casa al nome e cognome della persona al quale l'indirizzo si riferisce.
Il concetto di identificabile è meno immediato: se in una serie di questionari anonimi, relativi ad un gruppo di persone fisiche di cui tutti uomini ed una sola donna, uno di questi contenesse dati associabili unicamente ad un soggetto femminile, si avrebbe l'identificabilità dell'unico soggetto femminile del gruppo.
Il questionario relativo alla donna diventerebbe composto da dati personali, mentre quelli degli uomini continuerebbero a non esserlo.

La normativa individua, fra i dati personali, una serie di dati che richiedono una maggiore tutela, definiti dati sensibili, dati giudiziari, oltre a trattamenti che presentano rischi specifici.

DATI PERSONALI

- Dati personali comuni
- Dati personali sensibili
- Dati personali giudiziari
- Trattamento che presenta rischi specifici
- Dati identificativi

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;

Alcuni esempi di raccolte di informazioni che possono contenere dati sensibili sono:

- una busta paga (può contenere indicazioni circa periodi di malattia o l'adesione a sindacati)
- un estratto conto bancario (può contenere movimentazioni relative a spese mediche, elargizioni in favore di istituiti religiosi …)
- la dichiarazione dei redditi (può contenere indicazioni circa la destinazione dell'otto per mille…)

Da notare che nell'estratto conto bancario, a differenza di quanto comunemente si potrebbe credere, il dato potenzialmente sensibile non è l'importo, ma la descrizione del movimento.

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;

I dati giudiziari comprendono ad esempio :

- dati giudiziari penali di condanna definitivi
- dati giudiziari concernenti le pene accessorie

Art. 17. Trattamento che presenta rischi specifici
1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta 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, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.

2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare.

Ulteriore categorie di dati sono i cosiddetti dati identificativi:

c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;

(*) Restano comunque tutelate le persone fisiche che operano per conto di una persona giuridica, ente, associazione…

Le figure coinvolte

FIGURE COINVOLTE

Interessato

- Titolare
- Responsabile
- Incaricato
- Amministratore di sistema
- Custode delle password
- Custode degli archivi ad accesso controllato

I soggetti ai quali si riferiscono i dati sono definiti interessati.

i) "interessato", la persona fisica cui si riferiscono i dati personali:

Anche Lei, in quanto dipendente o collaboratore, è un interessato in quanto FEEM tratta i suoi dati personali per la gestione del rapporto di lavoro e per obblighi di legge.

Il trattamento dei dati personali può essere effettuato unicamente da un **incaricato** (Lei), previa formazione (questo documento ha questa specifica finalità) ed un incarico specifico (la lettera di incarico).

h) "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

La formazione all'incaricato deve essere pianificata **al momento dell'ingresso in servizio, in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali**.
Questo documento ha la duplice finalità di fornirle la formazione iniziale prevista dalla normativa e impartirle le opportune istruzioni per il corretto svolgimento della sua attività.
Nel caso di variazioni di mansioni o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento di dati personali, Lei riceverà una specifica formazione.

La formazione deve riguardare:

- i rischi che incombono sui dati
- le misure disponibili per prevenire eventi dannosi
- i profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività
- le responsabilità che ne derivano e le modalità per aggiornarsi sulle misure minime adottate dal titolare

L'incaricato nello svolgimento del suo compito risponde al **Responsabile** (se presente) ed al **Titolare**.

