Prot. n. (APC/08/1772)

IL DIRETTORE DELL'AGENZIA REGIONALE DI PROTEZIONE CIVILE

Visto il D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", di seguito denominato Codice;

Vista la deliberazione di Giunta regionale n. 960 del 27/06/2005 "Direttiva in materia di trattamento di dati personali con particolare riferimento alla ripartizione di competenze tra soggetti che effettuano il trattamento - modifica ed integrazione delle deliberazioni di Giunta regionale n. 447/2003 e n.1878/2004"; tale direttiva è stata riproposta nell'appendice 5 dell'Allegato A alla deliberazione della Giunta regionale n. 450 del 03/04/2007;

Visto il Regolamento di organizzazione e contabilità dell'Agenzia regionale di protezione civile, approvato con deliberazione della Giunta regionale n. 1769 del 11/12/2006 ed in particolare gli artt. 14 "Servizi informatici"e 15 "Trattamento dei dati personali" di seguito riportati:

- Art. 14

comma 1: Le funzioni ed i compiti dell'Agenzia sono svolte, di norma, con il supporto di sistemi informatici;i collaboratori dell'Agenzia, sia tecnici che amministrativi, sono collegati mediante rete telematica e hanno accesso alle informazioni, applicazioni e servizi di loro competenza.

comma 2: Per lo sviluppo e la gestione dei servizi informatici e telematici l'Agenzia si raccorda operativamente con le strutture regionali competenti e può avvalersi anche di risorse esterne.

comma 3: L'Agenzia provvede alla realizzazione ed all'implementazione del sistema informativo integrato di protezione civile orientato al supporto alle decisioni, assicurandone le migliori sinergie con i sistemi in uso alla Regione e alle altre strutture operative del sistema regionale di protezione civile.

- Art. 15

comma 1: Ai sensi della direttiva emanata in materia di trattamento di dati personali dalla Giunta regionale l'Agenzia è ente autonomo titolare del trattamento, avuto riguardo agli ambiti operativi di propria competenza previsti dalla legge istitutiva; l'Agenzia provvede al trattamento dei dati personali nel rispetto del Decreto Legislativo 30 giugno 2003, n. 196.

comma 2: In caso di utilizzo di sistemi informativi della Regione, l'Agenzia si conforma alle disposizioni da questa impartita;

Evidenziato che nella Regione Emilia-Romagna, avuto riguardo alle strutture organizzative della Giunta, sono stati adottati le "Linee guida della Giunta della Regione Emilia-Romagna in materia di protezione di dati personali" approvate con deliberazione di Giunta n. 1264/2005 e i Disciplinari tecnici in materia di protezione dei dati personali, approvati con le seguenti determinazioni del Direttore Generale all'Organizzazione, Personale, Sistemi informativi e Telematica:

- n. 2649/2007 "Disciplinare tecnico relativo al controllo agli accessi ai locali della Giunta della Regione Emilia-Romagna", che ha modificato alcune prescrizioni del precedente Disciplinare adottato con DD n. 1031/2006;

- n. 2650/2007 "Disciplinare tecnico per l'esercizio del diritto di accesso dell'interessato ai propri dati personali nella Giunta della Regione Emilia-Romagna" che ha confermato il precedente Disciplinare adottato con DD n. 1044/2006;

- n. 2651/2007 "Disciplinare tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta della Regione Emilia-Romagna", che ha confermato il precedente Disciplinare adottato con DD n. 1033/2006;

- n. 2653/2007 "Disciplinare tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta della Regione Emilia-Romagna" che ha apportato revisioni di mera forma al precedente Disciplinare adottato con DD n. 1035/2006;

- n. 604/2007 “Disciplinare tecnico in materia di videosorveglianza nella Giunta della Regione Emilia-Romagna”;

- n. 283/2008 “Disciplinare tecnico su modalità e procedure per verifiche di sicurezza su sistemi informativi, per controlli sull’utilizzo dei beni messi a disposizione dall’ente per attività lavorativa con riferimento alle strumentazioni informatiche e telefoniche ed esemplificazioni di comportamenti per il corretto utilizzo dei beni, da applicare nella Giunta e Assemblea legislativa RER”;

Dato atto che con proprie precedenti determinazioni n. 3689/2007 “Individuazione degli ambiti di attività dell’Agenzia regionale di protezione civile in cui si effettua il trattamento dei dati personali e dei relativi incaricati” e n. 4019/2007 “Approvazione del Documento programmatico sulla sicurezza dell’Agenzia regionale di protezione civile” si è disposto un rinvio ai principi di cui alle Linee Guida e alle regole previste nei Disciplinari tecnici sopra richiamati, nelle more dell’adozione di apposite politiche di sicurezza dell’Agenzia regionale di protezione civile;

Considerato tuttavia che la configurazione dei rapporti sia sul piano logistico che amministrativo tra l’Agenzia e la Regione Emilia-Romagna (ad es.: espletamento delle attività amministrative dell’Agenzia nei locali della Regione, impiego di strumentazioni informatiche regionali, appartenenza dei collaboratori al ruolo organico della Giunta regionale) suggerisce, anche per esigenze di semplificazione, di procedere al recepimento dei provvedimenti regionali sopra richiamati;

Considerato, altresì, che con nota prot. PG/08/73346 del 17/03/2007 del Direttore Generale Centrale “Organizzazione, Personale, Sistemi Informativi e Telematica” è stato espressamente richiesto all’Agenzia regionale di procedere al recepimento delle policy adottate dalla Giunta regionale sopra richiamate;

Ritenuto pertanto di recepire con atto formale i principi di cui alle Linee Guida e i Disciplinari tecnici sopra richiamati, con gli adattamenti al contesto organizzativo e

funzionale dell’Agenzia regionale, esplicitati negli indirizzi applicativi riportati nell’Allegato A al presente atto;

Richiamate:

- la L.R. 26 novembre 2001, n. 43, "Testo unico in materia di organizzazione e di rapporti di lavoro nella Regione Emilia-Romagna";

- la deliberazione della Giunta regionale n. 450 del 3 aprile 2007 “Adempimenti conseguenti alle delibere 1057/2006 e 1663/2006. Modifiche agli indirizzi approvati con delibera 447/2003 e successive modifiche”;

- la deliberazione della Giunta regionale n. 1499 del 19 settembre 2005 "Preliminari disposizioni procedimentali e di organizzazione per l'attivazione dell'Agenzia regionale di protezione civile ai sensi dell'art. 1, comma 6, e art. 20 e seguenti, L.R. 7 febbraio 2005, n. 1", con la quale lo scrivente è stato nominato Direttore dell'Agenzia regionale di protezione civile;

- la deliberazione della Giunta regionale n. 1769 del 11 dicembre 2006 “Agenzia regionale di protezione civile: modifica della propria deliberazione n. 1499/2005 e approvazione del relativo regolamento di organizzazione e contabilità;

Attestata la regolarità amministrativa del presente atto ai sensi della deliberazione della Giunta regionale n. 450/2007.;

D E T E R M I N A

per le ragioni espresse nella parte narrativa e che qui si intendono integralmente richiamate

1. di recepire i principi di cui alle Linee Guida approvate con deliberazione della Giunta regionale n. 1264/2005 e i Disciplinari tecnici approvati con le determinazioni del Direttore Generale all'Organizzazione, Personale, Sistemi informativi e Telematica nn. 2649/2007, 2650/2007,

2651/2007, 2653/2007, 604/2007 e 283/2008 con gli adattamenti al contesto organizzativo e funzionale dell’Agenzia regionale di protezione civile, esplicitati negli indirizzi applicativi riportati nell’Allegato A al presente atto;

2. di portare a conoscenza dei collaboratori dell’Agenzia regionale di protezione civile il presente atto e il relativo Allegato A, acquisendo da ciascuno di essi dichiarazione per presa visione, tramite firma in un apposito elenco.

IL DIRETTORE

(Ing. Demetrio Egidi)

ALLEGATO A

INDIRIZZI APPLICATIVI IN MATERIA DI TRATTAMENTO DI DATI PERSONALI NELL'AGENZIA REGIONALE DI PROTEZIONE CIVILE

Premessa

Con i presenti indirizzi applicativi ci si prefigge l'obiettivo di procedere ad una ricognizione del quadro normativo di riferimento in materia di trattamento di dati personali e contemporaneamente di portare a conoscenza dei collaboratori dell'Agenzia regionale le regole di comportamento da osservare al fine di assicurare la protezione dei dati personali trattati nell'ambito dell'attività lavorativa.

I presenti indirizzi sono articolati nelle seguenti sezioni:

Sezione A: sono illustrati gli atti amministrativi adottati dalla Regione;

Sezione B: sono illustrate sia la portata applicativa nell'ambito dell'Agenzia degli atti adottati dalla Regione sia le misure definite per lo specifico contesto organizzativo e funzionale dell'Agenzia.;

Sezione C: sono riportate le disposizioni più rilevanti dei Disciplinari tecnici adottati dalla Regione nelle seguenti materie: controllo degli accessi ai locali; sicurezza delle applicazioni informatiche; utilizzo dei sistemi informativi; diritto di accesso dell'interessato ai propri dati personali; videosorveglianza, verifiche di sicurezza e controlli sull'utilizzo delle strumentazioni informatiche e telefoniche.

Tutti i collaboratori sono tenuti ad attenersi a quanto esplicitato nei presenti indirizzi applicativi.

SEZIONE A

ATTI REGOLAMENTARI E AMMINISTRATIVI ADOTTATI DALLA REGIONE EMILIA-ROMAGNA

La Regione Emilia-Romagna con deliberazione di Giunta n. 960 del 27 giugno 2005 ha adottato una direttiva in materia di trattamento di dati personali con la quale si è individuato un criterio di delimitazione del confine di titolarità della Regione medesima.
La direttiva prevede che il criterio di delimitazione è dato dallo stesso Decreto Legislativo n. 196/2003 "Codice in materia di protezione dei dati personali" di seguito denominato Codice, che specifica che titolare è il soggetto cui spettano le decisioni in ordine alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Altro criterio sussidiario per verificare la titolarità o meno in capo alla Regione Emilia-Romagna dei trattamenti di dati personali effettuati da altri soggetti collegati a vario titolo alla Regione stessa è quello dato dall'attribuzione a tali soggetti, nelle relative leggi istitutive, della qualità di ente della Regione. In base a tale criterio sono quindi da considerarsi, secondo la direttiva, quali autonomi titolari del trattamento di dati personali, effettuati nell'ambito delle rispettive competenze, anche le Agenzie regionali dotate di particolari forme di autonomia (contabile, organizzativa o tecnico-operativa, amministrativa, etc**),** tra le quali l'Agenzia regionale di protezione civile.

La Regione Emilia-Romagna ha individuato con riferimento alla tecnostruttura nel suo complesso, due titolari autonomi del trattamento: Giunta regionale e relative strutture organizzative; Assemblea legislativa e relative strutture organizzative.

La citata direttiva approvata con DGR n. 960/2005, riprodotta integralmente nell'appendice n. 5 di cui alla DGR n. 450/2007, individua le competenze della Giunta regionale, quale titolare autonomo del trattamento dei dati personali, designa i soggetti responsabili del trattamento e definisce i criteri generali da rispettare nell'individuazione dei soggetti incaricati a compiere le operazioni di trattamento.

Tale direttiva, pur applicandosi alle strutture organizzative della Giunta regionale (Direzioni Generali e Servizi ad esse facenti capo, nonché Agenzie regionali non dotate delle forme di autonomia di cui sopra), costituisce per l'Agenzia regionale di protezione civile un utile quadro di riferimento.

