Deliberazione della Giunta comunale
N. 58 del 13.03.2012

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA – AGGIORNAMENTO DATI ANNO 2011.

VERBALE

Il 13 marzo 2012 alle ore 10:00 nel palazzo comunale di Sesto San Giovanni, convocata la Giunta comunale, sono intervenuti i Signori:

N. progressivo	Cognome e Nome		Qualifica	Presenze
1	Oldrini	Giorgio	Sindaco	SI
2	Morabito	Demetrio	Vicesindaco	SI
3	Amato	Vincenzo	Assessore	SI
4	Brambilla	Ersilia	Assessore	SI
5	Chittò	Monica	Assessore	NO
6	Pozzi	Alessandro	Assessore	SI
7	Scanagatti	Roberto	Assessore	NO
8	Teormino	Lucia	Assessore	SI
9	Urro	Giovanni	Assessore	SI
10	Zucchi	Claudio	Assessore	SI

Partecipa il Segretario generale Mario Spoto.
Assume la presidenza il Sindaco, Giorgio Oldrini, che riconosciuta legale l'adunanza dichiara aperta la seduta.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA – Aggiornamento dati Anno 2011

LA GIUNTA COMUNALE

- Vista l'allegata relazione del Servizio Assistenza agli Organi del 8 marzo 2012
- Visti i pareri favorevoli espressi a norma dell'art. 49 - 1° comma del D. Lgs. n. 267/00, come da foglio allegato;
- Richiamato l'articolo l'art. 134 - 4° comma del D. Lgs. n. 267/00;;
- Con voti unanimi, espressi nelle forme di legge, anche per quanto riguarda l'immediata eseguibilità della presente deliberazione;

DELIBERA

1. di approvare l'allegato Documento Programmatico sulla Sicurezza – aggiornamento dati Anno 2011, che fa parte integrante della presente deliberazione;
2. di dare atto che la presente deliberazione non comporta impegno di spesa;
3. di dichiarare la presente deliberazione immediatamente eseguibile ai sensi dell'art. 134 – 4° comma del D.Lgs. 267/00.

RELAZIONE

Il D.Lgs. 196 del 20 giugno 2003 "Codice in materia di trattamento dei dati personali" prevede che entro il 31 marzo di ogni anno venga predisposto e/o aggiornato un Documento Programmatico sulla Sicurezza (DPS) contenente una descrizione dettagliata delle attività e della struttura dell'Ente con particolare riferimento a:

- Elenco dei trattamenti di dati personali;
- Distribuzione dei compiti e delle responsabilità;
- .Analisi dei rischi che incombono sui dati;
- Misure in essere e da adottare;
- Criteri e modalità di ripristino delle disponibilità dei dati;
- Pianificazione degli interventi formativi previsti;
- Trattamenti affidati all'esterno

A tale scopo la nostra Amministrazione, con delibera di G.C. n. 90 del 27 marzo 2007 ha approvato il Documento Programmatico sulla sicurezza dei dati aggiornato al 31 dicembre 2006, con delibera di G.C. n. 33 del 12 febbraio 2008 ha approvato il Documento Programmatico sulla sicurezza dei dati aggiornato al 31 dicembre 2007, con delibera di G.C. n. 60 del 17 marzo 2009

ha approvato il Documento Programmatico sulla sicurezza dei dati aggiornato al 31 dicembre 2008, con delibera di G.C. n. 79 del 9 marzo 2010 ha approvato il Documento Programmatico sulla sicurezza dei dati aggiornato al 31 dicembre 2009, , con delibera di G.C. n. 80 del 15 marzo 2011 ha approvato il Documento Programmatico sulla sicurezza dei dati aggiornato al 31 dicembre 2010.

Il Settore Affari Istituzionali e Legali ha provveduto, con la collaborazione di tutti i Settori dell'Amministrazione Comunale, ad inserire nell'apposito programma tutte le variazioni intervenute nel corso del 2011 e a predisporre il nuovo DPS, aggiornato alla data del 31 dicembre 2011.

Si propone quindi di approvare il DOCUMENTO PROGRAMMATICO SULLA SICUREZZA, allegato al presente atto come parte integrante, ed aggiornato al 31 dicembre 2011.

Ai sensi del punto 26 del Disciplinare tecnico in materia di misure minime di sicurezza (all. B al Codice) il Sindaco dovrà riferire nella relazione accompagnatoria del Bilancio di Esercizio dell'avvenuto aggiornamento del DPS.

Il Responsabile del Servizio Assistenza agli Organi
Patrizia Morandi

Sesto San Giovanni 8 marzo 2011

CITTÀ DI SESTO SAN GIOVANNI
MEDAGLIA D'ORO AL VALOR MILITARE

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Redatto in base alle disposizioni del

Disciplinare tecnico in materia di misure minime di sicurezza del

"Codice in materia di Protezione dei Dati Personali"

(Art. 34 e Allegato B, regola 19 del D.Lgs. 30 giugno 2003 n. 196)

e del

Provvedimento del garante del 27 novembre 2008, G.U. n. 300 del 24 dicembre 2008

Provvedimento del Garante del 8 aprile 2010 pubblicato su G.U. n. 99 del 29 aprile 2010.

INDICE

Sezione I Documento Programmatico Sulla Sicurezza.

1. 1 **Revisione** 1
1.1. Scopo 1
1.2 Campo di applicazione. 2
1.3 Riferimenti normativi 3
1.4. Definizioni 4
1.4.1. Trattamento 4
1.4.2. Dato personale 4
1.4.3. Dati sensibili 4
1.4.4. Dati giudiziari 4
1.4.5. Titolare 4
1.4.6. Responsabile 4
1.4.7. Incaricati 4
1.4.8. Interessato 5
1.4.9. Comunicazione 5
1.4.10. Diffusione 5
1.4.11. Dato anonimo 5
1.4.12. Blocco 5
1.4.13. Banca dati 5
1.4.14. Comunicazione elettronica 5
1.4.15. Misure minime 5
1.4.16. Strumenti elettronici 6
1.4.17. Autenticazione informatica 6
1.4.18. Credenziali di autenticazione 6
1.4.19. Parola chiave 6
1.4.20. Profilo di autorizzazione 6
1.4.21. Sistema di autorizzazione 6

Sezione II Ruoli, compiti e nomina delle figure previste per la sicurezza dei dati personali.