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;

Amministratore di sistema

il Provvedimento:
"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema 27 novembre 2008"

ha introdotto la figura dell'amministratore di sistema, intendendo con tale termine:
In assenza di definizioni normative e tecniche condivise, nell'ambito del provvedimento del Garante l'amministratore di sistema è assunto quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi SOFTWARE complessi quali i sistemi ERP (ENTERPRISE RESOURCE PLANNING) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.
Il Garante non ha inteso equiparare gli "operatori di sistema" di cui agli articoli del Codice penale relativi ai delitti informatici, con gli "amministratori di sistema": questi ultimi sono dei particolari operatori di sistema, dotati di specifici privilegi.
Anche il riferimento al d.P.R. 318/1999 nella premessa del provvedimento è puramente descrittivo poiché la figura definita in quell'atto normativo (ormai abrogato) è di minore portata rispetto a quella cui si fa riferimento nel provvedimento.
Non rientrano invece nella definizione quei soggetti che solo occasionalmente intervengono (p.es., per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi software*.*

Custode delle password
…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.

Custode degli archivi
…L'accesso agli archivi contenenti dati sensibili o giudiziari è ***controllato***

Gli adempimenti

ADEMPIMENTI

Dati comuni
- Informativa
- Consenso (salvo deroga)

Dati sensibili
- Autorizzazione generale
- Autorizzazione specifica
- Informativa
- Consenso

Trattamenti particolari
- Notifica

La legge impone al Titolare, prima di procedere al trattamento dei dati personali, di rilasciare una idonea **informativa** ed in alcuni casi di raccogliere il **consenso** dell'interessato.
Come sinteticamente riportato più avanti all'interno di questo documento, Lei potrà effettuare solo i trattamenti per i quali è stato autorizzato e se gli interessati ai quali si riferiscono i dati sono stati preventivamente informati e, dove richiesto, abbiano rilasciato il loro consenso.

Modelli di informative e formule per l'espressione del consenso sono stati predisposti dal Titolare; anche a Lei, in quanto interessato è stata consegnata apposita informativa.

Le informative sono diversificate in funzione principalmente della tipologia di interessato e delle finalità dei trattamenti.
Ulteriore distinzione riguarda il caso in cui i dati siano raccolti o meno presso l'interessato (non necessariamente questo implica la presenza di due diverse informative).

La richiesta del consenso non sempre è necessaria; in particolare il consenso dell'interessato non è richiesto quando il trattamento:

a) è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

b) 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;

c) 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;

d) riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

e) 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. Si applica la disposizione di cui all'articolo 82, comma 2;

f) con esclusione della diffusione, 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 un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

g) con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei princìpi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;

h) con esclusione della comunicazione all'esterno e della diffusione, è effettuato 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, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;

i) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati;

i-bis) riguarda dati contenuti nei curricula, nei casi di cui all'articolo 13, comma 5-bis;

i-ter)con esclusione della diffusione e fatto salvo quanto previsto dall'articolo 130 del presente codice, 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, come definite all'articolo 34, comma 1-ter, e purché queste finalità siano previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa di cui all'articolo 13.

Per il trattamento dei dati sensibili il consenso è di norma richiesto.
Fanno eccezione a questa regola i trattamenti di dati sensibili relativi ad esempio alla gestione dei rapporti di lavoro.

I dati sensibili possono inoltre essere trattati unicamente se il Titolare ha ricevuto una specifica **autorizzazione** dal Garante Privacy o se è stata rilasciata una **autorizzazione di carattere generale**.

In alcuni casi, previsti dalla norma (consultabile presso il Titolare o sul sito www.garanteprivacy.it), prima di procedere ad alcuni trattamenti il Titolare deve **notificare** la sua intenzione al Garante.

I rischi e le misure di sicurezza

La normativa attribuisce una particolare importanza alla **sicurezza** nella gestione dei trattamenti, motivo per cui in questo documento Le sono prescritte una serie di istruzioni su come Lei deve comportarsi.
Tali istruzioni, unitamente alle misure di sicurezza intraprese dal Titolare hanno la finalità di limitare:

- i rischi di distruzione o perdita, anche accidentale, dei dati stessi
- l' accesso non autorizzato
- il trattamento non consentito o non conforme alle finalità della raccolta.