In base alla suddetta direttiva la Giunta regionale, quale titolare del trattamento provvede:

a) all'individuazione, con apposito atto di proposta di regolamento all'Assemblea legislativa della Regione, dei tipi di dati e di operazioni di trattamento relativi a dati sensibili e o giudiziari. **La Regione ha adottato il Regolamento n. 3 del 24 aprile 2006, pubblicato sul BURE-R n. 57 del 24 aprile 2006;**

b) all'adozione, con proprio atto, di linee guida in materia di protezione dei dati personali, al fine di dettare i principi cui devono attenersi, nello svolgimento della

propria attività, coloro che trattano dati personali nell'ambito della Giunta regionale, siano essi responsabili o incaricati del trattamento. **Le linee guida, composte di 16 articoli, sono state adottate con DGR n. 1264/2005;**

c) all'adozione con proprio atto, aggiornandolo periodicamente, del Documento Programmatico sulla la sicurezza (DPS), previsto dall'art. 34, lett. g) del Codice; **il DPS è stato approvato con DGR n. 430/2006 ed aggiornato con DGR n. 378/2007;**

d) alla designazione del Responsabile della sicurezza, con il compito, tra gli altri, di curare la redazione e l'aggiornamento del DPS per gli ambiti di trattamento delle strutture della Giunta; curare la redazione e il relativo aggiornamento del Disciplinare tecnico trasversale in materia di sicurezza delle applicazioni informatiche e del Disciplinare tecnico trasversale per utenti sull'utilizzo dei sistemi informativi nella Giunta regionale;

e) alla designazione del Coordinatore del diritto di accesso dell'interessato ai propri dati personali, con il compito, tra gli altri, di curare la redazione e l'aggiornamento del Disciplinare tecnico trasversale per l'esercizio del diritto di accesso dell'interessato ai propri dati personali e di proporre l'adozione delle opportune misure per agevolare l'accesso ai dati personali da parte dell'interessato. Si evidenzia, infatti, che il Codice, agli artt. 7 e ss.. attribuisce agli interessati il potere di esercitare, sui propri dati personali, un diritto di accesso, relativo sia alla conoscenza dei dati stessi che a determinati interventi (ad es. di integrazione, rettifica, cancellazione di dati personali);

f) alla designazione dei Responsabili del trattamento dei dati personali. Nella Giunta sono stati individuati quali Responsabili del trattamento dei dati personali, ciascuno per il proprio ambito di competenza: il Capo di Gabinetto, i Direttori generali e i Direttori delle Agenzie sfornite delle forme di autonomia di cui si è detto in precedenza. Con tale designazione sono stati specificati anche i compiti in capo ai Responsabili del trattamento.

Taluni dei compiti dei Responsabili del trattamento sono delegabili ai Responsabili di Servizio e ai Dirigenti professional. Tuttavia soltanto il soggetto delegante è responsabile del trattamento secondo quanto stabilito dall'art. 29 del Codice.

La direttiva in parola, inoltre, ha attribuito al Direttore generale "Organizzazione, personale, sistemi informativi e telematica" il compito di adottare disciplinari tecnici trasversali.

Ad oggi sono stati adottati i seguenti disciplinari tecnici con le seguenti determinazioni del Direttore sopra indicato:

- n. 2649/2007 "Disciplinare tecnico relativo al controllo agli accessi ai locali della Giunta della Regione Emilia-Romagna", che ha modificato alcune prescrizioni del precedente Disciplinare adottato con DD n. 1031/2006;

- n. 2650/2007 "Disciplinare tecnico per l'esercizio del diritto di accesso dell'interessato ai propri dati personali nella Giunta della Regione Emilia-Romagna" che ha confermato il precedente Disciplinare adottato con DD n. 1044/2006;

- n. 2651/2007 "Disciplinare tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta della Regione Emilia-Romagna", che ha confermato il precedente Disciplinare adottato con DD n. 1033/2006;

- n. 2653/2007 "Disciplinare tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta della Regione Emilia-Romagna" che ha apportato revisioni di mera forma al precedente Disciplinare adottato con DD n. 1035/2006;

- n. 604/2007 "Disciplinare tecnico in materia di videosorveglianza nella Giunta della Regione Emilia-Romagna";

- n. 283/2008 "Disciplinare tecnico su modalità e procedure per verifiche di sicurezza su sistemi informativi, per controlli sull'utilizzo dei beni messi a disposizione dall'ente per attività lavorativa con riferimento alle strumentazioni informatiche e telefoniche ed esemplificazioni di comportamenti per il corretto utilizzo dei beni, da applicare nella Giunta ed Assemblea legislativa".

SEZIONE B

PORTATA APPLICATIVA DEGLI ATTI REGOLAMENTARI E AMMINISTRATIVI REGIONALI NELL'AMBITO DELL'AGENZIA REGIONALE DI PROTEZIONE CIVILE. MISURE SPECIFICHE PER IL CONTESTO ORGANIZZATIVO E FUNZIONALE DELL'AGENZIA.

B.1) Linee guida regionali in materia di protezione dei dati personali

Ai principi recati dalle Linee guida approvate con DGR n. 1264/2005 devono attenersi anche i collaboratori dell'Agenzia regionale. In proposito si segnala che ai sensi dell'articolo 15 delle suddette Linee guida è stato istituito il "Registro informatico dei trattamenti dei dati personali" al fine di censire i trattamenti effettuati nelle strutture della Giunta e le relative banche dati. Anche i trattamenti effettuati dal Servizio Protezione Civile, prima della sua trasformazione, a decorrere dal mese di gennaio 2007, in Agenzia regionale sono stati censiti nell'ambito di tale Registro. L'Agenzia regionale non è obbligata a dotarsi di un registro informatico; tuttavia si valuterà l'opportunità di predisporre uno strumento equipollente al fine di censire, organizzare ed aggiornare in un archivio dedicato le schede relative a ciascun ambito di attività in cui si effettua il trattamento dei dati personali.

B.2) Regolamento regionale per il trattamento di dati sensibili e giudiziari

Il Regolamento regionale n. 3 del 24 aprile 2006, pubblicato sul BURE-R n. 57 del 24 aprile 2006, recante "*Regolamento per il trattamento dei dati sensibili e giudiziari di titolarità della Giunta regionale e delle Agenzie, Istituti ed Enti che fanno riferimento all'Amministrazione regionale*" costituisce norma di copertura per i trattamenti di dati sensibili e/o giudiziari effettuati anche dalle Agenzie regionali, tra cui l'Agenzia regionale di protezione civile. Il Regolamento sarà oggetto di aggiornamento periodico. Pertanto, ove l'Agenzia regionale dovesse in futuro, in relazione alle proprie competenze istituzionali, revisionare o individuare ulteriori ambiti di attività in cui si renderà necessario trattare dati sensibili e/o giudiziari, ne dovrà dare comunicazione alla struttura organizzativa della Giunta competente in materia.

B.3) Regolamento regionale per le operazioni di comunicazione e diffusione dei dati personali diversi da quelli sensibili e giudiziari

Il Regolamento regionale n. 2 del 31 ottobre 2007, pubblicato sul BURE-R n. 159 del 31 ottobre 2007, recante "*Regolamento per le operazioni di comunicazione e diffusione di dati personali diversi da quelli sensibili e giudiziari di titolarità della Giunta regionale e dell'Agrea, dell'Agenzia regionale di protezione civile, dell'Agenzia regionale Intercent-ER e dell'IBACN*" costituisce norma di copertura per le operazioni (comunicazione e diffusione) di cui all'art. 19 del Codice effettuate anche dall'Agenzia regionale di protezione civile.

B.4) Documento programmatico sulla sicurezza (DPS)

L'Agenzia regionale, quale titolare autonomo del trattamento, è tenuta ai sensi del Codice ad adottare ed aggiornare il Documento programmatico sulla sicurezza (DPS) relativo ai propri ambiti di attività in cui si effettua il trattamento dei dati personali. Al riguardo si

evidenzia che secondo il Codice il DPS è obbligatorio solo nel caso di trattamento – con strumenti informatici – di dati sensibili o giudiziari, tuttavia lo stesso è certamente utile in ogni caso, attesa la possibilità di riportare in un unico documento tutti i dati relativi alla riservatezza. Il primo DPS dell'Agenzia regionale è stato adottato con determinazione del Direttore n. 4019 del 30 marzo 2007, come comunicato a tutti i collaboratori con e-mail del 13 aprile 2007. Il DPS contiene informazioni sugli eventi potenzialmente dannosi per la sicurezza dei dati, le possibili conseguenze e la gravità stimata in relazione al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati e riguarda sia i dati sensibili e giudiziari sia i dati diversi da questi.

B.5) Titolare e Responsabile del trattamento

Nell'ambito dell'Agenzia regionale, considerate le sue dimensioni organizzative, si è ritenuto di non procedere alla designazione di un Responsabile del trattamento, né di un Responsabile della sicurezza o di un Coordinatore del diritto di accesso dell'interessato ai propri dati personali, diversamente da quanto stabilito all'interno di una struttura ben più complessa ed articolata quale quella della Giunta regionale, considerato peraltro che secondo il Codice la designazione di tali figure non è obbligatoria.

Gli obblighi, pertanto, previsti dal Codice in capo al Titolare o, ove designato, al Responsabile del trattamento, volti a garantire la protezione dei dati personali e il diritto di accesso dell'interessato ai propri dati personali si intendono, per quanto riguarda l'Agenzia regionale, in capo al Direttore, quale Legale rappresentante dell'Agenzia medesima.

B.6) Compiti del Direttore dell'Agenzia regionale quale Titolare del trattamento

In particolare competono al Direttore, in linea con quanto la citata direttiva regionale, approvata con D.G.R. n. 960/2005 e riprodotta nell'appendice 5 della D.G.R. n. 450/2007, ha previsto per i Direttori generali della Giunta regionale, i seguenti compiti:

a) verificare la legittimità dei trattamenti di dati personali effettuati dall'Agenzia regionale, con particolare riguardo al principio di necessità di cui all'art. 3 del Codice, sia relativamente ai trattamenti già in essere che ai nuovi trattamenti;
b) disporre, in conseguenza alla verifica di cui alla lettera a), le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
c) vigilare, anche tramite verifiche periodiche, sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, e sul rispetto delle proprie istruzioni;
d) aggiornare periodicamente l'elenco dei trattamenti di dati personali effettuati dall'Agenzia regionale, anche al fine di garantire un tempestivo aggiornamento del Documento Programmatico per la Sicurezza;
e) aggiornare periodicamente, in particolare, l'elenco dei trattamenti di dati sensibili e/o giudiziari, anche al fine di aggiornare il relativo regolamento regionale;
f) predisporre l'informativa di cui all'art. 13 del Codice (al riguardo si veda il punto B8 dei presenti indirizzi applicativi) e verificare che siano adottate le modalità operative necessarie perché l'informativa sia effettivamente portata a conoscenza degli interessati;

g) sottoscrivere il consenso richiesto da soggetti privati che trattano i dati dell'Agenzia regionale, qualora il consenso non sia escluso sulla base di quanto previsto all'art. 24 del Codice;
h) individuare gli incaricati del trattamento dei dati personali e fornire agli stessi istruzioni per il corretto trattamento dei dati stessi, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione viene effettuata prendendo a riferimento l'intera tecnostruttura dell'Agenzia regionale e indicando nominativamente le persone fisiche incaricate e i trattamenti che le stesse sono autorizzate ad effettuare; le istruzioni contengono l'espresso richiamo alle linee guida regionali per la protezione dei dati personali approvate con la citata DGR n. 1264/2005, ai Disciplinari tecnici citati nella precedente sezione A e ai presenti indirizzi applicativi;
i) predisporre ogni adempimento organizzativo necessario per garantire agli interessati il diritto di accesso ai propri dati personali e provvedere, tramite gli incaricati, a dare riscontro alle istanze degli interessati ai sensi dell'art. 7 del Codice (al riguardo si veda la Sezione C.4 dei presenti indirizzi applicativi);
j) disporre l'adozione dei provvedimenti imposti dal Garante quale misura conseguente all'accoglimento delle richieste degli interessati;
k) predisporre la documentazione e gli atti necessari per il Garante nei casi e nei modi previsti dal Codice;
l) assicurare che vengano fornite istruzioni al soggetto competente, affinché nei contratti con soggetti esterni che comportano l'adozione di misure minime di sicurezza, sia prevista l'attestazione di conformità dell'intervento ai sensi della misura 25 dell'allegato B del Codice, e che tale attestazione sia trasmessa all'Agenzia regionale.

B.7) Incaricati del trattamento

Il Titolare o il Responsabile del trattamento, secondo quanto previsto dall'art. 30 del Codice, devono designare, quali incaricati del trattamento dei dati personali, le persone fisiche che, operando sotto la loro diretta autorità, effettuano le operazioni del trattamento.

Devono, pertanto, essere designati quali incaricati, qualora effettuino operazioni di trattamento, non soltanto i dipendenti a tempo indeterminato o determinato, ma anche le altre persone fisiche che, ad altro titolo, operano sotto la diretta autorità del Titolare o del Responsabile del trattamento, quali ad esempio, i lavoratori con contratto di somministrazione di lavoro a tempo determinato (lavoratori cd. interinali) e, di norma, i collaboratori coordinati e continuativi o a progetto. In quest'ultimo caso la designazione deve essere contenuta anche nel contratto individuale.