1.1. Titolare del trattamento dei dati personali. 7
1.1..1. Compiti del titolare del trattamento dei dati personali 7
1.2. Amministratore di sistema 8
1.2..1. Compiti dell'Amministratori di sistema 9
1.2..2. Nomina dell'Amministratore di sistema 10
1.3. Responsabile del trattamento 11
1.3..1. Compiti del Responsabile del Trattamento 11
1.3..2. Nomina dei responsabili del trattamento 11
1.4. Incaricati della gestione e della manutenzione degli strumenti elettronici 13
1.4..1. Compiti degli incaricati della gestione e della manutenzione degli strumenti elettronici 13
1.4..2. Nomina degli incaricati della gestione e della manutenzione degli strumenti elettronici 14
1.5. Incaricati della custodia delle credenziali 15
1.5..1. Compiti degli incaricati custodia delle credenziali 15
1.5..2. Nomina degli incaricati custodia delle credenziali 16
1.6. Incaricato delle copie di sicurezza delle Banche dati 17
1.6..1. Compiti dell'incaricato delle copie di sicurezza delle Banche dati 17
1.6..2. Nomina degli incaricati delle copie di sicurezza delle Banche dati. 18
1.7. Incaricato del trattamento dei dati personali. 19
1.7..1. Compiti degli incaricati del trattamento dei dati personali. 19
1.7..2. Nomina degli incaricati del trattamento dei dati. 21

2. Trattamenti di dati personali 22
2.1. elenco degli archivi dei dati oggetto del trattamento (punto 19.1 del disciplinare) 22
2.2. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati. 22
2.2..1. Distribuzione dei compiti e delle responsabilità 22
2.2..2. Elenco dei soggetti autorizzati al trattamento dei dati. 22
2.2..3. Formazione degli incaricati 22
2.3. Analisi dei rischi nel trattamento dei dati 23
2.4. Misure da adottare per garantire l'integrità e la disponibilità dei dati 23
2.5. Misure da adottare per garantire l'integrità e la disponibilità dei dati 23

3. Criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti affidati all'esterno della struttura del titolare. 24
3.1. Trattamenti di dati personali affidati all'esterno della struttura del titolare. 24
3.2. Nomina del Responsabile del trattamento in Out-sourcing. 24

4. Diritti dell'interessato 25
4.1. Diritto di accesso ai dati personali 25
4.2. Esercizio dei diritti 25
4.3. Modalità di esercizio 26
4.4. Riscontro all'interessato 28

Allegati

LI_ASIS	lettera di nomina	Amministratore di sistema
LI_RST	lettera d'incarico	Responsabile del trattamento dei dati
LI_IDT	lettera d'incarico	Incaricato del trattamento dei dati personali
DTEC_W	lettera d'incarico	Responsabile del trattamento dei dati in Out-Sourcing
DTEC_A		Elenco degli archivi dei dati oggetto del trattamento
DTEC_B		Elenco delle sedi/uffici in cui vengono trattati i dati
DTEC_C		Elenco Amministratori di base dati, di sistema e di reti
DTEC_D		Sistemi di elaborazione per il trattamento dei dati
DTEC_E		Soggetti terzi a cui è affidato il trattamento dei dati in Out-Sourcing
DTEC_F		Personale autorizzato al trattamento dei dati
DTEC_G		Permessi di accesso ai dati
DTEC_H		Piano di formazione del personale autorizzato al trattamento dei dati
DTEC_J		Distribuzione dei compiti e delle responsabilità
DTEC_M		Criteri e procedure per garantire l'integrità dei dati
DTEC_N		Piano di formazione degli incaricati di back-up
DTEC_O		Report annuale rischi
DTEC_P		Report annuale misure da adottare
DTEC_S		Criteri di assegnazione delle credenziali
DTEC_V		Videosorveglianza

Sezione I - Documento Programmatico Sulla Sicurezza.

1. Revisione

Indice delle revisioni

Rev	Data	Decrizione	Redatto	Verificato	Approvato
1	31/12/2006	Aggiornamento	Gennaio 2007	Febbraio 2007	Del. G.C. n° 95 del 27 marzo 2007
2	31/12/2007	Aggiornamento	Gennaio 2008	Gennaio 2008	Del. G.C. n° 33 del 12/02/2008
3	31/12/2008	Aggiornamento	Gennaio 2009	Febbraio 2009	Del. G.C. n° 60 del 17/03/2009
4	31/12/2009	Aggiornamento	Gennaio 2010	Febbraio 2010	Del. G.C. n° 79 del 09/03/2010
5	31/12/2010	Aggiornamento	Gennaio 2011	Febbraio 2011	Del. G.C. n° 80 del 15/03/2011

1.1 Scopo

Il presente Documento Programmatico Sulla Sicurezza è redatto per soddisfare tutte le misure minime di sicurezza che devono essere adottate in via preventiva da tutti coloro che trattano dati personali, conformemente a quanto previsto dal **Codice in materia di protezione dei dati personali (Digs. n.196 del 30 giugno 2003)**.

Inoltre costituisce un valido strumento per la adozione delle misure previste **dall'Art. 31, dall'Art. 34 e dall'Art. 35** dello stesso **Codice in materia di protezione dei dati personali (Digs. n.196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Digs. n.196 del 30 giugno 2003)**.

Questo documento ha lo scopo di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali, effettuato dal Comune di Sesto San Giovanni, in modo da ridurre al minimo i rischi di distruzione o perdita, anche in modo accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.