Più dettagliatamente, il Garante Privacy ha individuato una serie di eventi che possono comportare rischi per i dati:

1) comportamenti degli operatori:
   - sottrazione di credenziali di autenticazione
   - carenza di consapevolezza, disattenzione o incuria
   - comportamenti sleali o fraudolenti
   - errore materiale
2) eventi relativi agli strumenti:
   - azione di virus informatici o di programmi suscettibili di recare danno
   - spamming o tecniche di sabotaggio
   - malfunzionamento, indisponibilità o degrado degli strumenti
   - accessi esterni non autorizzati
   - intercettazione di informazioni in rete
3) eventi relativi al contesto fisico-ambientale:
   - ingressi non autorizzati a locali/aree ad accesso ristretto
   - sottrazione di strumenti contenenti dati
   - eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria
   - guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)
   - errori umani nella gestione della sicurezza fisica

Relativamente a tali eventi il Titolare ha effettuato una dettagliata **analisi dei rischi**, in funzione delle misure di sicurezza in atto.
L'analisi dei rischi e le **misure di sicurezza** che il Titolare ha intrapreso sono descritte nel **Documento privacy**, che è consultabile previa richiesta al Titolare.

Le misure di sicurezza comprendono:

Per i trattamenti effettuati con strumenti elettronici

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- tenuta di un aggiornato documento programmatico sulla sicurezza;
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari

.

Sistema di autenticazione informatica

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

- *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

- *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 **[REGOLA ABROGATA]**

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 di cui al successivo punto 23;*
- *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 di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.*

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

- *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

- *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.* **[REGOLA ABROGATA]**

Per i trattamenti effettuati senza l'ausilio di strumenti elettronici

- 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.

- *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 è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.*

Le responsabilità
Tutti i soggetti che partecipano ai trattamenti di dati personali sono coinvolti nel corretto e lecito svolgimento degli stessi.

Lei, in qualità di incaricato, dovrà attenersi alle istruzioni ricevute dal Titolare e dal Responsabile (se nominato), sia direttamente, sia tramite queste **Norme di comportamento,** sia tramite quanto indicato nella sua **Lettera di incarico**.

In particolare dovrà adoperarsi affinché le misure di sicurezza in atto siano rispettate, segnalando ogni anomalia riscontrata al Responsabile (se nominato) o al Titolare.

Durante lo svolgimento della sua attività dovrà evitare che i dati personali oggetto di trattamento siano soggetti a:

- rischi di distruzione o perdita, anche accidentale, dei dati stessi
- accesso non autorizzato da parte di terzi
- trattamento non consentito o non conforme alle finalità della raccolta.

Potrà accedere ai soli dati relativi ai trattamenti per i quali è autorizzato mediante apposita lettera di incarico.
Al riguardo sarà autorizzato ad accedere ai soli documenti e file, strettamente necessari per lo svolgimento del suo incarico.

Relativamente alle misure di sicurezza si evidenzia che le stesse sono da adottare a cura del Titolare, del Responsabile (ove designato), e dell'**Incaricato**.

Le sanzioni

VIOLAZIONI AMMINISTRATIVE

Art. 161. Omessa o inidonea informativa all'interessato
Art. 162. Altre fattispecie
Art. 162-BIS. Sanzioni in materia di conservazione dei dati di traffico
Art. 163. Omessa o incompleta notificazione
Art. 164. Omessa informazione o esibizione al Garante
Art. 164-BIS. Casi di minore gravità e ipotesi aggravate (1)
Art. 165. Pubblicazione del provvedimento del Garante
Art. 166. Procedimento di applicazione

Capo I - Violazioni amministrative

Art. 161. Omessa o inidonea informativa all'interessato
1. La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da seimila euro a trentaseimila euro. (1)

(1) Comma così modificato dall'art. 44, comma 2, del decreto legge 30 dicembre 2008, n. 207 convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14.