Gli ambiti di attività dell'Agenzia regionale in cui si effettua il trattamento dei dati personali e i collaboratori della stessa incaricati del trattamento, sono stati individuati con determinazione del Direttore n. 3689 del 26 marzo 2007. L'elenco degli ambiti di attività e degli incaricati viene aggiornato almeno annualmente e ciascun collaboratore è autorizzato a trattare i dati personali limitatamente agli ambiti per cui è stato incaricato.

B.8) Informativa agli interessati ai sensi dell'art. 13 del Codice. Modello standard di informativa utilizzabile all'interno dell'Agenzia regionale

Il trattamento dei dati personali da parte dell'Agenzia regionale comporta l'obbligo di fornire l'informativa all'interessato ai sensi dell'art. 13 del Codice**.** Nell'**Allegato 1** ai presenti indirizzi applicativi è riportato il modello standard di informativa utilizzabile dalle strutture dell'Agenzia regionale e da completare a cura delle strutture medesime (Servizi, Unità Funzionale e relativi settori interni) per gli specifici ambiti di rispettiva competenza.

B.9) Responsabili del trattamento esterni all'Agenzia regionale

In linea con quanto previsto dalla direttiva regionale più volte richiamata, si ritiene opportuno stabilire che siano designati, di norma, quali responsabili del trattamento dei dati personali, i soggetti esterni all'Agenzia regionale che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamenti di dati per conto dell'Agenzia medesima.

Pertanto, qualora occorra affidare un incarico comportante anche trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Per poter operare tale valutazione, occorre quindi specificare che l'incarico ricomprende anche la designazione a responsabile del trattamento di dati personali già nel bando di gara e nel capitolato d'appalto.

Tale designazione deve essere effettuata direttamente in convenzione, nel contratto, nel verbale di aggiudicazione o nel provvedimento di nomina tramite:

a) l'indicazione nominativa qualora al trattamento di dati personali siano preposte persone fisiche;
b) l'individuazione della persona giuridica qualora al suddetto trattamento sia preposta una persona giuridica;
c) l'individuazione della pubblica amministrazione o di qualsiasi altro ente qualora al trattamento siano preposti rispettivamente una pubblica amministrazione o qualsiasi altro ente;
d) l'individuazione di una o più persone fisiche qualora, nei sopra riportati casi di cui alle lettere b) e c), il trattamento di dati personali riguardi esclusivamente un settore specifico e limitato dell'ente.

Qualora siano presenti specifiche e peculiari esigenze, tale individuazione non è effettuata e quindi i soggetti esterni non sono responsabili del trattamento di dati personali, ma titolari o contitolari dello stesso.

In tal caso, pertanto, si procede alla comunicazione dei dati personali al soggetto esterno secondo le modalità previste dall'art. 19 del Codice.

Al fine di facilitare l'individuazione dei casi in cui è necessario da parte dell'Agenzia designare i Responsabili esterni del trattamento, si puntualizza che, qualora i soggetti che si convenzionano o stipulano contratti con l'Agenzia si limitano a scambiare con

quest'ultima dati personali, quali, a titolo indicativo, generalità, numeri di fax e di telefono dei rispettivi collaboratori e referenti, per esigenze connesse all'attuazione di tali convenzioni e contratti, non sarà necessaria la designazione del Responsabile esterno del trattamento. La designazione si renderà invece necessaria qualora tali soggetti trattino, nell'esercizio di attività dedotte in convenzione o contratto, dati personali di terzi per conto dell'Agenzia.

B.9.1) Compiti dei Responsabili del trattamento esterni all'Agenzia regionale
I compiti affidati ai Responsabili esterni del trattamento di dati personali sono i seguenti:

a) adempiere all'incarico attribuito adottando idonee e preventive misure di sicurezza, con particolare riferimento a quanto stabilito dal Codice, dall'Allegato B del Codice, dalle linee guida regionali in materia di protezione dei dati personali e dai disciplinari tecnici regionali, recepiti con determinazione del Direttore dell'Agenzia regionale, e richiamati in tutto o in parte nello specifico incarico;
b) predisporre, qualora l'incarico comprenda la raccolta di dati personali, l'informativa di cui all'art. 13 del Codice e verificare che siano adottate le modalità operative necessarie perché la stessa sia effettivamente portata a conoscenza degli interessati;
c) dare direttamente riscontro oralmente, anche tramite propri incaricati, alle richieste verbali dell'interessato di cui all'art. 7, commi 1 e 2, del Codice, nei termini previsti dal medesimo Codice (art. 8, comma 1, art. 146) e con le modalità individuate nella Sezione C.4 dei presenti indirizzi applicativi ;
d) trasmettere, con la massima tempestività, le istanze dell'interessato per l'esercizio dei diritti di cui agli artt. 7 e ss. del Codice che necessitino di riscontro scritto al Direttore dell'Agenzia regionale, per consentire allo stesso di dare riscontro all'interessato nei termini stabiliti dal Codice (art. 8, comma 1, art. 146) e con le modalità individuate nella Sezione C.4 dei presenti indirizzi applicativi ;
e) fornire al Direttore dell'Agenzia regionale la massima assistenza, necessaria per soddisfare tali richieste, nell'ambito dell'incarico affidatogli;
f) individuare le persone fisiche incaricate del trattamento dei dati personali e fornire alle stesse istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; l'incarico è conferito con modalità tali da poter associare ai nominativi delle persone incaricate i trattamenti che le stesse sono autorizzate ad effettuare;
g) consentire al Direttore dell'Agenzia regionale, dandogli piena collaborazione, verifiche periodiche, tramite invio di specifici report a cadenza temporale (la cadenza è annuale, salvo che il rapporto contrattuale o convenzionale con il Responsabile esterno abbia durata inferiore) e/o a richiesta, contenenti a titolo esemplificativo e a seconda dell'incarico affidato al Responsabile esterno le seguenti informazioni: adozione del Documento programmatico sulla Sicurezza (DPS); adozione degli atti di individuazione degli incaricati, specificando in particolare le istruzioni fornite agli incaricati stessi; predisposizione dell'informativa di cui all'art. 13 del Codice (nel caso in cui il trattamento consista in una raccolta di dati personali), con specifica delle modalità operative con cui la stessa è portata a conoscenza degli interessati (ad esempio: consegna di copia dell'informativa e raccolta della firma per presa visione);
h) attestare, qualora l'incarico affidato ricomprenda l'adozione di misure minime di sicurezza, la conformità degli interventi alle disposizioni di cui alla misura 25

dell'Allegato B del Codice e trasmettere tale attestazione al Direttore dell'Agenzia regionale (al riguardo si evidenzia che la predetta misura 25 stabilisce che *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 Disciplinare tecnico in materia di misure minime di sicurezza di cui all'Allegato B del Codice).*

B.9.2) Nell'**Allegato 2** ai presenti indirizzi applicativi è riportato il fac-simile della clausola da inserire negli atti sopraindicati (convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina) stipulati o adottati dall'Agenzia regionale, ove, si ribadisce, l'altra parte effettui per conto dell'Agenzia un trattamento di dati personali. Nel caso in cui tali atti siano già in essere, il fac-simile verrà utilizzato come nota integrativa degli atti medesimi, da trasmettere all'altra parte. Il fac-simile và completato a cura delle strutture dell'Agenzia regionale (Servizi, Unità Funzionale e relativi settori interni) per gli elementi di rispettiva competenza.

SEZIONE C

DISCIPLINARI TECNICI

Di seguito sono evidenziate, sia per la loro particolare rilevanza che per la loro ricorrenza nella pratica, alcune regole previste nei Disciplinari tecnici adottati con le determinazioni del Direttore generale "Organizzazione, personale, sistemi informativi e telematica" e alla cui lettura integrale comunque si rinvia. Alle regole dei Disciplinari, adattate, ove si è reso necessario, al contesto organizzativo e funzionale dell'Agenzia regionale, devono attenersi tutti i collaboratori dell'Agenzia medesima, compresi coloro che prestano servizio in forza di contratti di collaborazione coordinata e continuativa o a progetto, e di contratti di somministrazione di lavoro a tempo determinato (lavoratori cd. interinali).

C.1) DISCIPLINARE TECNICO RELATIVO AL CONTROLLO DEGLI ACCESSI AI LOCALI DELLA GIUNTA DELLA REGIONE EMILIA-ROMAGNA

Le indicazioni contenute in detto Disciplinare mirano alla riduzione dei rischi derivanti dall'accesso di soggetti non autorizzati alle sedi della Giunta della Regione Emilia-Romagna (di seguito denominata Ente) e sono rivolte in particolare a chi, a vario titolo, è incaricato di esercitare un ruolo di controllo degli accessi, anche al fine di tutela delle persone e dei dati.
Le procedure indicate nel Disciplinare, che si differenziano in relazione ai soggetti che accedono e alla tipologia dei locali a cui è richiesto l'accesso, sono rivolte, oltre che agli addetti di portinerie:

- ai dipendenti regionali;
- ai collaboratori regionali non dipendenti;
- alle segreterie dell'Ente.

Con dipendenti regionali e collaboratori regionali non dipendenti si intendono tutti coloro che alle dipendenze dirette della Giunta e/o di Agenzie/Enti/Istituti regionali, svolgono la propria attività lavorativa in sedi della Giunta regionale.

I dipendenti e i collaboratori regionali non dipendenti sono tenuti a:

- esibire, se richiesto, agli addetti di portineria il badge/carta multiservizi/documento di riconoscimento;
- accertarsi dell'arrivo del visitatore atteso dopo essere stati avvertiti dagli addetti di portineria. Qualora, dopo un ragionevole lasso di tempo non fossero raggiunti dal visitatore, sono tenuti a darne immediata comunicazione agli addetti di portineria;
- richiedere al proprio responsabile di struttura, qualora necessario, l'autorizzazione ad accedere o permanere nei locali delle sedi dell'Ente al di fuori degli orari di apertura delle stesse;
- recarsi in maniera sollecita in portineria, qualora venga consegnato materiale a loro destinato.

Le segreterie, al fine di semplificare le procedure di controllo e agevolare l'accesso di visitatori attesi, comunicano anticipatamente alle portinerie della sede individuata la

convocazione di incontri/riunioni/conferenze stampa a cui partecipano anche soggetti esterni secondo le procedure previste nel Disciplinare tecnico.
Nel caso di convegni/seminari/corsi organizzati in ambienti non comunicanti con l'interno della sede regionale, le segreterie delle strutture sono tenute a:

- fornire agli addetti di portineria una preventiva informazione delle manifestazioni programmate al fine di un corretto indirizzamento dei partecipanti;
- provvedere, solo quando se ne ravvisa la necessità per finalità di servizio, alla registrazione dei partecipanti, premurandosi di raccogliere solo i dati strettamente necessari per le finalità della registrazione, quali nome e cognome e struttura/ente di appartenenza;
- fornire l'informativa di cui all'art. 13 del Codice a chiunque venga richiesto di registrare i propri dati personali. (Si veda il fac-simile di informativa di cui all'**Allegato 1** ai presenti indirizzi applicativi);
- non produrre fotocopia dei documenti di riconoscimento dei partecipanti.

Con riferimento particolare ai locali dell'Agenzia regionale che ospitano elaboratori Server, si fa presente che, data la natura di tali elaboratori, l'accesso agli stessi sarà consentito unicamente ai collaboratori autorizzati e al personale esterno all'Agenzia regionale, preposto ai relativi interventi di manutenzione. Le modalità di accesso autorizzato saranno definite con apposita nota del Direttore dell'Agenzia regionale.

C.2) DISCIPLINARE TECNICO IN MATERIA DI SICUREZZA DELLE APPLICAZIONI INFORMATICHE NELLA GIUNTA DELLA REGIONE EMILIA-ROMAGNA.

Il Disciplinare descrive gli aspetti tecnici e procedurali richiesti per il design, lo sviluppo, il deployment, il test e la gestione di un'applicazione sicura. Particolare riguardo è dedicato alle applicazioni web in quanto maggiormente esposte a minacce per la loro caratteristica intrinseca di rendere disponibili servizi ad un numero elevato, e spesso indefinito, di utenti. Nel Disciplinare sono riportati partitamene i rischi (minacce) cui sono esposte le applicazioni informatiche e le misure per contrastarli.
Il Disciplinare costituisce strumento di riferimento per i soggetti incaricati di:

- progettare, sviluppare, acquistare un'applicazione;
- valutare/scegliere fornitori di servizi di sviluppo applicazioni;
- testare la sicurezza di applicazioni;
- adeguare un'applicazione ai criteri di sicurezza previsti dalla normativa vigente;
- installare, gestire o manutenere un'applicazione.