1.2 Campo di applicazione

Il Documento Programmatico Sulla Sicurezza definisce le politiche e gli standard di sicurezza in merito al trattamento di tutti i dati personali.

Il Documento Programmatico Sulla Sicurezza riguarda il trattamento di tutti i dati personali:

- Sensibili
- Giudiziari
- Comuni

Il Documento Programmatico Sulla Sicurezza si applica al trattamento di tutti i dati personali effettuato per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (ad esempio cartacei, visivi, ecc..)

Il Documento programmatico sulla sicurezza deve essere conosciuto ed applicato da tutte le funzioni che fanno parte dell'organizzazione.

1.3 Riferimenti normativi

a. Codice in Materia di Dati Personali (D.Lgs. n. 196 del 30 giugno 2003);
b. Disciplinare Tecnico in Materia di Misure Minime di Sicurezza (Allegato B al D.Lgs n. 196 del 30 giugno 2003);
c. Provvedimento del Garante del 27 novmbre 2008 pubblicato su G.U. n. 300 del 24 dicembre 2008.
d. Provvedimento del Garante del 8 aprile 2010 pubblicato su G.U. n. 99 del 29 aprile 2010.

1.4. Definizioni

1.4.1. Trattamento

Qualunque operazione o complesso di operazioni, effettuate 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.

1.4.2. 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.

1.4.3. Dati sensibili

I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

1.4.4. 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.

1.4.5. 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.

1.4.6. 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.

1.4.7. Incaricati

Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

1.4.8. Interessato

La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

1.4.9. 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.

1.4.10. Diffusione

Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

1.4.11. Dato anonimo

Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

1.4.12. Blocco

La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

1.4.13. Banca dati

Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

1.4.14. 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.

1.4.15. 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.

1.4.16. Strumenti elettronici

Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

1.4.17. Autenticazione informatica

L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

1.4.18. 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.

1.4.19. 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.

1.4.20. Profilo di autorizzazione

L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

1.4.21. 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.

Sezione II - Ruoli, compiti e nomina delle figure previste per la sicurezza dei dati personali.

1.1. Titolare del trattamento dei dati personali.

1.1..1. Compiti del titolare del trattamento dei dati personali

In base a quanto stabilito dall'**Art. 4, comma 1, lettera f) del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** il *"**Titolare del trattamento** è 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".*

Il **Titolare del trattamento** si impegna ad assicurare e garantire direttamente che vengano adottate le misure di sicurezza ai sensi del **Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** e del **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003)** tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previe idonee istruzioni fornite per iscritto.

Il **Titolare del trattamento** può decidere, qualora lo ritenga opportuno, di affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.

In base a quanto stabilito dall'**Art. 29 del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)**, il **Titolare del trattamento**, ove necessario, per esigenze organizzative, può designare facoltativamente uno o più soggetti **Responsabili del trattamento** anche mediante suddivisione di compiti.

I **Responsabili del trattamento** sono individuati 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.

I compiti affidati ai **Responsabili del trattamento** sono analiticamente specificati per iscritto dal **Titolare del trattamento**.

I **Responsabili del trattamento** effettuano il trattamento attenendosi alle istruzioni impartite dal **Titolare del trattamento**.

- In base a quanto stabilito dall'**Art. 29 del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** il **Titolare del trattamento**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più **Responsabili della sicurezza dei dati** che assicurino e garantiscano che vengano adottate tutte le misure di sicurezza ai sensi del **Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** e del **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003)**.
- Qualora il **Titolare del trattamento** ritenga di non nominare alcun **Responsabile della sicurezza dei dati**, ne assumerà tutte le responsabilità e funzioni.

CITTA' DI SESTO SAN GIOVANNI

- In base a quanto stabilito dall'**Art. 29 del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** il **Titolare del trattamento**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più **Responsabili di specifici trattamenti** con il compito di individuare, nominare e incaricare per iscritto, gli **Incaricati del trattamento dei dati personali**.
- Qualora il **Titolare del trattamento** ritenga di non nominare alcun **Responsabile di specifici trattamenti**, ne assumerà tutte le responsabilità e funzioni.

1.2. Amministratore di sistema, Base dati e rete

In base a quanto stabilito dal **Provvedimento a carattere generale del 27 novembre 2008 pubblicato nella G.U. n. 300 del 24 dicembre 2008**, il **Titolare del trattamento**, in presenza di sistemi *software* complessi, deve designare uno o più soggetti **Amministratori di sistema, Amministratori di base dati e Amministratori di rete** anche mediante suddivisione di compiti, laddove tali funzioni siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali.

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico sulla sicurezza, oppure, nei casi in cui il titolare non è tenuto a redigerlo, annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico la cui adozione è prevista dal provvedimento del Garante n. 13 del 1° marzo 2007 (in *G.U.* 10 marzo 2007, n. 58); in alternativa si possono anche

utilizzare strumenti di comunicazione interna (a es., *Intranet* aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tale forma di pubblicità o di conoscibilità non sia esclusa in forza di un'eventuale disposizione di legge che disciplini in modo difforme uno specifico settore.

Nel caso di servizi di amministrazione di sistema affidati in *outsourcing* il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi

1.2..1. Compiti dell'Amministratore di sistema, Base dati e rete

L' **Amministratore di sistema, se nominato, ha il compito di:**

- Redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione.
- Individuare, nominare e incaricare per iscritto, uno o più **incaricati della gestione e della manutenzione degli strumenti elettronici (facoltativamente può nominare anche uno o più incaricati delle copie di sicurezza delle banche dati e uno o più incaricati della custodia delle copie delle credenziali)**
- Ai sensi del Provvedimento del Garante del 27/11/2008 comma 2 lettera f, adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi

L' **Amministratore di base dati, se nominato, ha il compito di:**

- Individuare, nominare e incaricare per iscritto, uno o più **incaricati delle copie di sicurezza delle banche dati.**
- Individuare, nominare e incaricare per iscritto, uno o più **incaricati della custodia delle copie delle credenziali.**
- Custodire e conservare i supporti utilizzati per le copie dei dati.