Art. 162. Altre fattispecie
1. La cessione dei dati in violazione di quanto previsto dall'articolo 16, comma 1, lettera b), 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 diecimila euro a sessantamila euro. (1)

2. La violazione della disposizione di cui all'articolo 84, comma 1, è punita con la sanzione amministrativa del pagamento di una somma da mille euro a seimila euro. (2)

2-bis. In caso di trattamento di dati personali effettuato in violazione delle misure indicate nell'articolo 33 o delle disposizioni indicate nell'articolo 167 è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da diecimila euro a centoventimila euro. Nei casi di cui all'articolo 33 è escluso il pagamento in misura ridotta. (3)

2-ter. In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto 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 trentamila euro a centottantamila euro. (4)

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. (5)

(1) Comma così modificato dall'art. 44, comma, 3 lett. a), del decreto legge 30 dicembre 2008, n. 207 convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14.
(2) Comma così modificato dall'art. 44, comma 3, lett. b), del decreto legge 30 dicembre 2008, n. 207 convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14.
(3) Comma aggiunto dall'art. 44, comma 3, lett. c), del decreto legge 30 dicembre 2008, n. 207, convertito con modificazioni, dalla legge 27 febbraio 2009, n. 14, e poi così modificato dall'art. 20-bis, comma 1, lettera c), punto 1), del decreto legge 25 settembre 2009, n. 135, convertito, con modificazioni, dalla legge 20 novembre 2009, n. 166.
(4) Comma aggiunto dall'art. 44, comma 3, lett. c), del decreto legge 30 dicembre 2008, n. 207, convertito con modificazioni, dalla legge 27 febbraio 2009, n. 14.
(5) Comma aggiunto dall'art. 20 bis, comma 1, lett. c), punto 2), del decreto legge 25 settembre 2009, n. 135, convertito, con modificazioni, dalla legge 20 novembre 2009, n. 166.

Art. 162-bis. Sanzioni in materia di conservazione dei dati di traffico (1)
1. Salvo che il fatto costituisca reato e salvo quanto previsto dall'articolo 5, comma 2, del decreto legislativo di recepimento della direttiva 2006/24/Ce del Parlamento europeo e del Consiglio del 15 marzo 2006, nel caso di violazione delle disposizioni di cui all'art. 132, commi 1 e 1-bis, si applica la sanzione amministrativa pecuniaria da 10.000 euro a 50.000 euro. (2)

(1) Articolo aggiunto dall'art. 5, comma 1, del decreto legislativo 30 maggio 2008, n. 109, di attuazione della direttiva 2006/24/Ce riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/Ce.
Per completezza, si riporta il comma 2 del predetto articolo 5, richiamato dall'articolo 162-bis del Codice:

"2. Salvo che il fatto costituisca reato, l'omessa o l'incompleta conservazione dei dati ai sensi dell'articolo 132, commi 1 e 1-bis, del Codice, è punita con la sanzione amministrativa pecuniaria da euro 10.000 ad euro 50.000 che può essere aumentata fino al triplo in ragione delle condizioni economiche dei responsabili della violazione. Nel caso di assegnazione di indirizzo IP che non consente l'identificazione univoca dell'utente o abbonato si applica la sanzione amministrativa pecuniaria da 5.000 euro a 50.000 euro, che può essere aumentata fino al triplo in ragione delle condizioni economiche dei responsabili della violazione. Le violazioni sono contestate e le sanzioni sono applicate dal Ministero dello sviluppo economico.".

(2) Comma così modificato dall'art. 44, comma 4, del decreto legge 30 dicembre 2008, n. 207 convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14.

Art. 162-ter. Sanzioni nei confronti di fornitori di servizi di comunicazione elettronica accessibili al pubblico (1)
1. La violazione delle disposizioni di cui all'articolo 32-bis, comma 1, è punita con la sanzione amministrativa del pagamento di una somma da venticinquemila euro a centocinquantamila euro.