I destinatari del Disciplinare devono considerare le minacce di sicurezza e le contromisure disponibili relativamente a dati e informazioni, secondo le indicazioni ivi fornite. Tali indicazioni si basano sul fondamento che un'applicazione è sicura quando è in grado di preservare *confidenzialità*, *integrità* e *disponibilità* delle risorse, assicurando costantemente:

- l'identificazione dell'utente che accede alle risorse;

- la limitazione degli accessi alle risorse;
- la comunicazione sicura con l'esterno;
- la conservazione sicura dei dati.

Requisiti minimi previsti dalla normativa vigente

Secondo quanto stabilito dalla regola 25 dell'Allegato B del Codice, qualora i destinatari del Disciplinare in parola siano soggetti esterni fornitori di prodotti o servizi utilizzati dall'Agenzia regionale per l'adozione di misure minime di sicurezza ai sensi della normativa vigente, gli stessi devono attestare la conformità di quanto fornito alle seguenti disposizioni:

1) utilizzo di una procedura di autenticazione che permetta l'identificazione dell'incaricato attraverso opportune credenziali di autenticazione;
2) utilizzo di una parola chiave, quando prevista dal sistema di autenticazione, composta da almeno otto caratteri;
3) possibilità di modifica della parola chiave, quando prevista dal sistema di autenticazione, da parte dell'incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi;
4) possibilità di disattivazione delle credenziali di autenticazione non utilizzate da almeno sei mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
5) esistenza di meccanismi di autorizzazione per la separazione dei privilegi degli incaricati in base a diversi profili autorizzativi;
6) esistenza di meccanismi di backup che consentano il salvataggio dei dati con frequenza almeno settimanale.

Nel caso l'applicazione fornita sia destinata al trattamento di dati sensibili e/o giudiziari, l'attestazione deve inoltre indicare la conformità della stessa alle seguenti ulteriori disposizioni:

7) possibilità di modifica della parola chiave quando prevista dal sistema di autenticazione, da parte dell'incaricato al primo utilizzo e, successivamente, almeno ogni tre mesi;
8) esistenza di meccanismi di ripristino dei dati che permettano la ricostruzione degli stessi, in caso di danneggiamento, in tempi non superiori ai sette giorni;
9) utilizzo di tecniche di cifratura o codici identificativi, tali da rendere temporaneamente inintelligibili i dati sensibili e/o giudiziari anche a chi è autorizzato ad accedervi e da permettere l'identificazione degli interessati solo in caso di necessità.

Il Disciplinare deve essere portato a conoscenza dei soggetti che forniscono all'Agenzia regionale servizi di progettazione, sviluppo e installazione di applicazioni informatiche, i quali, peraltro, devono essere designati Responsabili esterni con un'apposita clausola, utilizzando il fac-simile di cui all'**Allegato 2** ai presenti indirizzi applicativi, da inserire nei contratti stipulati con l'Agenzia medesima, qualora trattino dati personali per conto di

quest'ultima. I fornitori dei suddetti servizi possono trattare dati personali per conto dell'Agenzia regionale nella fase in cui testano la funzionalità dei programmi realizzati e in quella di manutenzione, in quanto in tali occasioni tali fornitori potrebbero venire a conoscenza di dati personali già inseriti dai collaboratori dell'Agenzia nelle banche dati gestite con i programmi da essi sviluppati. Si fa presente, infatti, che il venire a conoscenza di dati personali costituisce ai sensi del Codice trattamento dei dati medesimi.
Ove i fornitori di tali servizi in nessun caso venissero a conoscenza di dati personali, sia perché non vengono incaricati di curare i test di funzionalità o la manutenzione, o perché, ove incaricati di ciò, i dati personali sono anonimi (es. criptati), non sarà necessario individuarli Responsabili esterni del trattamento e quindi nei contratti di fornitura non si dovrà inserire la clausola di cui al suddetto fac-simile in **Allegato 2**. Sarà in ogni caso necessario inserire nel contratto una clausola in base alla quale il fornitore del servizio "*Si impegna ad attestare la conformità del servizio che verrà fornito alle disposizioni di cui alla misura 25 dell'Allegato B del Codice e a trasmettere tale attestazione al Direttore dell'Agenzia regionale*".

C.3) DISCIPLINARE TECNICO PER UTENTI SULL'UTILIZZO DEI SISTEMI INFORMATIVI NELLA GIUNTA DELLA REGIONE EMILIA-ROMAGNA

Ai fini di tale Disciplinare tecnico, si intende per sistema informativo il complesso dei dati, delle applicazioni, delle risorse tecnologiche, delle risorse umane, delle regole organizzative e delle procedure deputate all'acquisizione, memorizzazione, consultazione, elaborazione, conservazione, cancellazione, trasmissione e diffusione delle informazioni.
I destinatari del Disciplinare devono considerare le minacce di sicurezza e le contromisure disponibili (comportamenti da evitare o da tenere) relativamente a dati e informazioni, secondo le indicazioni ivi fornite che disciplinano i seguenti aspetti della sicurezza globale del sistema informativo:

- sicurezza fisica;
- controllo degli accessi;
- protezione dei dati trattati senza l'ausilio di strumenti elettronici;
- protezione e disponibilità dei dati;
- protezione delle reti e delle comunicazioni;
- prevenzione e gestione degli incidenti informatici.

La protezione dei dati e delle informazioni nel loro complesso è condizione necessaria per garantire il rispetto dei requisiti di sicurezza che la normativa vigente impone a tutti i soggetti che, a vario titolo, effettuano il trattamento di dati personali. A causa dell'interconnettività e dell'interdipendenza fra le componenti di un sistema informativo, infatti, i problemi di sicurezza su una sola di esse propagano i loro effetti, incidendo gravemente sulla sicurezza del sistema (per es. una postazione di lavoro non adeguatamente protetta può rendere vulnerabile la intranet dell'Ente anche in presenza di firewall o altri sistemi di sicurezza perimetrale).
Per quanto sopra, l'ambito di applicabilità del Disciplinare tecnico si estende non solo ai cd. responsabili e incaricati del trattamento di dati personali individuati dal titolare, ma a

tutti i dipendenti appartenenti all'organico dell'Ente che utilizzano le risorse dei sistemi informativi, nonché a tutti coloro che a vario titolo le utilizzano in nome e/o per conto dell'Ente, ovvero che sono autorizzati, in base ad uno specifico titolo (per es. convenzioni, contratti, ecc.) ad utilizzarlo. Nel seguito del Disciplinare, i soggetti di cui sopra sono denominati "utenti".

Con riferimento particolare alle postazioni di lavoro il Disciplinare prevede quanto segue:

1. Utilizzare la postazione di lavoro, fornita dall'Ente quale supporto all'attività lavorativa, in modo pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi.
2. Proteggere i computer e le altre strumentazioni informatiche, in caso di assenza, anche temporanea, dalla postazione di lavoro, tramite la sospensione o il blocco della sessione di lavoro. In particolare:

   2.1 L'utente che si allontana dalla propria postazione di lavoro, ma sia certo di ritornarvi entro la fine della giornata lavorativa, è tenuto a:

   - accertarsi di aver chiuso tutti i documenti aperti, per permettere ad altri utenti di utilizzare gli stessi se condivisi su server di rete;
   - bloccare il sistema (per es. sui sistemi Windows 2000/XP con la combinazione di tasti CRTL+ALT+CANC e quindi "Blocca computer") o attivare la funzione di logout (per es. sui sistemi Windows 2000/XP con la combinazione di tasti CRTL+ALT+CANC e quindi "Disconnetti");
   - impostare l'attivazione dello screen saver entro pochi minuti di inattività per impedire la lettura dei dati presenti a video; è necessario che l'accesso al sistema dopo l'intervento dello screen saver sia vincolato all'autenticazione dell'utente, abilitando l'opzione "Al ripristino proteggi con password".

   2.2 L'utente che si allontana dalla propria postazione di lavoro per non ritornarvi entro la fine della giornata lavorativa, è tenuto a terminare la sessione di lavoro (per es. arrestando il sistema o attivando la funzione "Disconnetti").

Con riferimento particolare ai dispositivi mobili (computer portatili, palmari, telefoni cellulari, pendrive, macchine fotografiche digitali, videocamere, ecc.) il Disciplinare prevede tra l'altro che gli stessi possono essere utilizzati in contesti diversi anche al di fuori di sedi dell'Ente ed in aree non sicure. Ciò rappresenta una minaccia per la sicurezza dei sistemi nel momento in cui, per esempio, un portatile si riconnette alla rete interna.
L'utente dei dispositivi mobili è tenuto in particolare sia all'interno che all'esterno della sede di lavoro a:

- custodire adeguatamente i dispositivi durante le ore notturne o in periodi di assenza (per es. non lasciare i dispositivi sulla scrivania ma custodirli invece in armadi o cassetti chiusi a chiave, dotare i portatili di dispositivi di fissaggio, ecc.);
- trasportare i dispositivi come bagaglio a mano durante i viaggi in aereo;
- non lasciare i dispositivi incustoditi, neanche temporaneamente, durante i viaggi effettuati in treno o con altri mezzi di trasporto;

- non lasciare i dispositivi in auto, se non in casi eccezionali, e comunque chiuderli nel bagagliaio non a vista in modo da non evidenziarne la presenza dall'esterno;
- non lasciare i dispositivi in vista nelle stanze degli hotel, ma chiuderli in un armadio o in una valigia o depositarli in cassaforte se si prevede un'assenza prolungata.

Ogni collaboratore dell'Agenzia che ha in dotazione un computer portatile deve procedere al collegamento di tale dispositivo mobile alla LAN della Regione almeno una volta ogni 30 giorni per effettuare gli aggiornamenti automatici del software antivirus e delle patch di sicurezza, chiedendo, ove necessario, il supporto tecnico del referente dell'Agenzia appositamente individuato.

C.4) DISCIPLINARE TECNICO PER L'ESERCIZIO DEL DIRITTO DI ACCESSO DELL'INTERESSATO AI PROPRI DATI PERSONALI NELLA GIUNTA DELLA REGIONE EMILIA-ROMAGNA.

Il Disciplinare in oggetto premette che il Codice individua tre diritti fondamentali:
- il diritto alla protezione dei dati personali (chiunque ha il diritto di esercitare un controllo sui dati che lo riguardano);
- il diritto alla riservatezza (chiunque ha il diritto di proteggere la propria vita privata o familiare);
- il diritto all'identità personale (chiunque ha il diritto di non vedere sviata la propria immagine, politica, etica o sociale diritto di ottenere la conoscenza).

L'interessato, che è il soggetto cui si riferiscono i dati, ha, in base al Codice, specifici diritti distinguibili in due categorie ben determinate: la prima, riferita ai primi tre commi dell'art. 7, consiste nel di dati e notizie e di compiere particolari attività; la seconda, riferita al comma 4 dell'art. 7, consiste nel diritto di opporsi al trattamento dei propri dati personali.

Il Titolo II del Codice, interamente dedicato ai diritti dell'interessato, è costituito da un complesso di disposizioni che individuano tali diritti e ne disciplinano le modalità di esercizio. Tali disposizioni sono riportate nell'**Allegato 5** ai presenti indirizzi applicativi.

Diritto di accesso ai propri dati personali e diritto di accesso ai documenti amministrativi

Le due forme di accesso previste dalle vigenti disposizioni di legge (accesso ai documenti amministrativi secondo quanto disposto dalla L. 241/90 e successive modificazioni ed accesso ai propri dati personali ai sensi dell'art. 7 del Codice) restano soggette alle rispettive discipline.

Qualora la richiesta di accesso non sia qualificata dal richiedente, specificando se si tratta di accesso ai propri dati personali o di accesso a documenti amministrativi, la qualificazione stessa è effettuata dal soggetto ricevente (P.A.) sulla base del contenuto della richiesta.