• Ai sensi del Provvedimento del Garante del 27/11/2008 comma 2 lettera f, adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi

L' **Amministratore di rete, se nominato, ha il compito di:**

• Gestire e mantenere le connessioni di rete aziendali, garantendone la funzionalità e la sicurezza specie nei contesti nei quali queste siano interfacciate con altre reti pubbliche o private

Qualora il **Titolare del trattamento** ritenga di non nominare alcun **Amministratore di sistema, Amministratore di base dati, Amministratore di rete**, ne assumerà tutte le responsabilità e funzioni e sarà demandato a lui l'onere di nominare uno o più **incaricati della gestione e della manutenzione degli strumenti elettronici,** uno o più **incaricati delle copie di sicurezza delle banche dati,** uno o più **incaricati della custodia delle copie delle credenziali.**

Il Titolare **del trattamento** informa che

Egli ha la facoltà di prevenire ed accertare eventuali accessi non consentiti ai dati personali e con cadenza per lo meno annuale verificare la rispondenza dell'operato dell'Amministratore di Rete in merito alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali

1.2..2. Nomina dell'Amministratore di sistema, Amministratore di base di dati, Amministratore di rete

La nomina di uno o più Amministratori di sistema, Amministratore di base di dati, Amministratore di rete, deve essere fatta per iscritto da parte del Titolare con una lettera d'incarico in cui sono specificate le responsabilità che gli sono state affidate e deve essere controfirmata per accettazione.
Copia della lettera di nomina (LI_ASIS) deve essere conservata a cura del Titolare del trattamento in luogo sicuro.

Il **Titolare del trattamento** deve informare ciascun **Amministratore di sistema, Amministratore di base dati, Amministratore di rete,**delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (Digs. n.196 del 30 giugno 2003)** e del **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al Digs. n.196 del 30 giugno 2003)** e del **Provvedimento del Garante del 27 novembre 2008.**

La nomina degli **Amministratori sopra menzionati** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

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

1.3. Responsabile del trattamento

In base a quanto stabilito dall'**Art. 29 del Codice in materia di protezione dei dati personali (Digs. n.196 del 30 giugno 2003)**, il **Titolare del trattamento**, ove necessario, per esigenze organizzative, può designare facoltativamente uno o più soggetti **Responsabili del trattamento** anche mediante suddivisione di compiti.

Il **Responsabile di uno specifico trattamento di dati personali** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo al quale il **Titolare del trattamento** affida il compito di gestire il trattamento dei dati personali di una o più **Banche di dati** ed ha il compito di individuare, nominare e incaricare per iscritto, gli **incaricati del trattamento dei dati personali** del trattamento specifico di cui gli è stata assegnata la responsabilità.

I **Responsabili di uno specifico trattamento di dati personali** sono individuati 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.

1.3..1. Compiti del Responsabile del Trattamento

Il **Responsabile di uno specifico trattamento di dati personali** ha il compito di:

- Nominare gli **incaricati del trattamento dei dati personali** limitatamente alle **Banche di dati** di cui sono responsabili.
- Sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal **Codice in materia di protezione dei dati personali (Digs. n.196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Digs. n.196 del 30 giugno 2003)**.
- Dare le istruzioni adeguate agli **incaricati del trattamento** effettuato con strumenti elettronici.
- Dare le istruzioni adeguate agli **incaricati del trattamento** effettuato senza l'ausilio di strumenti elettronici.
- Verificare periodicamente, e comunque almeno annualmente, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli **incaricati del trattamento dei dati personali**.

Qualora il **Titolare del trattamento** ritenga di non nominare uno o più di un **Responsabile di uno specifico trattamento di dati personali**, ne assumerà tutte le responsabilità e funzioni.

1.3..2. Nomina dei responsabili del trattamento

La nomina di ciascun **Responsabile di uno specifico trattamento di dati personali** deve essere effettuata dal **Titolare del trattamento** con una lettera di incarico in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione.

Nella lettera di nomina devono essere indicate le **Banche dati** di cui è responsabile per quanto attiene alla sicurezza e a quanto stabilito dal **Codice in materia di protezione dei dati personali (Digs. n.196 del 30 giugno 2003)** e del **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al Digs. n.196 del 30 giugno 2003)**.

Copia della lettera di nomina (LI_RST) accettata deve essere conservata a cura del **Titolare del trattamento** in luogo sicuro.

Il **Titolare del trattamento** deve informare ciascun **Responsabile di uno specifico trattamento di dati personali** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003)**.

La nomina del **Responsabile di uno specifico trattamento di dati personali** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

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

1.4. Incaricati della gestione e della manutenzione degli strumenti elettronici

1.4..1. Compiti degli incaricati della gestione e della manutenzione degli strumenti elettronici

In conformità a quanto disposto dal **punto 15, punto 16, punto 17 e punto 20 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)** l'**Amministratore di sistema o in alternativa il Titolare del trattamento**, in relazione all'attività svolta, possono individuare, nominare e incaricare per iscritto, se lo ritengono opportuno, uno o più **incaricati della gestione e della manutenzione degli strumenti elettronici**.

L'**incaricato della gestione e della manutenzione degli strumenti elettronici** è la persona fisica che sovrintende alle risorse del sistema operativo di un elaboratore o di un sistema di **Banche di dati**.

E' onere dell'**Amministratore di sistema o in alternativa del Titolare del trattamento**, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritengono opportuno, uno o più **incaricati della gestione e della manutenzione degli strumenti elettronici**.