2. La violazione delle disposizioni di cui all'articolo 32-bis, comma 2, è punita con la sanzione amministrativa del pagamento di una somma da centocinquanta euro a mille euro per ciascun contraente o altra persona nei cui confronti venga omessa o ritardata la comunicazione di cui al medesimo articolo 32-bis, comma 2. Non si applica l'articolo 8 della legge 24 novembre 1981, n. 689.

3. La sanzione amministrativa di cui al comma 2 non può essere applicata in misura superiore al 5 per cento del volume d'affari realizzato dal fornitore di servizi di comunicazione

elettronica accessibili al pubblico nell'ultimo esercizio chiuso anteriormente alla notificazione della contestazione della violazione amministrativa, fermo restando quanto previsto dall'articolo 164-bis, comma 4.

4. La violazione delle disposizioni di cui all'articolo 32-bis, comma 7, è punita con la sanzione amministrativa del pagamento di una somma da ventimila euro a centoventimila euro.

5. Le medesime sanzioni di cui al presente articolo si applicano nei confronti dei soggetti a cui il fornitore di servizi di comunicazione elettronica accessibili al pubblico abbia affidato l'erogazione dei predetti servizi, qualora tali soggetti non abbiano comunicato senza indebito ritardo, al fornitore, ai sensi dell'articolo 32-bis, comma 8, le informazioni necessarie ai fini degli adempimenti di cui all'articolo 32-bis.

(1) Articolo inserito dall'art. 1, comma 9, del decreto legislativo 28 maggio 2012, n. 69.

Art. 163. Omessa o incompleta notificazione
1. Chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione ai sensi degli articoli 37 e 38, ovvero indica in essa notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma da ventimila euro a centoventimila euro. (1)

(1) Comma così modificato dall'art. 44, comma 5, del decreto legge 30 dicembre 2008, n. 207 convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14.

Art. 164. Omessa informazione o esibizione al Garante
1. Chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi degli articoli 150, comma 2, e 157 è punito con la sanzione amministrativa del pagamento di una somma da diecimila euro a sessantamila euro. (1)

(1) Comma così modificato dall'art. 44, comma 6, del decreto legge 30 dicembre 2008, n. 207 convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14.

Art. 164-bis. Casi di minore gravità e ipotesi aggravate (1)

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)

2. In caso di più violazioni di un'unica o di più disposizioni di cui al presente Capo, 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 cinquantamila euro a trecentomila 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 presente Capo sono applicati in misura pari al doppio.

4. Le sanzioni di cui al presente Capo possono essere aumentate fino al quadruplo quando possono risultare inefficaci in ragione delle condizioni economiche del contravventore.

(1) Articolo inserito dall'art. 44, comma 7, del decreto legge 30 dicembre 2008, n. 207 convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14.
(2) Comma così modificato dall'art. 1, comma 10, del decreto legislativo 28 maggio 2012, n. 69.

Art. 165. Pubblicazione del provvedimento del Garante
1. Nei casi di cui agli articoli del presente Capo può essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica. La pubblicazione ha luogo a cura e spese del contravventore. (1)

(1) Comma così modificato dall'art. 44, comma 8, del decreto legge 30 dicembre 2008, n. 207 convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14.

Art. 166. Procedimento di applicazione
1. L'organo competente a ricevere il rapporto e ad irrogare le sanzioni di cui al presente capo e all'articolo 179, comma 3, è il Garante. Si osservano, in quanto applicabili, le disposizioni della legge 24 novembre 1981, n. 689, e successive modificazioni. I proventi, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all'articolo 156, comma 10, e sono utilizzati unicamente per l'esercizio dei compiti di cui agli articoli 154, comma 1, lettera h), e 158.

ILLECITI PENALI

Capo II - Illeciti penali

Art. 167. Trattamento illecito di dati
1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

Art. 168. Falsità nelle dichiarazioni e notificazioni al Garante
1. Chiunque, nelle comunicazioni di cui all'articolo 32-bis, commi 1 e 8, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

(1) Comma così modificato dall'art. 1, comma 11, del decreto legislativo 28 maggio 2012, n. 69.