Le principali distinzioni possono così riassumersi:

- per l’accesso ai documenti amministrativi è necessario dimostrare l’interesse ad accedere, mentre ciò non è richiesto per l’accesso ai propri dati personali;
- l’accesso ai documenti amministrativi è soggetto a limitazioni qualora il documento contenga dati relativi a soggetti terzi, mentre l’accesso ai propri dati personali è sempre possibile, con la sola esclusione delle specifiche disposizioni disciplinate dall’art. 8 del Codice (quali ad esempio trattamenti che sono effettuati da Commissioni parlamentari di inchiesta o per ragioni di giustizia). In particolare, nel caso di documenti amministrativi che contengano dati idonei a rivelare lo stato di salute o la vita sessuale, l’accesso ai documenti è consentito soltanto se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso è di rango almeno pari al diritto dell’interessato alla riservatezza dei dati che lo riguardano, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;
- in caso di accesso ai documenti amministrativi non sussiste l’obbligo della intelligibilità dei documenti forniti (in caso di codici o cifrature non è necessario fornire i parametri di riferimento), mentre tale obbligo sussiste nel caso di accesso ai propri dati personali;
- 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 dell’interessato;
- la richiesta di accesso ai documenti amministrativi avvia uno specifico procedimento amministrativo che prevede, tra l’altro, l’avviso ai controinteressati, mentre l’accesso ai propri dati personali non prevede la stessa accortezza procedurale;
- l’accesso ai documenti amministrativi non obbliga a rendere inintelligibili i dati

Il diritto di accesso ai documenti amministrativi può essere esercitato, anche in relazione a situazioni tutelate dal Codice, per ottenere la conoscenza di informazioni che, al contrario, non possono essere comunicate a soggetti privati o diffuse (ad esempio: nel caso di graduatorie di concorsi da un lato è vietato indicare espressamente nell’atto - da pubblicare o esporre in bacheca - il riferimento anche indiretto a particolari requisiti che consentono di associare dati sensibili a un soggetto identificato, dall’altro, qualora questi stessi requisiti producano punteggi o siano titoli di precedenza, il concorrente escluso dalla graduatoria può chiedere ed ottenere l’accesso a tali dati in quanto ha un interesse giuridico da tutelare).

<u>Esercizio del diritto di accesso ai propri dati personali.</u>

Il Disciplinare in parola distingue tra soggetti interni e soggetti esterni all’Ente che possono esercitare il diritto di accesso ai propri dati personali ai sensi dell’articolo 7 e ss. del Codice.

Per soggetti interni si intendono i soggetti che, a vario titolo e in vario modo, interagiscono, o hanno interagito, con l’Ente attraverso un rapporto di lavoro dipendente, o un rapporto di collaborazione in via continuativa, quindi:
- i dipendenti a tempo determinato o indeterminato, compresi i contratti di formazione e lavoro;
- gli ex dipendenti a tempo determinato o indeterminato;
- i lavoratori con contratto di somministrazione a tempo determinato (cd. interinali);

- i co.co.co e i co.co.pro. (collaboratori coordinati e continuativi e collaboratori a progetto);
- tutti i lavoratori che, attraverso una qualunque forma di collaborazione prevista dalla disciplina sul lavoro, prestano o hanno prestato attività presso l'Ente.

Per soggetti esterni si intendono i soggetti che non rientrano nella precedente definizione.

L'esercizio dei diritti previsti dall'art. 7 del Codice da parte dei soggetti esterni avviene mediante la formulazione di una richiesta presentata, di norma, direttamente dall'interessato (soggetto cui si riferiscono i dati personali).
L'interessato può essere:
- la persona fisica a cui si riferiscono i dati;
- il legale rappresentante dell'ente, associazione od organismo a cui si riferiscono i dati.

La richiesta può essere presentata anche da un soggetto terzo a cui l'interessato ha conferito, per iscritto, delega o procura, che agisce per conto dell'interessato, nell'esercizio dei diritti spettanti a quest'ultimo, cioè il delegato o procuratore dell'interessato (può trattarsi di persone fisiche o persone giuridiche, come ad esempio enti, organismi, associazioni, organismi portatori di interessi diffusi).

L'esercizio dei diritti individuati dall'art. 7 del Codice si estende anche ai dati relativi a persone decedute.

Modalità di presentazione della richiesta

Le modalità di presentazione della richiesta da parte dell'interessato possono essere varie: posta, lettera raccomandata, telefax, posta elettronica (e-mail), consegna manuale e, in alcuni casi, anche formulazione orale.

La richiesta orale è prevista solo per l'esercizio dei diritti di cui ai commi 1 e 2 dell'art. 7 del Codice.
Il soggetto che presenta la richiesta orale deve identificarsi, anche tramite esibizione di un documento di identità in corso di validità.
La richiesta che si riferisce ai primi due commi dell'art. 7 del Codice, sia presentata oralmente che per iscritto, dopo essere stata presentata una prima volta, può essere ripresentata solo se è trascorso un intervallo non minore di 90 giorni.
Solo se sussistono motivi di necessità e di urgenza, tale richiesta può essere presentata anche prima che siano trascorsi 90 giorni. Spetta al titolare del trattamento valutare la validità e sussistenza dei motivi ed accogliere la richiesta, oppure invocare il rispetto dei termini previsti dal Codice.

La richiesta scritta è prevista per l'esercizio di tutti i diritti indicati all'art. 7, ed è obbligatoria per l'esercizio di quelli descritti ai commi 3 e 4.
Se la richiesta è presentata per posta, fax o e-mail, deve essere allegata alla stessa fotocopia di un documento di identità in corso di validità; in particolare, se l'invio è effettuato per via telematica, il documento di riconoscimento deve essere digitalizzato.
Può essere formulata con testo libero, oppure utilizzando la modulistica riportata in **Allegato 3** ai presenti indirizzi applicativi.

La richiesta deve essere sottoscritta. Nei casi consentiti di formulazione orale della richiesta, le annotazioni da parte dell'incaricato o, in sua assenza, della Segreteria amministrativa, tengono luogo della sottoscrizione; le annotazioni sono fatte su un apposito registro tenuto dalla Segreteria amministrativa.

Riscontro della richiesta

Il riscontro scritto a firma del Direttore dell'Agenzia regionale è effettuato nei casi in cui:

- la richiesta dell'interessato sia volta ad ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, secondo quanto previsto dal comma 3, lettera b) dell'art. 7 del Codice;
- l'interessato si opponga, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, secondo quanto previsto dal comma 4 dell'art. 7 del Codice.

In tutti gli altri casi previsti dall'art. 7 del Codice il riscontro alle istanze degli interessati può essere dato anche tramite un incaricato, con le seguenti precisazioni:

- direttamente e verbalmente dall'incaricato che riceve un'istanza formulata oralmente; in questo caso l'incaricato può essere qualunque collaboratore dell'Agenzia regionale che opera nel settore competente a trattare i dati oggetto della richiesta;
- dal dirigente o dal funzionario competenti, secondo la vigente normativa, a fornire risposte scritte relativamente ai dati oggetto della richiesta (cfr. L.R. 32/1993 sul responsabile del procedimento e deliberazione di Giunta regionale n. 450/2007).

Contenuto del riscontro

Se non diversamente specificato nella richiesta, il riscontro all'interessato comprende tutti i dati personali, di cui l'Agenzia regionale è titolare, che si riferiscono all'interessato stesso.
Qualora la richiesta dell'interessato specifichi dati personali o categorie di essi, il riscontro è limitato all'oggetto della richiesta.

Tempi del riscontro

Il riscontro alla richiesta dell'interessato è fornito **entro 15 giorni** dal suo ricevimento.

Tale termine può essere **prolungato a 30 giorni**, nel caso in cui le operazioni necessarie per effettuare un integrale riscontro sono di particolare complessità, oppure se ricorre un altro giustificato motivo.

In caso di proroga è necessario darne comunicazione scritta all'interessato con nota entro il termine di 15 giorni dal ricevimento della richiesta di accesso, specificandone i motivi.

L'interessato può comunque ricorrere all'autorità giudiziaria ordinaria o al Garante per le forme di tutela previste, nel caso in cui:

- non venga data risposta entro il termine di 15 giorni dalla data di ricevimento della richiesta;
- la richiesta non venga accolta, in tutto o in parte. In questo caso può ricorrere anche prima della scadenza dei termini previsti per il riscontro;
- non ritenga sufficienti o adeguate le ragioni poste a sostegno della proroga. In questo caso può ricorrere solo allo scadere del termine minimo di 15 giorni.

Forma del riscontro
La modalità utilizzata per il riscontro è preferibilmente, quando ciò non contrasta con oggettive difficoltà, la stessa utilizzata dall'interessato per la presentazione dell'istanza (formulazione orale, cartacea, informatica). Il mezzo utilizzato per l'invio del riscontro al richiedente sarà di conseguenza: comunicazione orale o visione, posta o fax, e-mail.

Qualora l'estrazione dei dati si riveli di particolare difficoltà (per il trattamento, la natura, la qualità e la quantità dei dati), il riscontro all'interessato può essere dato anche tramite esibizione o consegna in copia degli atti e dei documenti che contengono i dati personali richiesti.

In alternativa alla comunicazione orale il soggetto richiedente può richiedere di visionare i dati direttamente su elaboratore elettronico, sempre che la comprensione dei dati richiesti risulti agevole e chiara. Alla comunicazione orale o visione è, non obbligatoriamente, affiancata l'estrazione dei dati su supporto cartaceo o informatico, da consegnare al richiedente.

La trasposizione dei dati su supporto cartaceo o informatico, o la loro trasmissione per via telematica è viceversa sempre dovuta quando vi è una esplicita richiesta scritta.

Comprensibilità del riscontro
La comunicazione all'interessato dei dati personali che lo riguardano deve essere fornita in forma intelligibile e chiara, usando un linguaggio comprensibile.

Qualora i dati personali dell'interessato fossero costituiti da codici o sigle, quindi non risultassero intelligibili, il riscontro deve contenere anche i parametri per la comprensione del significato dei codici e delle sigle.
Se i dati dell'interessato sono collegati ad altri dati personali di soggetti terzi, questi ultimi devono essere esclusi dalla comunicazione all'interessato.
Solo nei casi in cui la protezione di dati personali di terzi comprometta la comprensibilità del riscontro fornito, è possibile non procedere a tale protezione e fornire nella comunicazione all'interessato anche dati personali altrui.
Questa particolare circostanza deve essere dimostrabile.

C.5) DISCIPLINARE TECNICO IN MATERIA DI VIDEOSORVEGLIANZA NELLA GIUNTA REGIONALE

Il Disciplinare tecnico descrive le regole tecniche ed organizzative da applicare nei casi di trattamento di dati personali effettuato mediante sistemi di videosorveglianza.

Si definisce sistema di videosorveglianza l'insieme di apparecchiature audiovisive che rilevano in modo continuativo immagini, eventualmente associate a suoni, relative a persone identificabili, la cui utilizzazione sia necessaria per adempiere a funzioni istituzionali di sorveglianza del Titolare, ovvero per protezione di beni, persone, dati personali e patrimonio informativo di proprietà, responsabilità o titolarità dell'Ente.

Principi generali

Quando si effettuano trattamenti di dati personali mediante sistemi di videosorveglianza deve essere garantito il rispetto dei principi di:

- liceità;
- necessità;
- proporzionalità;
- finalità.

In particolare, il trattamento di dati personali tramite un sistema di videosorveglianza è lecito solo se soddisfa il principio di finalità (cfr. art. 11, lett. b del Codice), ossia i dati sono trattati per scopi determinati, espliciti e legittimi. Gli scopi legittimi sono quelli che rientrano nelle funzioni istituzionali del Titolare.

Tali scopi sono:

a) tutela del patrimonio o delle persone;
b) protezione dei dati personali e dei sistemi informativi;
c) sorveglianza dei fenomeni ambientali, con particolare riferimento al controllo del livello dei corsi d'acqua o dei fenomeni idrogeologici.

Trattamenti consentiti

Le operazioni di trattamento di dati personali mediante l'impiego di sistemi di videosorveglianza sono:

- consultazione in tempo reale;
- registrazione;
- consultazione dei dati registrati;
- conservazione dei dati registrati;
- effettuazione di copie;
- comunicazione;
- cancellazione.

In nessun caso sono diffusi i dati rilevati attraverso sistemi di videosorveglianza.

Quanto al periodo di conservazione dei dati registrati, un tempo superiore a sette giorni deve essere valutato come eccezionale e in relazione a necessità derivanti da un evento già accaduto (ad es. atti di vandalismo verificatisi) o realmente incombente (ad es. sorveglianza del livello dei corsi d'acqua), la cui sussistenza possa risultare documentabile. In particolare, relativamente alla sorveglianza dei corsi d'acqua, il periodo di conservazione è pari a 30 giorni, trascorsi i quali i dati sono automaticamente cancellati dal sistema. Il prolungamento dei tempi di conservazione, in questo caso, è motivato dall'assoluta necessità di consentire agli operatori di valutare per intero l'evento di piena, che in alcuni casi può durare diversi giorni, e di recarsi in loco per eseguire il download dei dati che non può essere effettuato da remoto.