E' compito degli **incaricati della gestione e della manutenzione degli strumenti elettronici**:

- Attivare per tutti i trattamenti effettuati con strumenti elettronici le **Credenziali di autenticazione** assegnate agli **incaricati del trattamento,** su indicazione del **Responsabile di uno specifico trattamento di dati personali**.
- In conformità a quanto disposto dal **punto 16 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)** definire l'attivazione di idonei strumenti per la protezione contro il rischio di intrusione e dell'azione di programmi informatici aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento. Questi strumenti devono essere aggiornati con cadenza almeno semestrale.
- In conformità a quanto disposto dal **punto 17 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)** aggiornare periodicamente (almeno una volta l'anno) i programmi per elaboratore per prevenire la vulnerabilità degli strumenti elettronici e correggerne difetti. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
- In conformità a quanto disposto dal **punto 20 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)** proteggere, mediante l'utilizzo di idonei strumenti elettronici, i dati sensibili o giudiziari contro l'accesso da parte di chiunque abusivamente si introduce nel sistema informatico o telematico (art. 615-ter del Codice Penale).
- Informare l'**Amministratore di sistema** nell'eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Qualora l'**Amministratore di sistema o in alternativa il Titolare del trattamento** ritengano di non nominare alcun **incaricato della gestione e della manutenzione degli strumenti elettronici**, ne assumeranno tutte le responsabilità e funzioni.

1.4..2. Nomina degli incaricati della gestione e della manutenzione degli strumenti elettronici

L'**Amministratore di sistema o in alternativa il Titolare del trattamento** nominano uno o più soggetti **incaricati della gestione e della manutenzione degli strumenti elettronici** a cui è conferito il compito di sovrintendere al buon funzionamento delle risorse del sistema informativo e degli accessi alle **Banche di dati**.

Anche se non espressamente previsto dalla norma, è opportuno che l'**Amministratore di sistema o in alternativa il Titolare del trattamento** nominino uno o più **incaricati della gestione e della manutenzione degli strumenti elettronici**, specificando gli elaboratori o le banche dati che è chiamato a sovrintendere.

L'**Amministratore di sistema o in alternativa il Titolare del trattamento** devono informare ciascun **incaricato della gestione e della manutenzione degli strumenti elettronici** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al Dlgs. n.196 del 30 giugno 2003)**.

La nomina di uno o più **incaricati della gestione e della manutenzione degli strumenti elettronici** deve essere effettuata con una lettera di incarico e deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura dell'**Amministratore di sistema o in alternativa il Titolare del trattamento** in luogo sicuro.

L'**Amministratore di sistema o in alternativa il Titolare del trattamento** devono consegnare a ciascun **incaricato della gestione e della manutenzione degli strumenti elettronici** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina dell'**incaricato della gestione e della manutenzione degli strumenti elettronici** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina degli **incaricati della gestione e della manutenzione degli strumenti elettronici** può essere revocata in qualsiasi momento dall'**Amministratore di sistema o in alternativa il Titolare del trattamento** senza preavviso, ed eventualmente affidata ad altro soggetto

1.5. Incaricati della custodia delle credenziali

In conformità a quanto disposto dal **punto 10 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)** devono essere impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il **Titolare del trattamento** può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

E' onere del **Titolare del trattamento** o, se designato, dell'**Amministratore di base di dati**, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **incaricati della custodia delle copie delle credenziali.**

1.5..1. Compiti degli incaricati custodia delle credenziali

E' compito degli **incaricati della custodia delle copie delle credenziali:**

- Autorizzare l'assegnazione e la gestione delle **Credenziali di autenticazione** per l'accesso ai dati personali degli **incaricati del trattamento,** su richiesta del **Responsabile dello specifico trattamento**, avvalendosi del supporto tecnico dell'**incaricato della gestione e della manutenzione degli strumenti elettronici**, in conformità a quanto disposto dal **punto 3 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)**.
- Istruire gli incaricati del trattamento sull'uso delle **componenti riservata delle credenziali di autenticazione**, e sulle caratteristiche che devono avere, e sulle modalità per la loro modifica in autonomia, in conformità a quanto disposto dal **punto 4 e dal punto 5 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)**.
- Assicurare che il **Codice per l'identificazione**, laddove sia stato già utilizzato, non sia assegnato ad altri **incaricati del trattamento**, neppure in tempi diversi, in conformità a quanto disposto dal **punto 6 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)**.
- Revocare le **Credenziali di autenticazione** per l'accesso ai dati degli **incaricati del trattamento** nel caso di mancato utilizzo per oltre 6 (sei) mesi, in conformità a quanto disposto dal **punto 7 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)**.
- Revocare tutte le **Credenziali di autenticazione** non utilizzate in caso di perdita della qualità che consentiva all'**incaricato del trattamento** l'accesso ai dati personali, in conformità a quanto disposto dal **punto 8 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)**.
- Impartire istruzioni agli **incaricati del trattamento** per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento, in conformità a quanto disposto dal **punto 9 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)**.

In caso di prolungata assenza o impedimento di un **incaricato del trattamento** che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, l'**incaricato della custodia delle copie delle credenziali,** in accordo con il **Responsabile dello specifico trattamento di dati personali** può assicurare la disponibilità di dati o strumenti elettronici operando secondo le seguenti istruzioni:

1. Utilizzando i diritti di "amministratore di sistema", può modificare in modo forzoso la componente riservata delle credenziali di autenticazione dell'incaricato del trattamento dei dati personali assente o impedito ad effettuare il trattamento.
2. Comunica la componente riservata delle credenziali di autenticazione così modificata ad un altro incaricato del trattamento dei dati personali designato dal Responsabile dello specifico trattamento di dati personali il quale potrà utilizzarla solo temporaneamente.
3. Terminata l'assenza o l'impedimento dell'**Incaricato del trattamento** che aveva reso indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, quest'ultimo dovrà essere informato dell'intervento effettuato e dovrà modificare la propria componente riservata delle credenziali di autenticazione

Qualora l'**Amministratore di base di dati o in alternativa il Titolare del trattamento** ritengano di non nominare alcun **Incaricato della custodia delle copie delle credenziali**, ne assumeranno tutte le responsabilità e funzioni.