Art. 169. Misure di sicurezza
1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni. (1)

2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, 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. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili. (2)

(1) Comma così modificato dall'art. 44, comma 9, lett. a), del decreto legge 30 dicembre 2008, n. 207 convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14.
(2) Comma così modificato dall'art. 44, comma 9, lett. b), del decreto legge 30 dicembre 2008, n. 207 convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14.

Art. 170. Inosservanza di provvedimenti del Garante
1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la reclusione da tre mesi a due anni.

Art. 171. Altre fattispecie
1. La violazione delle disposizioni di cui agli articoli 113, comma 1, e 114 è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300.

Art. 172. Pene accessorie
1. La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza.

GESTIONE DEI DIRITTI DELL'INTERESSATO
Lei deve dare pronta soddisfazione alle richieste che i soggetti interessati possono rivolgerLe, conformemente a quanto prescritto dall'articolo 7 Dlgs 196/2003 (Diritto di accesso ai dati personali ed altri diritti), segnalando tali richieste al Titolare.

Titolo II DIRITTI DELL'INTERESSATO

Art. 7. Diritto di accesso ai dati personali ed altri diritti
1. L'interessato ha diritto 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.

2. L'interessato ha diritto di ottenere l'indicazione:

a) dell'origine dei dati personali;

b) delle finalità e modalità del trattamento;

c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;

e) 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 designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:

a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

b) 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;

c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Art. 8. Esercizio dei diritti
1. I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al titolare o

al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo.

2. I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati:

a) in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni, in materia di riciclaggio;

b) in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive;

c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;

d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;

e) ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;

f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397;

g) per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;

h) ai sensi dell'articolo 53, fermo restando quanto previsto dalla legge 1 aprile 1981, n. 121.

3. Il Garante, anche su segnalazione dell'interessato, nei casi di cui al comma 2, lettere a), b), d), e) ed f) provvede nei modi di cui agli articoli 157, 158 e 159 e, nei casi di cui alle lettere c), g) ed h) del medesimo comma, provvede nei modi di cui all'articolo 160.

4. L'esercizio dei diritti di cui all'articolo 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

Art. 9. Modalità di esercizio

1. La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti

di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.

2. Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.

3. I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

4. L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. (1)

5. La richiesta di cui all'articolo 7, commi 1 e 2, è formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.

Art. 10. Riscontro all'interessato

1. Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:

a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;

b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

2. I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.

3. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'articolo 84, comma 1.

4. Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.

5. Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

6. La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.

7. Quando, a seguito della richiesta di cui all'articolo 7, commi 1 e 2, lettere a), b) e c) non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.

8. Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.

9. Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque non oltre quindici giorni da tale riscontro.

DEFINZIONI

Art. 4. Definizioni *

1. Ai fini del presente codice si intende per:

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; (1)

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: (2)

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.

2. Ai fini del presente codice si intende, inoltre, per:

a) "comunicazione elettronica", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un contraente o utente ricevente, identificato o identificabile;

b) "chiamata", la connessione istituita da un servizio di comunicazione elettronica accessibile al pubblico che consente la comunicazione bidirezionale; (3)

c) "reti di comunicazione elettronica", i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato; (4)

d) "rete pubblica di comunicazioni", una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di reti; (5)

e) "servizio di comunicazione elettronica", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

*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; **

g) "utente", qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

h) "dati relativi al traffico", qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

i) "dati relativi all'ubicazione", ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico; (6)

l) "servizio a valore aggiunto", il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

m) "posta elettronica", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

3. Ai fini del presente codice si intende, altresì, per:

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;

g-bis) "violazione di dati personali": violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico. (7)

4. Ai fini del presente codice si intende per:

a) "scopi storici", le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;

b) "scopi statistici", le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;

c) "scopi scientifici", le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.