Informativa di cui all'art. 13 del Codice

Le zone soggette a videosorveglianza devono essere adeguatamente segnalate e agli interessati deve essere fornita idonea informativa.

L'informativa da utilizzare in ambienti esterni deve essere conforme al modello indicato in **Allegato 4** ai presenti indirizzi applicativi, da completarsi con l'indicazione del fine per cui

si installa una videocamera. Il numero e le modalità di affissione della stessa dipendono dalla vastità dell'area, dalle modalità di ripresa e dal numero di videocamere installate.
In luoghi diversi dalle aree esterne, il modello di cui sopra va integrato con almeno un avviso circostanziato che riporti gli elementi dell'art. 13 del Codice.
In particolare l'informativa, sia essa posta internamente o esternamente agli ambienti:
- deve essere collocata nell'area effettivamente ripresa o nelle immediate vicinanze;
- deve avere un formato ed un posizionamento tali da essere chiaramente visibile;
- può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione.

Nuove installazioni/riposizionamenti/rimozioni delle apparecchiature di videosorveglianza
Prima di installare ciascuna nuova apparecchiatura, il Titolare deve valutare la proporzionalità del sistema agli scopi prefissati e deve motivare per iscritto le scelte fatte, anche sulla base degli elementi forniti dallo specifico settore che richiede l'installazione dell'apparecchiatura.
Preventivamente ad ogni singola nuova installazione, il documento con le motivazioni dell'installazione è depositato alle Rappresentanze sindacali per un periodo non inferiore a 20 giorni, trascorsi i quali, in mancanza di osservazioni da parte delle stesse, si considera acquisito il loro consenso alla nuova installazione.
In un apposito elenco devono essere riportate le videocamere installate dall'Agenzia regionale, la loro ubicazione e la relativa motivazione di installazione. Tale elenco dovrà essere conservato ed aggiornato anche ai fini dell'eventuale esibizione in occasione di visite ispettive o dell'esercizio dei diritti dell'interessato o di contenzioso.
Nel caso di riposizionamento delle apparecchiature deve essere applicata la medesima procedura prevista per le nuove installazioni.
Nel caso di rimozione delle apparecchiature, della stessa è data informazione alle organizzazioni sindacali e la documentazione è conservata quale aggiornamento dell'elenco sopraindicato.

C.6) DISCIPLINARE TECNICO IN MATERIA DI VERIFICHE DI SICUREZZA E CONTROLLI SULL'UTILIZZO DEI BENI MESSI A DISPOSIZIONE DALL'AMMINISTRAZIONE (IN PARTICOLARE SULLE STRUMENTAZIONI INFORMATICHE E TELEFONICHE)

Le verifiche di sicurezza previste dal Disciplinare in parola sono effettuate sul sistema informativo della Giunta regionale.
Per "sistema informativo" si intende il complesso dei dati, delle applicazioni, delle risorse tecnologiche, delle risorse umane, delle regole organizzative e delle procedure deputate all'acquisizione, memorizzazione, consultazione, elaborazione, conservazione, cancellazione, trasmissione e diffusione delle informazioni.
A causa dell'interconnettività e dell'interdipendenza fra le componenti di un sistema informativo, i problemi di sicurezza su una sola di esse propagano i loro effetti incidendo gravemente sulla sicurezza del sistema nel suo complesso (per esempio: una postazione di lavoro non adeguatamente protetta può rendere vulnerabile la intranet dell'Ente anche in presenza di firewall o altri sistemi di sicurezza perimetrale). Le verifiche di sicurezza oggetto del Disciplinare sono effettuate, pertanto, anche sulle strumentazioni assegnate ad altri titolari di trattamenti di dati personali, quali le Agenzie regionali, tra cui quella di

protezione civile, quando vi è condivisione o interconnessione con le infrastrutture tecnologiche dell'Ente (ad esempio: dominio di autenticazione e servizi di rete). A tale fine il Disciplinare ha previsto che gli altri titolari di trattamenti di dati personali che utilizzano strumentazioni in condivisione o interconnessione con le infrastrutture tecnologiche dell'Ente sottoscrivono con lo stesso Ente appositi protocolli di intesa. Successive disposizioni della Regione, tuttavia, hanno stabilito che, in luogo del protocollo di intesa, ogni Agenzia regionale designasse la Giunta regionale Responsabile esterno del trattamento dei dati.
Le verifiche sono effettuate:
- per preservare la riservatezza, l'integrità e la disponibilità dei dati e delle informazioni;
- per garantire il rispetto di leggi e regolamenti in materia di protezione dei dati personali, in particolare dei requisiti minimi di sicurezza previsti dalla normativa vigente.
Le verifiche consistono in un'attività di monitoraggio sulla conformità dei sistemi informativi e dei comportamenti dei soggetti tenuti a rispettare le prescrizioni e regole comportamentali disposte dagli atti amministrativi di seguito richiamati:

a) Linee guida della Giunta regionale, approvate con D.G.R. n. 1264/ 2005;
b) Disciplinare tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta regionale, approvato con D.D. n. 2653/2007;
c) Disciplinare tecnico relativo al controllo degli accessi ai locali della Giunta regionale,approvato con D.D. n. 2649/2007;
d) Disciplinare tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta regionale, approvato con D.D. n. 2651/2007;
e) Disciplinare tecnico in materia di videosorveglianza nella Giunta regionale, approvato con D.D. n. 604/2007.

Finalità

Le verifiche di sicurezza sono eseguite al fine di:

a) verificare la coerenza del funzionamento dei sistemi informativi con le politiche di sicurezza adottate dall'Ente;
b) verificare la coerenza delle misure di sicurezza adottate con gli standard nazionali e/o internazionali e le normative vigenti in materia;
c) verificare periodicamente la coerenza delle misure adottate con le politiche di sicurezza definite nel Documento Programmatico sulla Sicurezza dell'Ente;
d) individuare gli attacchi ai sistemi informativi (comportamenti che infrangono le politiche di sicurezza);
e) proporre eventuali modifiche o nuove implementazioni ai sistemi di sicurezza sulla base delle verifiche effettuate.

Modalità delle verifiche di sicurezza

Le verifiche di sicurezza possono essere di quattro tipi:

a) puntuali preventive: attività di verifica effettuate precedentemente all'implementazione o modifica sostanziale di un sistema o processo per verificarne la rispondenza alle politiche di sicurezza;

b) puntuali a posteriori: attività di verifica effettuate a seguito del verificarsi di incidenti di sicurezza;

c) periodiche: attività di verifica, manuali o automatizzate, per contrastare minacce incombenti o potenziali, effettuate con cadenza periodica programmata;

d) a campione: attività di verifica effettuate su campioni scelti secondo criteri prestabiliti e ad intervalli di tempo non fissi.

ALLEGATO 1

INFORMATIVA STANDARD PER IL TRATTAMENTO DEI DATI PERSONALI

1. Premessa
Ai sensi dell'art. 13 del D. Lgs. n. 196/2003 - "Codice in materia di protezione dei dati personali" (di seguito denominato "Codice"), l'Agenzia regionale di protezione civile, in qualità di "Titolare" del trattamento, è tenuta a fornirle informazioni in merito all'utilizzo dei suoi dati personali.
Il trattamento dei suoi dati per lo svolgimento di funzioni istituzionali da parte dell'Agenzia regionale di protezione civile in quanto soggetto pubblico non economico, non necessita del suo consenso.

2. Fonte dei dati personali
La raccolta dei suoi dati personali viene effettuata registrando i dati da lei stesso forniti, in qualità di interessato, al momento della iscrizione all'iniziativa/servizio (indicare l'iniziativa o servizio per cui si fa richiesta).

3. Finalità del trattamento
I dati personali sono trattati per le seguenti finalità:

a) ……. (indicare le finalità del trattamento).

4. Modalità di trattamento dei dati
In relazione alle finalità descritte, il trattamento dei dati personali avviene mediante strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità sopra evidenziate e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi.
Adempiute le finalità prefissate, i dati verranno cancellati o trasformati in forma anonima.

5. Facoltatività del conferimento dei dati
Il conferimento dei dati è facoltativo, ma in mancanza non sarà possibile adempiere alle finalità descritte al punto 3 ("Finalità del trattamento").

6. Categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di Responsabili o Incaricati
I suoi dati personali potranno essere conosciuti esclusivamente dagli operatori dell'Agenzia regionale di protezione civile, individuati quali Incaricati del trattamento. Esclusivamente per le finalità previste al paragrafo 3 (Finalità del trattamento), possono venire a conoscenza dei dati personali…….(indicare eventuali soggetti pubblici, autonomi titolari del trattamento, a cui i dati personali possono essere comunicati ed eventuali Responsabili esterni del trattamento, designati dall'Agenzia regionale di protezione civile a seguito di contratto, convenzione, ecc).

7. Diritti dell'Interessato
La informiamo, infine, che la normativa in materia di protezione dei dati personali conferisce agli Interessati la possibilità di esercitare specifici diritti, in base a quanto

indicato all'art. 7 del Codice che qui si riporta:

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'art. 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.

8. Titolare e Responsabili del trattamento

Il Titolare del trattamento dei dati personali di cui alla presente Informativa è l'Agenzia regionale di protezione civile, con sede in Bologna, Viale Silvani 6, cap 40122.
Il Direttore dell'Agenzia è responsabile del riscontro, in caso di esercizio dei diritti sopra descritti.

Le richieste di cui al precedente paragrafo 7 possono essere inoltrate per iscritto o

recandosi direttamente presso gli uffici della segreteria amministrativa dell'Agenzia regionale all'indirizzo sopraindicato. Per tali adempimenti gli uffici della segreteria sono aperti dal lunedì al venerdì dalle 10 alle 13 e il lunedì e il giovedì dalle 15 alle 17 (Tel. 051/284816-17-18-19; Fax 051/284418; e-mail Procivsegr@regione.emilia-romagna.it).

Le richieste di cui all'art. 7, commi 1 e 2, del Codice possono essere formulate anche oralmente.

ALLEGATO 2

CLAUSOLA DA INSERIRE NEI CONTRATTI/CONVENZIONI/VERBALI DI AGGIUDICAZIONE/PROVVEDIMENTI DI NOMINA CON SOGGETTI ESTERNI PER LA DESIGNAZIONE QUALI RESPONSABILI ESTERNI DEL TRATTAMENTO DI DATI PERSONALI

Designazione quale responsabile esterno del trattamento di dati personali

La persona fisica/giuridica/ente/associazione, ai sensi e per gli effetti dell'art. 29 del D.Lgs. n. 196/2003, di seguito denominato Codice, è designata responsabile esterno del trattamento dei dati personali, di cui l'Agenzia regionale di protezione civile è titolare, di seguito specificato:

– ……(indicare l'ambito del trattamento);

e di quei trattamenti che in futuro verranno affidati nell'ambito di questo stesso incarico per iscritto.

Si sottolinea che i compiti e le funzioni conseguenti a tale individuazione sono indicati nel Codice**,** negli indirizzi applicativi approvati con determinazione n. …..del …… del Direttore dell'Agenzia regionale, Sezione B.