1.5..2. Nomina degli incaricati custodia delle credenziali

In conformità a quanto disposto dai **punti 3, 4, 5, 6, 7, 8, 9 e 10 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)**, l'**Amministratore di base di dati o in alternativa il Titolare del trattamento** nominano uno o più soggetti **Incaricati della custodia delle copie delle credenziali** a cui è conferito il compito di autorizzare l'assegnazione e la gestione delle **Credenziali di autenticazione** per l'accesso ai dati gestiti con strumenti elettronici.

La nomina di uno o più **Incaricati della custodia delle copie delle credenziali** deve essere effettuata con una lettera di incarico, deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura dell' **Amministratore di base di dati o in alternativa il Titolare del trattamento** in luogo sicuro.

L'**Amministratore di base di dati o in alternativa il Titolare del trattamento** devono informare gli **Incaricati della custodia delle copie delle credenziali** della responsabilità che è stata loro affidata in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al Dlgs. n.196 del 30 giugno 2003)**.

L' **Amministratore di base di dati o in alternativa il Titolare del trattamento** devono consegnare a ciascun **Incaricato della custodia delle copie delle credenziali**, una copia di tutte le norme che riguardano la Sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina di uno o più **Incaricati della custodia delle copie delle credenziali** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina di uno o più **Incaricati della custodia delle copie delle credenziali** può essere revocata in qualsiasi momento dall' **Amministratore di base di dati o in alternativa il Titolare del trattamento** senza preavviso, ed essere affidata ad altro soggetto.

1.6. Incaricato delle copie di sicurezza delle Banche dati

1.6..1. Compiti degli incaricati delle copie di sicurezza delle Banche dati

In conformità a quanto disposto dal **punto 18 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003)** l'**Amministratore di base di dati o in alternativa il Titolare del trattamento**, in relazione all'attività svolta, possono individuare, nominare e incaricare per iscritto, se lo ritengono opportuno, uno o più **incaricati delle copie di sicurezza delle banche dati.**

L'**incaricato delle copie di sicurezza delle banche dati** è la persona fisica o la persona giuridica che ha il compito di sovraintendere alla esecuzione periodica delle copie di sicurezza delle **Banche di dati** personali gestite.

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, l' **Amministratore di base di dati o in alternativa il Titolare del trattamento** stabiliscono, con il supporto tecnico dell'**incaricato della gestione e della manutenzione degli strumenti elettronici** la periodicità con cui devono essere effettuate le copie di sicurezza delle **Banche di dati** trattate.

I criteri devono essere concordati con l'**incaricato della gestione e della manutenzione degli strumenti elettronici** in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In conformità a quanto disposto dal **punto 18 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003)** la frequenza con cui devono essere effettuate le copie dei dati personali non deve superare in nessun caso i 7 (sette) giorni.

In particolare per ogni **Banca di dati** devono essere definite le seguenti specifiche:

- Il "Tipo di supporto" da utilizzare per le "Copie di Back-Up".
- Il numero di "Copie di Back-Up" effettuate ogni volta.
- Se i supporti utilizzati per le "Copie di Back-Up" sono riutilizzati e in questo caso con quale periodicità.
- Se per effettuare le "Copie di Back-Up" si utilizzano procedure automatizzate e programmate.
- Le modalità di controllo delle "Copie di Back-Up".
- La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
- L'incaricato del trattamento a cui è stato assegnato il compito di effettuare le "Copie di Back-Up".
- Le istruzioni e i comandi necessari per effettuare le "Copie di Back-Up".

E' compito degli **incaricati delle copie di sicurezza delle banche dati**:

- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dall'**Amministratore di base di dati o in alternativa il Titolare del trattamento**.
- Assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro.
- Assicurarsi della conservazione delle copie di sicurezza in luogo adatto e sicuro e ad accesso controllato.

• Di provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato.
• Di segnalare tempestivamente all'**incaricato della gestione e della manutenzione degli strumenti elettronici**, ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

Qualora l' **Amministratore di base di dati o in alternativa il Titolare del trattamento** ritengano di non nominare alcun **incaricato delle copie di sicurezza delle banche dati**, ne assumeranno tutte le responsabilità e funzioni.

1.6..2. Nomina degli incaricati delle copie di sicurezza delle banche dati

In conformità a quanto disposto dal **punto 18 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003)** l'**Amministratore di base di dati o in alternativa il Titolare del trattamento**, in relazione all'attività svolta, possono individuare, nominare e incaricare per iscritto, se lo ritengono opportuno, uno o più **incaricati delle copie di sicurezza delle banche dati** a cui è conferito il compito di effettuare periodicamente le copie di sicurezza delle Banche di dati gestite specificando gli elaboratori o le banche dati che è chiamato a sovrintendere.

L' **Amministratore di base di dati o in alternativa il Titolare del trattamento** devono informare ciascun **incaricato delle copie di sicurezza delle banche dati** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003)**.

La nomina di uno o più **incaricati delle copie di sicurezza delle banche dati** deve essere effettuata con una lettera di incarico (LI_BKP) e deve essere controfirmata.

Copia della lettera di nomina accettata deve essere conservata a cura del **Amministratore di base di dati o in alternativa il Titolare del trattamento** in luogo sicuro.

L' **Amministratore di base di dati o in alternativa il Titolare del trattamento** devono consegnare a ciascun **incaricato delle copie di sicurezza delle banche dati** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

1.7. Incaricato del trattamento dei dati personali.

1.7..1. Compiti degli incaricati del trattamento dei dati personali.