I compiti sono di seguito riportati:

a) adempiere all'incarico attribuito adottando idonee e preventive misure di sicurezza, con particolare riferimento a quanto stabilito dal Codice e dal relativo Allegato B, dalla D.G.R. n. 1264/2005 e dal/i Disciplinare/i tecnico/i regionale/i, approvato/i con determinazione/i del Direttore Generale all'Organizzazione, Personale, Sistemi Informativi e Telematica n./nn……del…… e recepito/i con determinazione n. … del……. del Direttore dell'Agenzia regionale (indicare solo il Disciplinare o i Disciplinari che riguardano lo specifico incarico);
b) predisporre, qualora l'incarico comprenda la raccolta di dati personali, l'informativa di cui all'art. 13 del Codice e verificare che siano adottate le modalità operative necessarie perché la stessa sia effettivamente portata a conoscenza degli interessati;
c) dare direttamente riscontro oralmente, anche tramite propri incaricati, alle richieste verbali dell'interessato di cui all'art. 7, commi 1 e 2, del Codice, nei termini previsti dal medesimo Codice (art. 8, comma 1, art. 146) e con le modalità individuate nella Sezione C.4 degli indirizzi applicativi approvati con determinazione n. … del…… del Direttore dell'Agenzia regionale;
d) trasmettere, con la massima tempestività, le istanze dell'interessato per l'esercizio dei diritti di cui agli artt. 7 e ss. del Codice che necessitino di riscontro scritto al Direttore dell'Agenzia regionale, per consentire allo stesso di dare riscontro all'interessato nei termini stabiliti dal Codice medesimo (art. 8, comma 1, art. 146) e con le modalità individuate nella Sezione C.4 degli indirizzi applicativi approvati con determinazione n. … del…… del Direttore dell'Agenzia regionale;
e) fornire al Direttore dell'Agenzia regionale la massima assistenza, necessaria per soddisfare tali richieste, nell'ambito dell'incarico affidatogli;
f) individuare le persone fisiche incaricate del trattamento dei dati personali e fornire alle stesse istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando

sull'attuazione delle istruzioni impartite; l'incarico è conferito con modalità tali da poter associare ai nominativi delle persone incaricate i trattamenti che le stesse sono autorizzate ad effettuare;

g) consentire al Direttore dell'Agenzia regionale, dandogli piena collaborazione, verifiche periodiche, tramite invio di specifici report a cadenza …….. (la cadenza è annuale, salvo che il rapporto contrattuale o convenzionale con il Responsabile esterno abbia durata inferiore) e/o a richiesta, contenenti (a titolo esemplificativo e a seconda dell'incarico affidato al Responsabile esterno) le seguenti informazioni: adozione del Documento programmatico sulla Sicurezza (DPS); adozione degli atti di individuazione degli incaricati, specificando in particolare le istruzioni fornite agli incaricati stessi; predisposizione dell'informativa di cui all'art. 13 del Codice (nel caso in cui il trattamento consista in una raccolta di dati personali), con specifica delle modalità operative con cui la stessa è portata a conoscenza degli interessati (ad esempio: consegna di copia dell'informativa e raccolta della firma per presa visione) ;

h) attestare, qualora l'incarico affidato ricomprenda l'adozione di misure minime di sicurezza, la conformità degli interventi alle disposizioni di cui alla misura 25 dell'Allegato B del Codice e trasmettere tale attestazione al Direttore dell'Agenzia regionale;

Tutti i testi dei principali riferimenti normativi citati sono pubblicati all'indirizzo http://www.regione.emilia-romagna.it/privacy.htm

Gli indirizzi applicativi e il Disciplinare/i tecnico/i menzionato/i è/sono allegato/i al presente contratto/convenzione/verbale di aggiudicazione/provvedimento di nomina.

ALLEGATO 3

ESERCIZIO DEI DIRITTI DI CUI ALL'ARTICOLO 7 DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (D. LGS. N. 196 DEL 30 GIUGNO 2003)

Luogo, …… Data ……..

Spett.le Agenzia regionale di Protezione Civile

Io sottoscritto.....……, nato a……..……, prov. ....., il.....……., residente a…….....…….……...……..., prov. .....…..., in via/piazza……..…….……n……..…CAP…..……..,

in qualità di:

- ❑ **interessato** *(1)*
- ❑ **delegato o procuratore dell'interessato** *(2)*

……
(indicare il nome dell'interessato)
nato a……, prov. ....., il.....……., residente a ….....……....…..…, prov. ....., in via/piazza……..……n……CAP…..……..,

la cui legittimità a presentare la richiesta è data dalla procura
- ❑ allegata
- ❑ esibita ……
(*spazio riservato all'ufficio)*

o dalla delega
- ❑ sottoscritta in presenza di ……
(*spazio riservato all'ufficio)*
- ❑ sottoscritta con fotocopia di un documento dell'interessato

- ❑ **legale rappresentante** *(3)*

……
……..
(indicare ente, associazione, organismo)

- ❑ **interessato a dati personali di persona deceduta** *(4)*

……
nato a……, prov. ....., il .....……..,
(indicare il nome e i dati della persona deceduta)

Per le ragioni di seguito manifestate
……
……
……
……

La cui identità è stata verificata sulla base degli elementi di valutazione esibiti/allegati alla presente richiesta *(5)*……
…….
(*spazio riservato all'ufficio)*

A) Ai sensi dell'art. 7, comma 1, del D.Lgs. n. 196/2003, richiedo (questa richiesta può essere formulata anche oralmente)**:**

- ❑ la conferma dell'esistenza o meno nel vostro archivio o sistema informativo di dati personali che mi riguardano/che riguardano l'interessato, anche se non ancora registrati, relativamente a :

……
……
……
……
……

(indicare il particolare trattamento, o gli specifici dati o categorie di dati personali. Diversamente il riscontro comprenderà tutti i dati personali dell'interessato trattati dall' Agenzia regionale di Protezione Civile)

- ❑ la comunicazione in forma intelligibile dei medesimi dati.

La richiesta può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.
Per ogni richiesta di cui all'art. 7, comma 1, del D.Lgs. 196/2003, l 'Agenzia regionale di Protezione Civile si riserva di richiedere all'interessato - qualora non risulti confermata l'esistenza di dati che lo riguardano - un contributo spese.

B) Ai sensi dell'art. 7, comma 2, del D.Lgs. n. 196/2003, con specifico riferimento ai dati personali che mi riguardano/che riguardano l'interessato, anche se non ancora registrati, richiedo:

- ❑ di ottenere l'indicazione *(6)*, (questa richiesta può essere formulata anche oralmente):

  - ❑ delle finalità e modalità del trattamento da voi effettuato sui miei dati personali/sui dati personali dell'interessato;
  - ❑ della logica applicata, qualora i dati fossero trattati con l'ausilio di strumenti informatici *(7)*;
  - ❑ degli estremi identificativi del titolare e dei responsabili da esso designati;
  - ❑ 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.

relativamente a :

……
……
……
……
…….

(indicare il particolare trattamento, o gli specifici dati o categorie di dati personali. Diversamente il riscontro comprenderà tutti i dati personali dell'interessato trattati dall'Agenzia regionale di Protezione Civile)

La richiesta può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.
Per ogni richiesta di cui all'art. 7, comma 2, lettere a), b) e c) del D.Lgs. 196/2003, l 'Agenzia regionale di Protezione Civile si riserva di richiedere all'interessato - qualora non risulti confermata l'esistenza di dati che lo riguardano - un contributo spese

C) Ai sensi dell'art. 7, comma 3, lettera a) del D.Lgs. n. 196/2003, richiedo:

- ❑ l'**aggiornamento** *(8)* dei miei dati personali/dei dati personali dell'interessato

  Dati da aggiornare:

  ……
  ……
  ……

Dati aggiornati:
……
……
……
(indicare gli aggiornamenti)

❑ la **rettifica** *(9)* dei miei dati personali/dei dati personali dell'interessato
Dati da rettificare:
……
……
……

Dati rettificati:
……
……
……
(indicare le rettifiche)

❑ l'**integrazione** *(10)* dei miei dati personali/dei dati personali dell'interessato
……
……
……
……
……
(indicare le integrazioni da fare e l'interesse a richiederle).

 Richiedo altresì l'attestazione che le operazioni sopra descritte sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati in precedenza comunicati *(11).*

Dichiaro, ai sensi degli articoli 46 e 47 del DPR 445/00, che quanto indicato nella presente richiesta corrisponde al vero *(12).*

D) Ho constatato che il trattamento dei miei dati personali/dei dati personali dell'interessato da Voi detenuti per
……
……
……
……
(indicare le finalità così come risultanti dall'informativa resa dall'Agenzia regionale di Protezione Civile)

è avvenuto in violazione di legge *(13)*
……
……
……..
(indicare sommariamente la violazione)

Ai sensi dell'art. 7, comma 3, lettera b) del D.Lgs. n. 196/2003,

richiedo

❑ la cancellazione *(14)*
❑ la trasformazione in forma anonima *(15)*
❑ il blocco *(16)*

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.

in alternativa richiedo

- ❑ che la scelta tra le modalità sopra indicate sia in capo all'Agenzia regionale di Protezione Civile, che opterà per la cancellazione qualora il trattamento sia stato effettuato determinando una violazione di legge insanabile e opterà per la trasformazione in forma anonima o il blocco se il trattamento ha determinato una violazione alla quale sia possibile porre rimedio. In quest'ultimo caso, il trattamento potrà riprendere nuovamente una volta ripristinata la situazione di liceità.

 Richiedo altresì l'attestazione, da parte vostra, che le operazioni sopra descritte sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati in precedenza comunicati.

E) Ai sensi dell'art. 7, comma 4, del D.Lgs. n. 196/2003, mi oppongo *(17)*

al trattamento dei miei dati personali/dei dati personali dell'interessato da Voi effettuato, relativi a

……..
……..
……..
(indicare il particolare trattamento, o gli specifici dati o categorie di dati personali. Diversamente l'opposizione si intenderà per tutti i dati personali dell'interessato trattati dall'Agenzia regionale di Protezione Civile)

per i seguenti motivi:
.....……
……
……
……
…….

(indicare i "motivi legittimi" in base ai quali ci si oppone al trattamento, tenendo conto che la legge non individua una fattispecie precisa, ma prevede solo la "legittimità" del motivo di opposizione)

Chiedo che il riscontro *(18)* su quanto richiesto sia comunicato al seguente recapito:
……
……

n. fax ……..

e-mail …….

Distinti saluti

.....……..
(firma leggibile)

(1) *Persona fisica a cui si riferiscono i dati.*

(2) *Persona fisica, ente, associazione od organismo a cui l'interessato ha conferito per iscritto delega o procura. Art.9, comma 4, del D.Lgs. n. 196 del 2003 "….L a 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 di un documento di riconoscimento dell'interessato".*

(3) *Legale rappresentante dell'ente, associazione od organismo a cui si riferiscono i dati.*

(4) *Art.9, comma 3, del D.Lgs. n. 196 del 2003: "I diritti di cui all'art 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".*

(5) *Art.9, comma 4, del D.Lgs. n. 196 del 2003: "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 ….".*

(6) *Barrare le indicazioni di interesse.*

(7) *Solo per i trattamenti effettuati con l'ausilio di strumenti informatici.*

(8) *Barrare la casella* ***aggiornamento*** *se si intende apportare variazioni ai propri dati personali/ai dati personali dell'interessato per rappresentare la situazione più recente.*

(9) *Barrare la casella* ***rettifica*** *se si intende correggere dati personali inesatti.*

(10) *Barrare la casella* ***integrazione*** *se si intende aggiungere dati personali mancanti.*

(11) *Art.7, comma 3- lettera c, D.lgs. n. 196 del 2003: "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".*

(12) *E' richiesta fotocopia di un documento di riconoscimento dell'interessato. In caso di delega è richiesta fotocopia di un documento di identità del delegante ed esibizione del documento di identità del delegato al responsabile o incaricato del trattamento. L'Amministrazione regionale provvederà ad effettuare controlli a campione sulla veridicità delle dichiarazioni rese. Qualora dal controllo emergesse la non veridicità del contenuto delle dichiarazioni, l'interessato, posta la responsabilità penale a suo carico ai sensi dell'art 76 del DPR 28.12.2000, n. 445, decade dai benefici eventualmente conseguiti sulla base delle medesime.*

(13) *Per violazione di legge si intende una violazione delle prescrizioni normative relative al trattamento, che abbia comportato una lesione in capo all'interessato, o una violazione delle prescrizioni normative che disciplinano l'attività del titolare o del responsabile*

(14) *Per cancellazione si intende la distruzione del dato personale, che rende l'informazione da esso ricavabile non intelligibile né tecnicamente ricostruibile in alcun modo*

(15) *Per trasformazione in forma anonima si intende il trattamento attraverso il quale un dato personale non può più essere associato ad un interessato*

(16) *Per blocco si intende la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento*

(17) *L'opposizione non è subordinata all'effettuazione di un trattamento illecito. Unica condizione per l'opposizione è la sussistenza di motivi legittimi che giustifichino l'interruzione del trattamento. Il diritto di opposizione si esplica con la cessazione dell'utilizzo del dato personale per la finalità oggetto dell'opposizione.*

(18) *Il riscontro alla richiesta sarà fornito entro 15 giorni dal suo ricevimento. Se le operazioni necessarie per un integrale riscontro sono di particolare complessità, o se ricorre un altro giustificato motivo, ne verrà data comunicazione all'interessato e l'integrale riscontro sarà fornito entro 30 giorni dal ricevimento della richiesta. Nel caso in cui non venga data risposta, o venga rifiutato l'accesso, l'interessato potrà ricorrere all'autorità giudiziaria ordinaria o al Garante per la protezione dei dati personali per le forme di tutela previste.*

ALLEGATO 4

N.B. Se le immagini non sono registrate, sostituire il termine "registrazione" con quello di "rilevazione".

ALLEGATO 5

PRINCIPALI DISPOSIZIONI DEL DECRETO LEGISLATIVO N. 196/2003 "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI"

Tra le disposizioni del Codice si segnalano quelle di particolare rilievo per gli operatori pubblici, recanti principi, definizioni aventi la funzione di chiarire i vari concetti utilizzati nel resto del corpo normativo, finalità, regole di comportamento e sanzioni e il cui testo è di seguito riportato, in alcuni casi, in versione integrale, e in altri, in forma sintetica. In qualche caso sono evidenziati elementi utili di riferimento per i trattamenti effettuati dall'Agenzia regionale. Per una lettura integrale delle norme del Codice, siano esse richiamate o meno nel presente allegato, si rinvia comunque al relativo testo reperibile nella sezione "Privacy" di Internos, alla voce "normativa".

Il Codice si compone di tre Parti:
la Parte I reca "Disposizioni generali" (articoli dal 1 al 45);
la Parte II reca"Disposizioni relative a specifici settori" (articoli dal 46 al 139);
la Parte III reca "Tutela dell'interessato e sanzioni" (articoli dal 140 al 186).

Della Parte I del Codice nei presenti indirizzi applicativi sono richiamati:

- il Titolo I, recante "Principi generali": articoli dal 1 al 4;
- il Titolo II, recante "Diritti dell'interessato": articoli dal 7 al 9;.
- il Titolo III recante "Regole generali per il trattamento dei dati"; Capo I "Regole per tutti i trattamenti": articoli 11, 13, 15 e 16; Capo II "Regole per tutti i soggetti pubblici": articoli dal 18 al 22;
- il Titolo IV, recante "Soggetti che effettuano il trattamento": articoli dal 28 al 30;
- il Titolo V, recante "Sicurezza dei dati e dei sistemi"; Capo I "Misure di sicurezza": articolo 31; Capo II "Misure minime di sicurezza": articoli dal 33 al 35;
- il Titolo VI, recante "Adempimenti": articoli 37 e 38.

Della Parte II del Codice è richiamato:

- il Titolo IV, recante "Trattamenti in ambito pubblico"; Capo I "Accesso ai documenti amministrativi": articoli 59 e 60.

Della Parte III del Codice è richiamato:

- il Titolo III, recante "Sanzioni"; Capo I "Violazioni amministrative": articoli dal 161 al 166; Capo II "Illeciti penali": articolo dal 167 al 172.

PARTE I “DISPOSIZIONI GENERALI”

TITOLO I, recante “Principi generali”: articoli dal 1 al 4

L’articolo 1 (Diritto alla protezione dei dati personali) prevede che chiunque ha diritto alla protezione dei dati personali che lo riguardano.

L’articolo 2 (Finalità) prevede che il Codice garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali..

L’articolo 3 (Principio di necessità nel trattamento dei dati) prevede che i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

L’articolo 4 (Definizioni) prevede che, ai fini del Codice si intende per:

"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;

"dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

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

"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, nonchè i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

"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;

"titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le

decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

"responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

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

"interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

"comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

"diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

"dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

"blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

"banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

"Garante", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

"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 abbonato o utente ricevente, identificato o identificabile;

"chiamata", la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;

"reti di comunicazione elettronica", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse 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 sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

"rete pubblica di comunicazioni", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

"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;

"abbonato", 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 ditali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

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

"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;

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

"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;

"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.

"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;

"strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

"autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

"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;

"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;

"profilo di autorizzazione", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonchè i trattamenti ad essa consentiti;

"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.

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

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

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

TITOLO II, recante "Diritti dell'interessato": articoli dal 7 al 9

L'articolo 7 (Diritto di accesso ai dati personali ed altri diritti) prevede che:
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, ancorchè 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.

L'articolo 8 (Esercizio dei diritti) prevede che 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. **Al riguardo si evidenzia che ai sensi dell'art. 146, commi 2 e 3 del Codice, il riscontro a tale richiesta è fornito entro 15 giorni dal suo ricevimento e che ove le operazioni necessarie per un integrale riscontro sono di particolare complessità, ovvero ricorre altro giustificato motivo, il titolare o il responsabile ne danno comunicazione all'interessato. In tal caso, il termine per l'integrale riscontro è di 30 giorni dal ricevimento della richiesta medesima.**

L'articolo 9 (Modalità di esercizio) prevede che la richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. 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. 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.

TITOLO III recante "Regole generali per il trattamento dei dati"

Capo I "Regole per tutti i trattamenti": articoli 11, 13, 15 e 16

L'articolo 11 (Modalità del trattamento e requisiti dei dati) prevede che i dati personali oggetto di trattamento sono:

a) trattati in modo lecito e secondo correttezza;

b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento intermini compatibili con tali scopi;

c) esatti e, se necessario, aggiornati;

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

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

L’articolo 13 (Informativa) prevede che l’interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:

a) le finalità e le modalità del trattamento cui sono destinati i dati;

b) la natura obbligatoria o facoltativa del conferimento dei dati;

c) le conseguenze di un eventuale rifiuto di rispondere;

d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;

e) i diritti di cui all'articolo 7;

f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

L’articolo 15 (Danni cagionati per effetto del trattamento) prevede che chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

L’articolo 16 (Cessazione del trattamento) prevede che in caso di cessazione, per qualsiasi causa, di un trattamento i dati sono:

a) distrutti;

b) ceduti ad altro titolare, purchè destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;

c) conservati per fini esclusivamente personali e non destinati aduna comunicazione sistematica o alla diffusione;

d) conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 12.

La cessione dei dati in violazione di quanto previsto dalla lettera b), o di altre disposizioni rilevanti in materia di trattamento dei dati personali è priva di effetti.

Capo II "Regole per tutti i soggetti pubblici": articoli dal 18 al 22

L'articolo 18 (Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici) prevede che qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.

Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal Codice, anche in relazione alla diversa natura dei dati, nonchè dalla legge e dai regolamenti.

I soggetti pubblici non devono richiedere il consenso dell'interessato.

L'articolo 19 (Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari) prevede che il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando il trattamento svolto per lo svolgimento delle funzioni istituzionali, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente.

La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata solo se il titolare abbia previamente comunicato al Garante, ai sensi dell'articolo 39 del Codice, i dati personali che deve comunicare ad altro soggetto pubblico e solo se siano decorsi quarantacinque giorni dal ricevimento da parte del Garante di tale previa comunicazione, salvo diversa determinazione anche successiva del Garante medesimo.

La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

L'articolo 20 (Principi applicabili al trattamento di dati sensibili) prevede che il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. **Al riguardo si evidenzia che lo stesso Codice con riferimento a diverse materie ha statuito il carattere di rilevante interesse pubblico delle finalità perseguite. Si segnalano in particolare, per quanto di più immediato interesse per l'Agenzia regionale di protezione civile, l'art. 73, comma 2, lett. h) che attribuisce tale carattere alle finalità di protezione civile e l'articolo 112 che attribuisce tale carattere alle finalità di instaurazione e gestione da parte di soggetti pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato**.

Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in

riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante anche su schemi tipo. **Al riguardo si rammenta che i trattamenti di dati sensibili effettuati dall'Agenzia regionale sono quelli riportati nelle relative schede contenute nel Regolamento regionale n. 3/2006, pubblicato sul BURE-R n. 57/2006.**

L'articolo 21 (Principi applicabili al trattamento di dati giudiziari) prevede che il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili. E' comunque prevista la possibilità di rinviare, come per il trattamento di dati sensibili, ad un Regolamento la specificazione dei tipi di dati e di operazioni eseguibili. **In proposito si segnala che per l'attività di acquisizione di beni e servizi, che interessa anche l'Agenzia regionale, il Garante ha adottato appositi provvedimenti, e da ultimo il provvedimento n. 7/2007 che qualifica di rilevante interesse pubblico le finalità in detta materia.**

L'articolo 22 (Principi applicabili al trattamento di dati sensibili e giudiziari) stabilisce in particolare che i soggetti pubblici nel fornire l'informativa di cui all'articolo 13 fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.

I soggetti pubblici possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato.

I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui sopra anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.

I dati idonei a rivelare lo stato di salute non possono essere diffusi.

TITOLO IV, recante "Soggetti che effettuano il trattamento": articoli dal 28 al 30

L'articolo 28 (**Titolare del trattamento)** prevede che, quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente,associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

L’articolo 29 (Responsabile del trattamento) prevede che il responsabile è designato dal titolare facoltativamente.

Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui sopra e delle proprie istruzioni.

L’articolo 30 (Incaricati del trattamento) prevede che le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

TITOLO V, recante “Sicurezza dei dati e dei sistemi”

Capo I “Misure di sicurezza”: articolo 31

L’articolo 31 (Obblighi di sicurezza) prevede che i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Capo II “Misure minime di sicurezza”: articoli dal 33 al 35

L’articolo 33 (Misure minime) prevede che nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

L’articolo 34 (Trattamento con strumenti elettronici) prevede che il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal Disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

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.

L'articolo 35 (Trattamenti senza l'ausilio di strumenti elettronici) prevede che il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal Disciplinare tecnico contenuto nell'allegato B) al Codice, 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.

TITOLO VI recante "Adempimenti": articoli 37 e 38

L'articolo 37 (Notificazione del trattamento) prevede che il titolare ha un obbligo di previa notifica al Garante se il trattamento di dati personali cui intende procedere riguarda, tra l'altro, dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica.

L'articolo 38 (Modalità di notificazione) prevede che la notificazione del trattamento è presentata al Garante prima dell'inizio del trattamento ed una sola volta, a prescindere dal numero delle operazioni e della durata del trattamento da effettuare,e può anche riguardare uno o più trattamenti con finalità correlate.

La notificazione è validamente effettuata solo se è trasmessa per via telematica utilizzando il modello predisposto dal Garante e osservando le prescrizioni da questi impartite, anche per quanto riguarda le modalità di sottoscrizione con firma digitale e di conferma del ricevimento della notificazione. **Al riguardo si segnala che nel sito del Garante (http://www.garanteprivacy.it) è riportato il modello di notifica in parola.**

PARTE II “DISPOSIZIONI RELATIVE A SPECIFICI SETTORI”

TITOLO IV recante “Trattamenti in ambito pubblico”

Capo I “Accesso ai documenti amministrativi”: articoli 59 e 60

L’articolo 59 (Accesso ai documenti amministrativi) prevede che, fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonchè dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.

L’articolo 60 (Dati idonei a rivelare lo stato di salute e la vita sessuale) prevede che quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

PARTE III “TUTELA DELL’INTERESSATO E SANZIONI”

TITOLO III, recante “Sanzioni”

Capo I “Violazioni amministrative”: articoli dal 161 al 166

L’articolo 161 (Omessa o inidonea informativa all’interessato) prevede che la violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da tremila euro a diciottomila euro o, nei casi di dati sensibili o giudiziari o di trattamenti che presentano rischi specifici ai sensi dell'articolo 17 o, comunque, di maggiore rilevanza del pregiudizio per uno o più interessati, da cinquemila euro a trentamila euro. La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore.

L’articolo 162 (Altre fattispecie) prevede che 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 cinquemila euro a trentamila euro.

La violazione della disposizione di cui all'articolo 84, comma 1, è punita con la sanzione amministrativa del pagamento di una somma da cinquecento euro a tremila euro.

L’articolo 163 (Omessa o incompleta notificazione) prevede che 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 diecimila euro a sessantamila euro e con 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.

L’articolo 164 (Omessa informazione o esibizione al Garante) prevede che 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 quattromila euro a ventiquattro mila euro.

L’articolo 165 (Pubblicazione del provvedimento del Garante) prevede che nei casi di cui agli articoli 161, 162 e 164 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.

L’articolo 166 (Procedimento di applicazione) prevede che 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.

Capo II “Illeciti penali”: articoli dal 167 al 172

L’articolo 167 (Trattamento illecito di dati) prevede che, salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé 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.

Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé 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.

L’articolo 168 (Falsità nelle dichiarazioni e notificazioni al Garante) prevede che chiunque, 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.

L’articolo 169 (Misure di sicurezza) prevede che chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.

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 dell'ammenda stabilita per la contravvenzione. 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.

L’articolo 170 (Inosservanza dei provvedimenti del Garante) prevede che 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.

L’articolo 171 (Altre fattispecie) prevede che 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.

L’articolo 172 (Pene accessorie) prevede che la condanna per uno dei delitti previsti dal Codice importa la pubblicazione della sentenza.