I In base a quanto stabilito dall'**Art. 30 del Dlgs. n.196 del 30 giugno 2003**, le operazioni di trattamento possono essere effettuate solo da **incaricati del trattamento** che operano sotto la diretta autorità del **Titolare del trattamento** o, se designato, del **Responsabile di uno specifico trattamento di dati personali**, attenendosi alle istruzioni impartite.

In base a quanto definito dall'**Art. 4, punto 1, comma h) del Dlgs. n.196 del 30 giugno 2003**, gli *"**Incaricati del trattamento** sono persone fisiche autorizzate a compiere operazioni di trattamento sui dati personali dal **Titolare del trattamento** o, se designato, dal **Responsabile di uno specifico trattamento di dati personali**"*.

Per i **trattamenti di dati personali effettuato con l'ausilio di strumenti elettronici**, gli **incaricati del trattamento dei dati personali** devono osservare le seguenti disposizioni:

- Gli **incaricati del trattamento dei dati personali** sono autorizzati ad effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito per iscritto e comunicato all'atto della designazione, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati aziendali che contengono i predetti dati personali.
- Il **trattamento dei dati personali** deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate e, pertanto, in conformità alle informazioni comunicate agli **interessati**.
- L'**incaricato del trattamento dei dati personali** deve prestare particolare attenzione all'esattezza dei dati trattati e, se sono inesatti o incompleti, deve provvedere ad aggiornarli tempestivamente.
- Ogni **incaricato del trattamento dei dati personali** è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.
- Gli **incaricati del trattamento dei dati personali** che hanno ricevuto le **credenziali di autenticazione** per il trattamento dei dati personali, devono conservare con la massima segretezza le **componenti riservate delle credenziali di autenticazione** (parole chiave) e i dispositivi di autenticazione in loro possesso e uso esclusivo.
- La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
- La **componente riservata delle credenziali di autenticazione** (parola chiave) non deve contenere riferimenti agevolmente riconducibili all'incaricato.
- L'**incaricato del trattamento dei dati personali** deve modificare la **componente riservata delle credenziali di autenticazione** (parola chiave) al primo utilizzo e, successivamente, almeno ogni sei mesi.
- In caso di trattamento di dati sensibili e di dati giudiziari la **componente riservata delle credenziali di autenticazione** (parola chiave) deve essere modificata almeno ogni tre mesi.
- Gli incaricati del trattamento non devono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.

Per i **trattamenti di dati personali effettuato senza l'ausilio di strumenti elettronici** gli **incaricati del trattamento dei dati personali** devono osservare le seguenti disposizioni:

- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.
- Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non dovrà lasciarli mai incustoditi.
- L'incaricato del trattamento deve inoltre controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici , composti da numerose pagine o più raccoglitori, siano sempre completi e integri.
- Al termine dell'orario di lavoro l'incaricato del trattamento deve riportare tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, nei locali individuati per la loro conservazione.
- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.
- Si deve adottare ogni cautela affinché ogni persona non autorizzata, possa venire a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici.
- Per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche.
- Particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro incaricato debitamente autorizzato;
- Documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura.
- Quando i documenti devono essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, l'incaricato del trattamento deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti.
- L'incaricato del trattamento deve inoltre evitare che un soggetto terzo non autorizzato al trattamento possa esaminare, anche solo la copertina del documento in questione.
- E' proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un incaricato autorizzato a potere trattare i dati in questione.
- Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente.
- Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico od aperto al pubblico.

1.7..2. Nomina degli incaricati del trattamento dei dati.

La nomina di ciascun **Incaricato del trattamento dei dati personali** deve essere effettuata da un **Responsabile di uno specifico trattamento di dati personali** con una **lettera di incarico** in cui sono specificati i compiti che gli sono stati affidati che deve essere controfirmata dall'interessato per presa visione.

Copia della lettera di nomina (LI_IDT) firmata deve essere conservata a cura del **Responsabile di uno specifico trattamento di dati personali** in luogo sicuro.

Il **Responsabile di uno specifico trattamento di dati personali** deve informare ciascun **Incaricato del trattamento dei dati personali** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al Dlgs. n.196 del 30 giugno 2003)**.

Il **Responsabile di uno specifico trattamento di dati personali** deve consegnare a ciascun **Incaricato del trattamento dei dati personali** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

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

Agli **Incaricati del trattamento dei dati personali** deve essere assegnata una **credenziale di autenticazione**.

Agli **Incaricati del trattamento dei dati personali** è prescritto di adottare le necessarie cautele per assicurare la segretezza della **componente riservata della credenziale di autenticazione** e la diligente custodia dei dispositivi in possesso e ad uso esclusivo dell'incaricato.

La nomina dell'**Incaricato del trattamento dei dati personali** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina dell'**Incaricato del trattamento dei dati personali** può essere revocata in qualsiasi momento dal **Responsabile dello specifico trattamento di dati personali** che gli ha affidato l'incarico, senza preavviso, ed eventualmente può essere affidata ad altro soggetto.

2. Trattamenti di dati personali

Conformemente a quanto prescrive *il punto 19* del Disciplinare tecnico, allegato B) al D.lgs. 196/2003, nel presente documento si forniscono idonee informazioni riguardanti:

2.1..1. **l'elenco degli archivi dei dati oggetto del trattamento** (punto 19.1 del disciplinare), mediante:

- l' individuazione dei tipi di dati personali trattati,
  - Per l'individuazione dei dati oggetto del trattamento deve essere utilizzato il modulo DETEC_A che deve essere allegato al Presente Documento Programmatico Sulla Sicurezza.
- la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti,
  - Per redigere l'elenco delle sedi in cui vengono trattati i dati deve essere utilizzato il modulo DETEC_B che deve essere allegato al Presente Documento Programmatico Sulla Sicurezza.
- l'elenco dei Sistemi di elaborazione per il trattamento
  - per ogni sistema deve essere utilizzato il modulo DTEC_d che deve essere allegato al presente Documento Programmatico Sulla Sicurezza.

2.2. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati.

2.2..1. Distribuzione dei compiti e delle responsabilità

La distribuzione dei compiti e delle responsabilità (punto 19.2 del disciplinare), nell'ambito delle strutture preposte al trattamento dei dati, deve essere redatto il modulo DTEC_J che deve essere allegato al presente Documento Programmatico Sulla Sicurezza.

2.2..2. Elenco dei soggetti autorizzati al trattamento dei dati.

Ogni Responsabile del trattamento dei dati personali ha il compito di:

- Nominare gli incaricati limitatamente alle banche dati di cui sono responsabili.
- Tenere aggiornato ad ogni variazione l'elenco del personale autorizzato al trattamento dei dati. (Modulo DTEC_F) che deve essere allegato al presente Documento Programmatico Sulla Sicurezza.)

2.2..3. Formazione degli incaricati

Devono essere previsti interventi formativi degli incaricati del trattamento, finalizzati a renderli edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali;
- responsabilità conseguenti;
- rischi che incombono sui dati
- misure disponibili per prevenire eventi dannosi;
- modalità per aggiornarsi sulle misure di sicurezza, adottate dal titolare.

Della previsione di interventi formativi degli incaricati del trattamento *(punto 19.6 del disciplinare)* devono essere redatti i moduli DTEC_H (piano di formazione del personale autorizzato al trattamento dei dati) e DTEC_ N (piano di formazione degli incaricati di back-up), entrambi devono essere allegati al presente Documento Programmatico Sulla Sicurezza.

2.3. Analisi dei rischi nel trattamento dei dati

Al Responsabile è affidato il compito di analizzare eventuali rischi connessi al trattamento dei dati. Deve aggiornare annualmente il report annuale dei rischi conformemente al modulo DTEC_O in conformità a quanto disposto dal Disciplinare Tecnico in materia di misure minime di sicurezza (Allegato "B" del Dlgs. n. 196 del 30 giugno 2003) il Modulo DTEC_O deve essere allegato al presente Documento Programmatico Sulla Sicurezza.

2.4. Misure da adottare per garantire l'integrità e la disponibilità dei dati

Al Responsabile della sicurezza dei dati è affidato il compito di verificare ogni anno entro il 31 marzo le misure da adottare al fine ridurre gli eventuali rischi connessi al trattamento dei dati aggiornando il Modulo DTEC_P che deve essere allegato al presente Documento Programmatico Sulla Sicurezza.

2.5. Misure da adottare per garantire l'integrità e la disponibilità dei dati

L'**Amministratore di base di dati** in collaborazione con gli **incaricati della gestione e della manutenzione degli strumenti elettronici**, al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce la periodicità con cui devono essere effettuate le copie di sicurezza delle banca di dati trattati.

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

Gli **incaricati della gestione e della manutenzione degli strumenti elettronici**, per ogni banca di dati devono predisporre le istruzioni di copia, verifica e ripristino dei dati, utilizzando il modulo DTEC_M.

In particolare per ogni banca di dati devono essere definite le seguenti specifiche:

- Il Tipo di supporto da utilizzare per le Copie di sicurezza dei dati.
- Il numero di Copie di sicurezza dei dati effettuate ogni volta
- Se i supporti utilizzati per le Copie di sicurezza dei dati sono riutilizzati e in questo caso con quale periodicità .
- Se per effettuare le Copie di sicurezza dei dati si utilizzano procedure automatizzate e programmate.
- Le modalità di controllo delle Copie di sicurezza dei dati.
- La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
- Il nome dell'incaricato a cui è stato assegnato il compito di effettuare le Copie di sicurezza dei dati.
- Le istruzioni e i comandi necessari per effettuare le Copie di sicurezza dei dati.
- Le istruzioni e i comandi necessari per effettuare il ripristino delle Copie di sicurezza dei dati.

In conformità a quanto disposto dal **punto 19.4 e dal punto 19.5 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003)** il modulo DTEC_M, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3. Criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti affidati all'esterno della struttura del titolare.

3.1. Trattamenti di dati personali affidati all'esterno della struttura del titolare.

Il Responsabile può decidere di affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.
Il Responsabile deve redigere e aggiornare, ad ogni variazione, l'elenco dei soggetti che effettuano il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare ed indicare per ognuno di essi il tipo di trattamento effettuato specificando:

- Descrizione sintetica dell'attività esternalizzata.
- Trattamenti di dati interessati
- Soggetto esterno
- Descrizione dei criteri e degli impegni assunti per l'adozione delle misure.

Per l'inventario dei soggetti a cui affidare il trattamento dei dati all'esterno della struttura del titolare, deve essere utilizzato il Modulo DTEC_E che deve essere allegato al presente Documento Programmatico Sulla Sicurezza.

3.2. Nomina del Responsabile del trattamento in Out-sourcing.

Per ogni trattamento affidato ad un soggetto esterno alla struttura del titolare, il Responsabile deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.
In conformità a quanto disposto al punto 19.7 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato "B" del Dlgs. n. 196 del 30 giugno 2003) il Responsabile del trattamento in Out-sourcing deve accettare la nomina secondo il Modulo DTEC_W che deve essere allegato al presente Documento Programmatico Sulla Sicurezza.

4. Diritti dell'interessato

4.1. Diritto di accesso ai dati personali

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 nelterritorio 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.

4.2. Esercizio dei diritti

1. I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo.
2. I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati:
   a) in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni, in materia di riciclaggio;
   b) in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive;

c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
e) ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;
f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397;
g) per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;
h) ai sensi dell'articolo 53, fermo restando quanto previsto dalla legge 1 aprile 1981, n. 121.

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

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

4.3. **Modalità di esercizio**

1. La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.

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

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

4. L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.

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

4.4. **Riscontro all'interessato**

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

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

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

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

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

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

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

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

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

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

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